	Department of Administration **Purchasing Division** **2019 Washington Street East** **Post Office Box 50130** **Charleston, WV 25305-0130**	**State of West Virginia** **Master Agreement** **Order Date:** 04-10-2024	CORRECT ORDER NUMBER MUST APPEAR ON ALL PACKAGES, INVOICES, AND SHIPPING PAPERS. QUESTIONS CONCERNING THIS ORDER SHOULD BE DIRECTED TO THE DEPARTMENT CONTACT.

Order Number:	CMA 0212 0212 CLOUD-G 1	**Procurement Folder:**	1244671
Document Name:	Statewide Contract for Google Cloud Infrastructure	**Reason for Modification:**	
Document Description:	Statewide Contract for Google Cloud Infrastructure		
Procurement Type:	Central Master Agreement		
Buyer Name:			
Telephone:			
Email:			
Shipping Method:	Best Way	**Effective Start Date:**	2024-05-01
Free on Board:	FOB Dest, Freight Prepaid	**Effective End Date:**	2026-09-15

VENDOR	**DEPARTMENT CONTACT**
Vendor Customer Code: 000000195808 CARAHSOFT TECHNOLOGY CORP 11493 SUNSET HILLS RD STE 100 RESTON VA 20190 US **Vendor Contact Phone:** 703-673-3652 **Extension:**	**Requestor Name:** Heather D Abbott **Requestor Phone:** (304) 957-8136 **Requestor Email:** heather.d.abbott@wv.gov 24 FILE LOCATION

Discount Details:

	Discount Allowed	Discount Percentage	Discount Days
#1	No	0.0000	0
#2	No		
#3	No		
#4	No		

INVOICE TO	**SHIP TO**
DEPARTMENT OF ADMINISTRATION OFFICE OF TECHNOLOGY 1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR CHARLESTON WV 25305 US	STATE OF WEST VIRGINIA VARIOUS LOCATIONS AS INDICATED BY ORDER No City WV 99999 US

6-11-24 GC

Total Order Amount:	Open End

Purchasing Division's File Copy

PURCHASING DIVISION AUTHORIZATION	**ATTORNEY GENERAL APPROVAL AS TO FORM**	**ENCUMBRANCE CERTIFICATION**
MA 04/15/2024 **DATE:** 4/10/24 **ELECTRONIC SIGNATURE ON FILE**	**DATE:** 6/24/2024 **ELECTRONIC SIGNATURE ON FILE**	**DATE:** 6-24-24 **ELECTRONIC SIGNATURE ON FILE**

Extended Description:
STATEWIDE CONTRACT

The Vendor, Carahsoft Technology Corp, agrees to enter into an open-end contract with the State of West Virginia for Google Cloud Services, per the attached Participating Addendum incorporated herein.

Effective Dates: 05/01/2024 - 09/15/2026

Line	Commodity Code	Manufacturer	Model No	Unit	Unit Price
1	81110000			EA	0.000000
	Service From	**Service To**		**Service Contract Amount**	
				0.00	

Commodity Line Description: Google Cloud Infrastructure

Extended Description:

NASPO ValuePoint
PARTICIPATING ADDENDUM

Cloud solutions 2016-2026
Lead by the State of **Utah**

Master Agreement #: AR2472

Contractor: **CARAHSOFT TECHNOLOGY CORPORATION**

Participating Entity: **State of West Virginia**

The following products or services are included in this contract portfolio:

- *All Google Cloud products and accessories listed on the Contractor page of the NASPO ValuePoint website.*

Master Agreement Terms and Conditions:

1. Scope: This addendum covers ***Cloud Solutions*** led by the State of Utah for use by state agencies and other entities located in the Participating State authorized by that state's statutes to utilize state contracts with the prior approval of the State's Chief Procurement Official.

2. Participation: This NASPO ValuePoint Master Agreement may be used by all state agencies, institutions of higher institution, political subdivisions and other entities authorized to use public contracts in the State of West Virginia. Issues of interpretation and eligibility for participation are solely within the authority of the State Chief Procurement Official.

3. Enterprise Architecture & State CIO Approval: Unless otherwise stipulated in this Participating Addendum, specific services accessed through this NASPO ValuePoint cooperative Master Agreement for Cloud Solutions by state executive branch agencies are subject to the authority and prior approval of the State Chief Information Officer's Office. The State Chief Information Officer means the individual designated by the state Governor within the Executive Branch with enterprise-wide responsibilities for leadership and management of information technology resources of a state. Additionally, the services are subject to compliance with the WV Enterprise Architecture.

4. Primary Contacts: The primary contact individuals for this Participating Addendum are as follows (or their named successors):

Contractor

Name:	Carhasoft Technology Corp.
Address:	11493 Sunset Hills Rd. Suite 100 Reston VA. 20152
Telephone:	703-871-8500
Fax:	
Email:	NASPO@carahsoft.com

Participating Entity

Name:	West Virginia Office of Technology
Address:	Building 5, 10th Floor Charleston, WV 25305
Telephone:	304-558-8100
Fax:	
Email:	heather.d.abbott@wv.gov

5. Participating Entity Modifications Or Additions To The Master Agreement

These modifications or additions apply only to actions and relationships within the Participating Entity.
Participating Entity must check one of the boxes below.

[___] No changes to the terms and conditions of the Master Agreement are required.

[X] The following changes are modifying or supplementing the Master Agreement terms and conditions.

a. Additional Contract Terms. The following additional terms are added to the Contract.

i. VOID CONTRACT CLAUSES – This Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law.

ii. BACKGROUND CHECK: In accordance with W. Va. Code § 15-2D-3, the State reserves the right to prohibit a service provider's employees from accessing sensitive or critical information or to be present at the Capitol complex based upon results addressed from a criminal background check. Service providers should contact the West Virginia Division of Protective Services by phone at (304) 558-9911 for more information.

iii. ANTITRUST: In submitting a bid to, signing a contract with, or accepting a Award Document from any agency of the State of West Virginia, the Vendor agrees to convey, sell, assign, or transfer to the State of West Virginia all rights, title, and interest in and to all causes of action it may now or hereafter acquire under the antitrust laws of the United States and the State of West Virginia for price fixing and/or unreasonable restraints of trade relating to the particular commodities or services purchased or acquired by the State of West Virginia. Such assignment shall be made and become effective at the time the purchasing agency tenders the initial payment to Vendor.

iv. PRIVACY, SECURITY, AND CONFIDENTIALITY: The Vendor agrees that it will not disclose to anyone, directly or indirectly, any such personally identifiable information or other confidential information gained from the Agency, unless the individual who is the subject of the information consents to the disclosure in writing or the disclosure is made pursuant to the Agency's policies, procedures, and rules. Vendor further agrees to comply with the Confidentiality Policies and Information Security Accountability Requirements, set forth in http://www.state.wv.us/admin/purchase/privacy/default.html

v. ISRAEL BOYCOTT: Vendor understands and agrees that pursuant to W. Va. Code § 5A-3-63, it is prohibited from engaging in a boycott of Israel during the term of this contract.

vi. NO DEBT CERTIFICATION: In accordance with West Virginia Code §§ 5A-3-10a and 5-22-1(i), the State is prohibited from awarding a contract to any bidder that owes a debt to the State or a political subdivision of the State. By submitting a bid, or entering into a contract with the State, Vendor is affirming that (1) for construction contracts, the Vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, neither the Vendor nor any related party owe a debt as defined above, and neither the Vendor nor any related party are in employer default as defined in the statute cited above unless the debt or employer default is permitted under the statute.

6. Subcontractors: All contactors, dealers, and resellers authorized in the State of West Virginia, as shown on the dedicated Contractor (cooperative contract) website, are approved to provide sales and service support to participants in the NASPO ValuePoint Master Agreement. The contractor's dealer participation will be in accordance with the terms and conditions set forth in the aforementioned Master Agreement.

7. Order of Priority: The Contract created by this Participating Addendum is comprised of the documents described below, and will be interpreted in the following order:
    a. This Participating Addendum - First Priority
    b. Carahsoft Response to West Virginia/Scope of Cloud Services - Second Priority
    c. NASPO Master Agreement Contract #AR2472 - Third Priority
    d. Google Cloud Master Agreement Public Sector - Fourth Priority
    e. Google HIPAA Business Associate Addendum - Fifth Priority
    f. Google Supplemental Terms - Sixth Priority
        I. Google Data Processing Addendum
        II. Google Cloud Platform Terms of Service
        III. Google Cloud Platform Acceptable Use Policy
        IV. Google Cloud Platform Service Specific Terms
        V. Google Cloud Platform Services Summary
        VI. Google Cloud Platform Technical Support Services Guidelines
        VII. Google Professional Services Organization (PSO) Services List
        VIII. Google Workspace Terms of Service
        IX. Google Looker Platform Service Level Agreement for Looker Hosted Deployments
        X. Google Looker Data Processing Addendum
        XI. Google Looker Service Specific Terms
        XII. Google Looker Technical Support Services Guidelines
        XIII. Google Looker Notices & Acknowledgements
        XIV. Mandiant Solutions and Services Agreement
8. Orders: Any order placed by a Participating Entity or Purchasing Entity for a product and/or service available from this Master Agreement shall be deemed to be a sale under (and governed by the prices and other terms and conditions) of the Master Agreement unless the parties to the order agree in writing that another contract or agreement applies to such order.

IN WITNESS WHEREOF, the parties have executed this Addendum as of the date of execution by both parties below.

Participating Entity: WV Office of Technology	Contractor: Carahsoft Technology Corp.
Signature:	Signature: Colby Bender
Name: Heather D. Abbott	Name: Colby Bender
Title: Chief Information Officer	Title: Contract Manager
Date: March 15, 2024	Date: 3/14/2024

[Additional signatures may be added if required by the Participating Entity]

For questions on executing a participating addendum, please contact:

NASPO ValuePoint

Cooperative Development Coordinator:	Shannon Berry
Telephone:	775-720-3404
Email:	sberry@naspovaluepoint.org

Please email fully executed PDF copy of this document to PA@naspovaluepoint.org to support documentation of participation and posting in appropriate data bases.

carahsoft.

October 25, 2022

West Virginia Office of Technology
1900 Kanawha Boulevard E.
Building 5, 10th Floor
Charleston, West Virginia 25305

Re: Carahsoft's Response to the West Virginia Office of Technology's Solicitation of Bids: West Virginia Cloud Services

Andrew Lore:

Carahsoft Technology Corp. appreciates the opportunity to respond to the West Virginia Office of Technology (WVOT)'s Solicitation of Bids: West Virginia Cloud Services.

Carahsoft is responding as a NASPO ValuePoint Cooperative Agreement contractor for Cloud Services (Master Agreement No.: AR2472, West Virginia Participating Addendum No.: WV-96A), and a reseller for Amazon Web Services (AWS), Google Cloud, and Microsoft Azure. As the Master Government Aggregator® for a portfolio of industry-leading cloud service providers, Carahsoft has combined extensive knowledge of the technologies we provide with a thorough understanding of the government procurement process, to analyze needs, provide configuration support, simplify the ordering process, and offer special government pricing since 2004. Working with resellers, systems integrators and consultants, our sales and marketing teams provide industry leading IT products, services, and training to support Public Sector organizations across Federal, State and Local Government agencies and Education and Healthcare markets.

Carahsoft has provided a signed, completed version of the Scope of Services document as a separate attachment.

Carahsoft has also provided the Identification of Service Models Matrix (Attachment B) that was submitted with our original proposal as a separate attachment.

AWS and Microsoft were added to Carahsoft's Price Catalog via modification after Carahsoft received our award in 2016. Carahsoft's current NASPO ValuePoint Price Catalog can be found at the following link: https://www.naspovaluepoint.org/portfolio/cloud-solutions-2016-2026/carahsoft-technology-corporation/

Please feel free to contact me directly at 703.889.9815/George.Nicholls@carahsoft.com or Catie Saylor at 703.230.7589/Catie.Saylor@carahsoft.com with any questions or communications that will assist WVOT in the evaluation of our response.

Thank you for your time and consideration.

Sincerely,

George Nicholls

George Nicholls
Proposals Manager

SCOPE OF SERVICES - CLOUD SERVICES

Purpose and Scope:

The West Virginia Office of Technology (WVOT) is soliciting bids to establish open-end, catalog-based statewide contracts for a traditional reseller, not solely a managed service provider (MSP) of information technology cloud services. As such, the State of West Virginia will be utilizing the NASPO Cloud Solutions contract as its prequalification agreement (found here: https://www.naspovaluepoint.org/cloud-solutions-evergreen/). Any Vendor wishing to compete for a resulting contract must first be a Vendor on NASPO Cloud Solutions.

Additionally, the State of West Virginia's Chief Information Officer (CIO), under the authority granted in WV Code §5A-6-4, has established standards for the State of West Virginia's cloud services and the resulting contracts obtained via the secondary bid process will allow the State to leverage cloud services in a quick and efficient manner on an as-needed basis. The State of WV is seeking to partner with a reseller(s) for the following cloud services providers: Microsoft Azure, Amazon Web Services, and Google Cloud. As circumstances warrant, the State will leverage the appropriate contract for public cloud services in accordance with state policy to include the enterprise architecture (EA) policy and standards. (https://sites.google.com/wv.gov/wvotenterprisearchitecture/home)

Cloud instances (IaaS/PaaS) procured through the contract(s) will be provisioned within a West Virginia-owned cloud environment, at the state's discretion. Cloud services (SaaS) procured will reside in the cloud environment presenting the State best value. The contract rates shall be uploadable into the appropriate public cloud environment, allowing the state to evaluate usage/cost projections.

Requirements:

- Vendors must be authorized to sell at least one (1) of the proposed cloud service providers (Microsoft Azure, Amazon Web Services, Google Cloud) on the NASPO Cloud Solutions contract. Must provide a copy of contractual documentation from the NASPO Cloud Contract illustrating the vendor response for such services. The State prefers the Vendor provide validation by submitting Attachment H Identification of Service Models published in the NASPO solicitation.

  Is your firm an authorized reseller of Microsoft Azure on the NASPO Cloud Solutions contract?

  __X__ Yes _____ No

  Is your firm an authorized reseller of Amazon Web Services on the NASPO Cloud Solutions contract?

  __X__ Yes _____ No

  Is your firm an authorized reseller of Google Cloud on the NASPO Cloud Solutions contract?

__X__ Yes _____ No

- Vendors must be eligible to provide the entire service catalog for its cloud offerings including Infrastructure as a Service (Iaas), Software as a Service (SaaS), Platform as a Service (PaaS), and Value-Add Services (VAS) to accomplish implementations and support on the NASPO Cloud Solutions contract.

  Is your firm authorized to sell the entire catalog for Microsoft Azure?

  __X__ Yes _____ No

  Is your firm authorized to sell the entire catalog for Amazon Web Services?

  __X__ Yes _____ No

  Is your firm authorized to sell the entire catalog for Google Cloud?

  __X__ Yes _____ No

- Vendors must provide a minimum percentage discount off list price equal to or greater than what is provided in the NASPO Cloud Solutions contract.

  Does your firm agree to supply the State of West Virginia with a percentage discount greater than or equal to what is provided in the NASPO Cloud Solutions contract?

  __X__ Yes _____ No

- Vendors must provide all catalog items on an ongoing, as-needed basis to the State and the minimum percentage discount must be firm for the term of the contract.

  Does your firm agree to provide all catalog items on an on-going, as-needed basis to the State and further agree that the minimum percentage discount will be firm for the term of the contract?

  __X__ Yes _____ No

- Vendors must provide the minimum percentage discount for the catalog of services it will supply to the State.
  - Vendors are not required to bid on each Microsoft Azure, Amazon Web Services, and Google Cloud in order to secure a contract.
  - The State will award contract(s) to the Vendor with lowest cost to the State for each of the three named providers. (Ex. Vendor with lowest cost to the State for Microsoft Azure catalog will receive one contract, Vendor with lowest cost to the State for Amazon Web Services will receive one contract, and Vendor with lowest cost to the State for Google Cloud will receive one contract.)

- An award will be based on the total combined percentage discount for each of the services, i.e., (IaaS Discount + PaaS Discount + SaaS Discount + Value-Add Services Discount = Combined Total Discount.)

Service	Minimum Percentage Discount
Amazon Web Services (AWS)	
IaaS	2%
PaaS	2%
SaaS	2%
Value-Add Services	2%
Google Cloud	
IaaS	2%
PaaS	2%
SaaS	2%
Value-Add Services	1%
Microsoft Azure	
IaaS	2%
PaaS	2%
SaaS	2%
Value-Add Services	2%

- Vendors must not fulfill any orders under a resulting agreement without first obtaining approval from the West Virginia Office of Technology.

  Does your firm agree to not fulfill any orders from a resulting contract without approval from the West Virginia Office of Technology?

  X Yes _____ No

CERTIFICATION AND SIGNATURE: By signing below, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Carahsoft Technology Corp.

(Company Name)

George Nicholls George Nicholls, Proposals Manager 10-24-2022

(Authorized Signature and Printed Name) Date

Contract # AR2472

STATE OF UTAH COOPERATIVE CONTRACT

1. CONTRACTING PARTIES: This contract is between the Division of Purchasing and the following Contractor:

Carahsoft Technology Corporation
Name
1860 Michael Faraday Drive, Suite 100
Address
Reston | VA | 20190
City | State | Zip

LEGAL STATUS OF CONTRACTOR
- ☐ Sole Proprietor
- ☐ Non-Profit Corporation
- ☒ For-Profit Corporation
- ☐ Partnership
- ☐ Government Agency

Contact Person Bethany Blackwell Phone #703-230-7435 Email NASPO@carahsoft.com
Vendor #VC0000116540 Commodity Code #920-05

2. GENERAL PURPOSE OF CONTRACT: Contractor is permitted to provide the Cloud Solutions identified in Attachment B to Participating States once a Participating Addendum has been signed

3. PROCUREMENT PROCESS: This contract is entered into as a result of the procurement process on Bid#CH16012.

4. CONTRACT PERIOD: Effective Date: 10/14/2016 Termination Date: 09/15/2026 unless terminated early or extended in accordance with the terms and conditions of this contract. Note: Pursuant to Solicitation #CH16012, Contract must re-certify its qualifications each year.

5. Administrative Fee, as described in the Solicitation and Attachment A: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services.

6. ATTACHMENT A: NASPO ValuePoint Master Terms and Conditions, including the attached Exhibits
ATTACHMENT B: Scope of Services Awarded to Contractor
ATTACHMENT C: Pricing Discounts and Pricing Schedule
ATTACHMENT D: Contractor's Response to Solicitation #CH16012
ATTACHMENT E: Service Offering EULAs

Any conflicts between Attachment A and the other Attachments will be resolved in favor of Attachment A.

8. DOCUMENTS INCORPORATED INTO THIS CONTRACT BY REFERENCE BUT NOT ATTACHED:
   a. All other governmental laws, regulations, or actions applicable to the goods and/or services authorized by this contract.
   b. Utah State Procurement Code and the Procurement Rules.

9. Each signatory below represents that he or she has the requisite authority to enter into this contract.

IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

Contractor's signature — Date: 10/11/16

Robert Moore, Vice President
Type or Print Name and Title

STATE

Director, Division of Purchasing — Date: 10.13.16

Christopher Hughes	801-538-3254		christopherhughes@utah.gov
Division of Purchasing Contact Person	Telephone Number	Fax Number	Email

(Revision 16 June 2016)

This document includes salient or non-standard provisions extracted from NASPO/ValuePoint Model Contract for Cloud Services.

February 17, 2016.



Attachment A: NASPO ValuePoint Master Agreement Terms and Conditions

1. Master Agreement Order of Precedence

a. Any Order placed under this Master Agreement shall consist of the following documents:

(1) A Participating Entity's Participating Addendum[1] ("PA");
(2) NASPO ValuePoint Master Agreement Terms & Conditions, including the applicable Exhibits[2] to the Master Agreement;
(3) The Solicitation;
(4) Contractor's response to the Solicitation, as revised (if permitted) and accepted by the Lead State; and
(5) A Service Level Agreement issued against the Participating Addendum.

b. These documents shall be read to be consistent and complementary. Any conflict among these documents shall be resolved by giving priority to these documents in the order listed above. Contractor terms and conditions that apply to this Master Agreement are only those that are expressly accepted by the Lead State and must be in writing and attached to this Master Agreement as an Exhibit or Attachment.

2. Definitions - Unless otherwise provided in this Master Agreement, capitalized terms will have the meanings given to those terms in this Section.

Confidential Information means any and all information of any form that is marked as confidential or would by its nature be deemed confidential obtained by Contractor or its employees or agents in the performance of this Master Agreement, including, but not necessarily limited to (1) any Purchasing Entity's records, (2) personnel records, and (3) information concerning individuals, is confidential information of Purchasing Entity.

Contractor means the person or entity providing solutions under the terms and conditions set forth in this Master Agreement. Contractor also includes its employees, subcontractors, agents and affiliates who are providing the services agreed to under the

[1] A Sample Participating Addendum will be published after the contracts have been awarded.
[2] The Exhibits comprise the terms and conditions for the service models: PaaS, IaaS, and PaaS.

This document includes salient or non-standard provisions extracted from NASPO/ValuePoint Model Contract for Cloud Services.

February 17, 2016.

Master Agreement.

Data means all information, whether in oral or written (including electronic) form, created by or in any way originating with a Participating Entity or Purchasing Entity, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with a Participating Entity or Purchasing Entity, in the course of using and configuring the Services provided under this Agreement.

Data Breach means any actual or reasonably suspected non-authorized access to or acquisition of computerized Non-Public Data or Personal Data that compromises the security, confidentiality, or integrity of the Non-Public Data or Personal Data, or the ability of Purchasing Entity to access the Non-Public Data or Personal Data.

Data Categorization means the process of risk assessment of Data. See also "High Risk Data", "Moderate Risk Data" and "Low Risk Data".

Disabling Code means computer instructions or programs, subroutines, code, instructions, data or functions, (including but not limited to viruses, worms, date bombs or time bombs), including but not limited to other programs, data storage, computer libraries and programs that self-replicate without manual intervention, instructions programmed to activate at a predetermined time or upon a specified event, and/or programs purporting to do a meaningful function but designed for a different function, that alter, destroy, inhibit, damage, interrupt, interfere with or hinder the operation of the Purchasing Entity's' software, applications and/or its end users processing environment, the system in which it resides, or any other software or data on such system or any other system with which it is capable of communicating.

Fulfillment Partner means a third-party contractor qualified and authorized by Contractor, and approved by the Participating State under a Participating Addendum, who may, to the extent authorized by Contractor, fulfill any of the requirements of this Master Agreement including but not limited to providing Services under this Master Agreement and billing Customers directly for such Services. Contractor may, upon written notice to the Participating State, add or delete authorized Fulfillment Partners as necessary at any time during the contract term. Fulfillment Partner has no authority to amend this Master Agreement or to bind Contractor to any additional terms and conditions.

High Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("High Impact Data").

Infrastructure as a Service (IaaS) as used in this Master Agreement is defined the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run

arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Intellectual Property means any and all patents, copyrights, service marks, trademarks, trade secrets, trade names, patentable inventions, or other similar proprietary rights, in tangible or intangible form, and all rights, title, and interest therein.

Lead State means the State centrally administering the solicitation and any resulting Master Agreement(s).

Low Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Low Impact Data").

Master Agreement means this agreement executed by and between the Lead State, acting on behalf of NASPO ValuePoint, and the Contractor, as now or hereafter amended.

Moderate Risk Data is as defined in FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems ("Moderate Impact Data").

NASPO ValuePoint is the NASPO ValuePoint Cooperative Purchasing Program, facilitated by the NASPO Cooperative Purchasing Organization LLC, a 501(c)(3) limited liability company (doing business as NASPO ValuePoint) is a subsidiary organization the National Association of State Procurement Officials (NASPO), the sole member of NASPO ValuePoint. The NASPO ValuePoint Cooperative Purchasing Organization facilitates administration of the cooperative group contracting consortium of state chief procurement officials for the benefit of state departments, institutions, agencies, and political subdivisions and other eligible entities (i.e., colleges, school districts, counties, cities, some nonprofit organizations, etc.) for all states and the District of Columbia. The NASPO ValuePoint Cooperative Development Team is identified in the Master Agreement as the recipient of reports and may be performing contract administration functions as assigned by the Lead State.

Non-Public Data means High Risk Data and Moderate Risk Data that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the Purchasing Entity because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Participating Addendum means a bilateral agreement executed by a Contractor and a Participating Entity incorporating this Master Agreement and any other additional Participating Entity specific language or other requirements, e.g. ordering procedures

specific to the Participating Entity, other terms and conditions.

Participating Entity means a state, or other legal entity, properly authorized to enter into a Participating Addendum.

Participating State means a state, the District of Columbia, or one of the territories of the United States that is listed in the Request for Proposal as intending to participate. Upon execution of the Participating Addendum, a Participating State becomes a Participating Entity.

Personal Data means data alone or in combination that includes information relating to an individual that identifies the individual by name, identifying number, mark or description can be readily associated with a particular individual and which is not a public record. Personal Information may include the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or Protected Health Information (PHI) relating to a person.

Platform as a Service (PaaS) as used in this Master Agreement is defined as the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

Product means any deliverable under this Master Agreement, including Services, software, and any incidental tangible goods.

Protected Health Information (PHI) means individually identifiable health information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. PHI may also include information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

This document includes salient or non-standard provisions extracted from NASPO/ValuePoint Model Contract for Cloud Services.

February 17, 2016.

Purchasing Entity means a state, city, county, district, other political subdivision of a State, and a nonprofit organization under the laws of some states if authorized by a Participating Addendum, who issues a Purchase Order against the Master Agreement and becomes financially committed to the purchase.

Services mean any of the specifications described in the Scope of Services that are supplied or created by the Contractor pursuant to this Master Agreement.

Security Incident means the possible or actual unauthorized access to a Purchasing Entity's Non-Public Data and Personal Data the Contractor believes could reasonably result in the use, disclosure or theft of a Purchasing Entity's Non-Public Data within the possession or control of the Contractor. A Security Incident also includes a major security breach to the Contractor's system, regardless if Contractor is aware of unauthorized access to a Purchasing Entity's Non-Public Data. A Security Incident may or may not turn into a Data Breach.

Service Level Agreement (SLA) means a written agreement between both the Purchasing Entity and the Contractor that is subject to the terms and conditions in this Master Agreement and relevant Participating Addendum unless otherwise expressly agreed in writing between the Purchasing Entity and the Contractor. SLAs should include: (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) remedies, such as credits, and (5) an explanation of how remedies or credits are calculated and issued.

Software as a Service (SaaS) as used in this Master Agreement is defined as the capability provided to the consumer to use the Contractor's applications running on a Contractor's infrastructure (commonly referred to as 'cloud infrastructure). The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Solicitation means the documents used by the State of Utah, as the Lead State, to obtain Contractor's Proposal.

Statement of Work means a written statement in a solicitation document or contract that describes the Purchasing Entity's service needs and expectations.

6. Discount Guarantee Period: All discounts must be guaranteed for the entire term of the Master Agreement. Participating Entities and Purchasing Entities shall receive the immediate benefit of price or rate reduction of the services provided under this Master Agreement. A price or rate reduction will apply automatically to the Master Agreement

and an amendment is not necessary.

8. Confidentiality, Non-Disclosure, and Injunctive Relief

a. Confidentiality. Contractor acknowledges that it and its employees or agents may, in the course of providing a Product under this Master Agreement, be exposed to or acquire information that is confidential to Purchasing Entity's or Purchasing Entity's clients. Any reports or other documents or items (including software) that result from the use of the Confidential Information by Contractor shall be treated in the same manner as the Confidential Information. Confidential Information does not include information that (1) is or becomes (other than by disclosure by Contractor) publicly known; (2) is furnished by Purchasing Entity to others without restrictions similar to those imposed by this Master Agreement; (3) is rightfully in Contractor's possession without the obligation of nondisclosure prior to the time of its disclosure under this Master Agreement; (4) is obtained from a source other than Purchasing Entity without the obligation of confidentiality, (5) is disclosed with the written consent of Purchasing Entity or; (6) is independently developed by employees, agents or subcontractors of Contractor who can be shown to have had no access to the Confidential Information.

b. Non-Disclosure. Contractor shall hold Confidential Information in confidence, using at least the industry standard of confidentiality, and shall not copy, reproduce, sell, assign, license, market, transfer or otherwise dispose of, give, or disclose Confidential Information to third parties or use Confidential Information for any purposes whatsoever other than what is necessary to the performance of Orders placed under this Master Agreement. Contractor shall advise each of its employees and agents of their obligations to keep Confidential Information confidential. Contractor shall use commercially reasonable efforts to assist Purchasing Entity in identifying and preventing any unauthorized use or disclosure of any Confidential Information. Without limiting the generality of the foregoing, Contractor shall advise Purchasing Entity, applicable Participating Entity, and the Lead State immediately if Contractor learns or has reason to believe that any person who has had access to Confidential Information has violated or intends to violate the terms of this Master Agreement, and Contractor shall at its expense cooperate with Purchasing Entity in seeking injunctive or other equitable relief in the name of Purchasing Entity or Contractor against any such person. Except as directed by Purchasing Entity, Contractor will not at any time during or after the term of this Master Agreement disclose, directly or indirectly, any Confidential Information to any person, except in accordance with this Master Agreement, and that upon termination of this Master Agreement or at Purchasing Entity's request, Contractor shall turn over to Purchasing Entity all documents, papers, and other matter in Contractor's possession that embody Confidential Information. Notwithstanding the foregoing, Contractor may keep one copy of such Confidential Information necessary for quality assurance, audits and evidence of the performance of this Master Agreement.

c. Injunctive Relief. Contractor acknowledges that breach of this section, including disclosure of any Confidential Information, will cause irreparable injury to Purchasing

Entity that is inadequately compensable in damages. Accordingly, Purchasing Entity may seek and obtain injunctive relief against the breach or threatened breach of the foregoing undertakings, in addition to any other legal remedies that may be available. Contractor acknowledges and agrees that the covenants contained herein are necessary for the protection of the legitimate business interests of Purchasing Entity and are reasonable in scope and content.

d. Purchasing Entity Law. These provisions shall be applicable only to extent they are not in conflict with the applicable public disclosure laws of any Purchasing Entity.

9. Right to Publish: Throughout the duration of this Master Agreement, Contractor must secure prior approval from the Lead State or Participating Entity for the release of any information that pertains to the potential work or activities covered by the Master Agreement , including but not limited to reference to or use of the Lead State or a Participating Entity's name, Great Seal of the State, Coat of Arms, any Agency or other subunits of the State government, or any State official or employee, for commercial promotion which is strictly prohibited. News releases or release of broadcast e-mails pertaining to this Master Agreement or Participating Addendum shall not be made without prior written approval of the Lead State or a Participating Entity.

The Contractor shall not make any representations of NASPO ValuePoint's opinion or position as to the quality or effectiveness of the services that are the subject of this Master Agreement without prior written consent. Failure to adhere to this requirement may result in termination of the Master Agreement for cause.

11. Changes in Contractor Representation: The Contractor must notify the Lead State of changes in the Contractor's key administrative personnel, in writing within 10 calendar days of the change. The Lead State reserves the right to approve changes in key personnel, as identified in the Contractor's proposal. The Contractor agrees to propose replacement key personnel having substantially equal or better education, training, and experience as was possessed by the key person proposed and evaluated in the Contractor's proposal.

13. Indemnification and Limitation of Liability

a. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, and Purchasing Entities, along with their officers, agents, and employees as well as any person or entity for which they may be liable, from and against claims, damages or causes of action including reasonable attorneys' fees and related costs for any death, bodily injury, or damage to real or tangible property arising directly or indirectly from the negligent or wrongful act(s), error(s), or omission(s) of the Contractor, its employees or subcontractors or volunteers, at any tier, relating to the performance under the Master Agreement.

b. Indemnification – Intellectual Property. The Contractor shall defend, indemnify and hold harmless NASPO, NASPO ValuePoint, the Lead State, Participating Entities, Purchasing Entities, along with their officers, agents, and employees as well as any

person or entity for which they may be liable ("Indemnified Party"), from and against claims, damages or causes of action including reasonable attorneys' fees and related costs arising out of the claim that the Product or its use, infringes Intellectual Property rights ("Intellectual Property Claim") of another person or entity.

(1) The Contractor's obligations under this section shall not extend to:

a. Any use of the Services provided hereunder not contemplated in the product documentation.
b. Any use of the Services provided hereunder in combination with other products not contemplated hereunder or in the documentation, any use of modification of the Services provided hereunder except as permitted by this Agreement.

(2) The Indemnified Party shall notify the Contractor within a reasonable time after receiving notice of an Intellectual Property Claim. Even if the Indemnified Party fails to provide reasonable notice, the Contractor shall not be relieved from its obligations unless the Contractor can demonstrate that it was prejudiced in defending the Intellectual Property Claim resulting in increased expenses or loss to the Contractor and then only to the extent of the prejudice or expenses. If the Contractor promptly and reasonably investigates and defends any Intellectual Property Claim, it shall have control over the defense and settlement of it. However, the Indemnified Party must consent in writing for any money damages or obligations for which it may be responsible. The Indemnified Party shall furnish, at the Contractor's reasonable request and expense, information and assistance necessary for such defense. If the Contractor fails to vigorously pursue the defense or settlement of the Intellectual Property Claim, the Indemnified Party may assume the defense or settlement of it and the Contractor shall be liable for all costs and expenses, including reasonable attorneys' fees and related costs, incurred by the Indemnified Party in the pursuit of the Intellectual Property Claim. Unless otherwise agreed in writing, this section is not subject to any limitations of liability in this Master Agreement or in any other document executed in conjunction with this Master Agreement.

b. Except as otherwise set forth in the Indemnification Paragraphs above, the limit of liability shall be as follows:

i. Contractor's liability for any claim, loss or liability arising out of, or connected with the Services provided, and whether based upon default, or other liability such as breach of contract, warranty, negligence, misrepresentation or otherwise, shall in no case exceed direct damages in: (i) an amount equal to two (2) times the charges specified in the Purchase Order for the Services, or parts thereof forming the basis of the Purchasing Entity's claim, (said amount not to exceed a total of twelve (12) months charges payable under the applicable

Purchase Order) or (ii) two million dollars ($2,000,000), whichever is greater.
ii. The Purchasing Entity may retain such monies from any amount due Contractor as may be necessary to satisfy any claim for damages, costs and the like asserted against the Purchasing Entity unless Contractor at the time of the presentation of claim shall demonstrate to the Purchasing Entity's satisfaction that sufficient monies are set aside by the Contractor in the form of a bond or through insurance coverage to cover associated damages and other costs.
iii. Notwithstanding the above, neither the Contractor nor the Purchasing Entity shall be liable for any consequential, indirect or special damages of any kind which may result directly or indirectly from such performance, including, without limitation, damages resulting from loss of use or loss of profit by the Purchasing Entity, the Contractor, or by others.

iv. The limitations of liability in Section 43 will not apply to claims for bodily injury or death as set forth in Section 13, and Section 30 when made applicable under a specific purchase order.

16. Insurance

a. Unless otherwise agreed in a Participating Addendum, Contractor shall, during the term of this Master Agreement, maintain in full force and effect, the insurance described in this section. Contractor shall acquire such insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state and having a rating of A-, Class VII or better, in the most recently published edition of Best's Reports. Failure to buy and maintain the required insurance may result in this Master Agreement's termination or, at a Participating Entity's option, result in termination of its Participating Addendum.

b. Coverage shall be written on an occurrence basis. The minimum acceptable limits shall be as indicated below, with no deductible for each of the following categories:

(1) Commercial General Liability covering premises operations, independent contractors, products and completed operations, blanket contractual liability, personal injury (including death), advertising liability, and property damage, with a limit of not less than $1 million per occurrence/$3 million general aggregate;

(2) CLOUD MINIMUM INSURANCE COVERAGE:

Level of Risk	**Data Breach and Privacy/Cyber Liability including Technology Errors and Omissions** Minimum Insurance Coverage	**Crime Insurance** Minimum Insurance Coverage
Low	$2,000,000	$2,000,000

Moderate	$5,000,000	$5,000,000
High	$10,000,000	$10,000,000

(3) Contractor must comply with any applicable State Workers Compensation or Employers Liability Insurance requirements.

(4) Professional Liability. As applicable, Professional Liability Insurance Policy in the minimum amount of $1,000,000 per occurrence and $1,000,000 in the aggregate, written on an occurrence form that provides coverage for its work undertaken pursuant to each Participating Addendum.

c. Contractor shall pay premiums on all insurance policies. Such policies shall also reference this Master Agreement and shall have a condition that they not be revoked by the insurer until thirty (30) calendar days after notice of intended revocation thereof shall have been given to Purchasing Entity and Participating Entity by the Contractor.

d. Prior to commencement of performance, Contractor shall provide to the Lead State a written endorsement to the Contractor's general liability insurance policy or other documentary evidence acceptable to the Lead State that (1) names the Participating States identified in the Request for Proposal as additional insureds, (2) provides that no material alteration, cancellation, non-renewal, or expiration of the coverage contained in such policy shall have effect unless the named Participating State has been given at least thirty (30) days prior written notice, and (3) provides that the Contractor's liability insurance policy shall be primary, with any liability insurance of any Participating State as secondary and noncontributory. Unless otherwise agreed in any Participating Addendum, the Participating Entity's rights and Contractor's obligations are the same as those specified in the first sentence of this subsection. Before performance of any Purchase Order issued after execution of a Participating Addendum authorizing it, the Contractor shall provide to a Purchasing Entity or Participating Entity who requests it the same information described in this subsection.

e. Contractor shall furnish to the Lead State, Participating Entity, and, on request, the Purchasing Entity copies of certificates of all required insurance within thirty (30) calendar days of the execution of this Master Agreement, the execution of a Participating Addendum, or the Purchase Order's effective date and prior to performing any work. The insurance certificate shall provide the following information: the name and address of the insured; name, address, telephone number and signature of the authorized agent; name of the insurance company (authorized to operate in all states); a description of coverage in detailed standard terminology (including policy period, policy number, limits of liability, exclusions and endorsements); and an acknowledgment of the requirement for notice of cancellation. Copies of renewal certificates of all required insurance shall be furnished within thirty (30) days after any renewal date. These certificates of insurance must expressly indicate compliance with each and every insurance requirement specified in this section. Failure to provide evidence of coverage

may, at sole option of the Lead State, or any Participating Entity, result in this Master Agreement's termination or the termination of any Participating Addendum.

f. Coverage and limits shall not limit Contractor's liability and obligations under this Master Agreement, any Participating Addendum, or any Purchase Order.

17. Laws and Regulations: Any and all Services offered and furnished shall comply fully with all applicable Federal and State laws and regulations.

The federal and state laws, regulations, policies, standards, and guidelines that Contractors doing business with the Participating Entities must be aware of, include, but not limited to: Criminal Justice Information Services (CJIS) Security Policy; Federal Educational Rights and Privacy Act (FERPA); Federal Information Security Management Act (FISMA); National Institute of Technology Standards; Gramm-Leach-Bliley Act (GLB) Act; Health Insurance Portability and Accountability Act (HIPAA); Health Information Technology for Economic and Clinical Health Act (HITECH); IRS Publication 1075; Payment Card Industry Data Security Standard (PCI DSS); Sarbanes-Oxley Act (SOX); Electronic Communications Privacy Act, Stored Communications Act and the PATRIOT Act. The list is intentionally United States-centric, and is not intended to be all-inclusive. Further, since laws, regulations, requirements and industry guidelines change, consulting definitive sources to assure a clear understanding of compliance requirements is critical. Many State Entities have additional program compliance requirements that must be considered in addressing compliance. (e.g., DMV Privacy Act, Public Service Law, etc.).

20. Participants and Scope

a. Contractor may not deliver Services under this Master Agreement until a Participating Addendum acceptable to the Participating Entity and Contractor is executed. The NASPO ValuePoint Master Agreement Terms and Conditions are applicable to any Order by a Participating Entity (and other Purchasing Entities covered by their Participating Addendum), except to the extent altered, modified, supplemented or amended by a Participating Addendum. By way of illustration and not limitation, this authority may apply to unique delivery and invoicing requirements, confidentiality requirements, defaults on Orders, governing law and venue relating to Orders by a Participating Entity, indemnification, and insurance requirements. Statutory or constitutional requirements relating to availability of funds may require specific language in some Participating Addenda in order to comply with applicable law. The expectation is that these alterations, modifications, supplements, or amendments will be addressed in the Participating Addendum or, with the consent of the Purchasing Entity and Contractor, may be included in the ordering document (e.g. purchase order or contract) used by the Purchasing Entity to place the Order.

b. Subject to subsection 20c and a Participating Entity's Participating Addendum, the use of specific NASPO ValuePoint cooperative Master Agreements by state agencies, political subdivisions and other Participating Entities (including cooperatives) authorized

by individual state's statutes to use state contracts is subject to the approval of the respective State Chief Procurement Official.

c. Unless otherwise stipulated in a Participating Entity's Participating Addendum, specific services accessed through the NASPO ValuePoint cooperative Master Agreements for Cloud Services by state executive branch agencies, as required by a Participating Entity's statutes, are subject to the authority and approval of the Participating Entity's Chief Information Officer's Office[3].

d. Obligations under this Master Agreement are limited to those Participating Entities who have signed a Participating Addendum and Purchasing Entities within the scope of those Participating Addenda. Financial obligations of Participating States are limited to the orders placed by the departments or other state agencies and institutions having available funds. Participating States incur no financial obligations on behalf of political subdivisions.

e. NASPO ValuePoint is not a party to the Master Agreement. It is a nonprofit cooperative purchasing organization assisting states in administering the NASPO ValuePoint cooperative purchasing program for state government departments, institutions, agencies and political subdivisions (e.g., colleges, school districts, counties, cities, etc.) for all 50 states, the District of Columbia and the territories of the United States.

f. Participating Addenda shall not be construed to amend the terms of this Master Agreement between the Lead State and Contractor.

g. Participating Entities who are not states may under some circumstances sign their own Participating Addendum, subject to the approval of participation by the Chief Procurement Official of the state where the Participating Entity is located. Coordinate requests for such participation through NASPO ValuePoint. Any permission to participate through execution of a Participating Addendum is not a determination that procurement authority exists in the Participating Entity; they must ensure that they have the requisite procurement authority to execute a Participating Addendum.

h. Resale. Subject to any explicit permission in a Participating Addendum, Purchasing Entities may not resell goods, software, or Services obtained under this Master Agreement. This limitation does not prohibit: payments by employees of a Purchasing Entity as explicitly permitted under this agreement; sales of goods to the general public as surplus property; and fees associated with inventory transactions with other governmental or nonprofit entities under cooperative agreements and consistent with a Purchasing Entity's laws and regulations. Any sale or transfer permitted by this

[3] Chief Information Officer means the individual designated by the Governor with Executive Branch, enterprise-wide responsibility for the leadership and management of information technology resources of a state.

subsection must be consistent with license rights granted for use of intellectual property.

22. Data Access Controls: Contractor will provide access to Purchasing Entity's Data only to those Contractor employees, contractors and subcontractors ("Contractor Staff") who need to access the Data to fulfill Contractor's obligations under this Agreement. Contractor shall not access a Purchasing Entity's user accounts or Data, except on the course of data center operations, response to service or technical issues, as required by the express terms of this Master Agreement, or at a Purchasing Entity's written request.

Contractor may not share a Purchasing Entity's Data with its parent corporation, other affiliates, or any other third party without the Purchasing Entity's express written consent.

Contractor will ensure that, prior to being granted access to the Data, Contractor Staff who perform work under this Agreement have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

23. Operations Management: Contractor shall maintain the administrative, physical, technical, and procedural infrastructure associated with the provision of the Product in a manner that is, at all times during the term of this Master Agreement, at a level equal to or more stringent than those specified in the Solicitation. Contractor must maintain any certifications required under the Solicitation.

24. Public Information: This Master Agreement and all related documents are subject to disclosure pursuant to the Purchasing Entity's public information laws.

26. Records Administration and Audit.

a. The Contractor shall maintain books, records, documents, and other evidence pertaining to this Master Agreement and orders placed by Purchasing Entities under it to the extent and in such detail as shall adequately reflect performance and administration of payments and fees. Contractor shall permit the Lead State, a Participating Entity, a Purchasing Entity, the federal government (including its grant awarding entities and the U.S. Comptroller General), and any other duly authorized agent of a governmental agency, to audit, inspect, examine, copy and/or transcribe Contractor's books, documents, papers and records directly pertinent to this Master Agreement or orders placed by a Purchasing Entity under it for the purpose of making audits, examinations, excerpts, and transcriptions. This right shall survive for a period of six (6) years following termination of this Agreement or final payment for any order placed by a Purchasing Entity against this Agreement, whichever is later, to assure compliance with the terms hereof or to evaluate performance hereunder.

b. Without limiting any other remedy available to any governmental entity, the

Contractor shall reimburse the applicable Lead State, Participating Entity, or Purchasing Entity for any overpayments inconsistent with the terms of the Master Agreement or orders or underpayment of fees found as a result of the examination of the Contractor's records.

c. The rights and obligations herein exist in addition to any quality assurance obligation in the Master Agreement requiring the Contractor to self-audit contract obligations and that permits the Lead State to review compliance with those obligations.

d. The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement and applicable Participating Addendum terms. The purchasing entity may perform this audit or contract with a third party at its discretion and at the purchasing entity's expense.

27. Administrative Fees: The Contractor shall pay to NASPO ValuePoint, or its assignee, a NASPO ValuePoint Administrative Fee of one-quarter of one percent (0.25% or 0.0025) no later than 60 days following the end of each calendar quarter. The NASPO ValuePoint Administrative Fee shall be submitted quarterly and is based on sales of the Services. The NASPO ValuePoint Administrative Fee is not negotiable. This fee is to be included as part of the pricing submitted with proposal.

Additionally, some states may require an additional administrative fee be paid directly to the state on purchases made by Purchasing Entities within that state. For all such requests, the fee level, payment method and schedule for such reports and payments will be incorporated into the Participating Addendum that is made a part of the Master Agreement. The Contractor may adjust the Master Agreement pricing accordingly for purchases made by Purchasing Entities within the jurisdiction of the state. All such agreements shall not affect the NASPO ValuePoint Administrative Fee percentage or the prices paid by the Purchasing Entities outside the jurisdiction of the state requesting the additional fee. The NASPO ValuePoint Administrative Fee shall be based on the gross amount of all sales at the adjusted prices (if any) in Participating Addenda.

28. System Failure or Damage: In the event of system failure or damage caused by Contractor or its Services, the Contractor agrees to use its best efforts to restore or assist in restoring the system to operational capacity.

29. Title to Product: If access to the Product requires an application program interface (API), Contractor shall convey to Purchasing Entity an irrevocable and perpetual license to use the API.

30. Data Privacy: When required by a specific purchase order issued under this Agreement or a Participating Addendum and accepted by the Contractor, the Contractor must comply with all applicable laws related to data privacy and security, including IRS Pub 1075. Prior to entering into a SLA with a Purchasing Entity, the Contractor and

Purchasing Entity must cooperate and hold a meeting to determine the Data Categorization to determine whether the Contractor will hold, store, or process High Risk Data, Moderate Risk Data and Low Risk Data. The Contractor must document the Data Categorization in the SLA or Statement of Work.

31. Warranty: At a minimum the Contractor must warrant the following:

a. Contractor has acquired any and all rights, grants, assignments, conveyances, licenses, permissions, and authorization for the Contractor to provide the Services described in this Master Agreement.

b. Contractor will perform materially as described in this Master Agreement, SLA, Statement of Work, including any performance representations contained in the Contractor's response to the Solicitation by the Lead State.

c. Contractor represents and warrants that the representations contained in its response to the Solicitation by the Lead State.

d. The Contractor will not interfere with a Purchasing Entity's access to and use of the Services it acquires from this Master Agreement.

e. The Services provided by the Contractor are compatible with and will operate successfully with any environment (including web browser and operating system) specified by the Contractor in its response to the Solicitation by the Lead State.

f. The Contractor warrants that the Products it provides under this Master Agreement are free of malware. The Contractor must use industry-leading technology to detect and remove worms, Trojans, rootkits, rogues, dialers, spyware, etc.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

35. Debarment : The Contractor certifies, to the best of its knowledge, that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in this transaction (contract) by any governmental department or agency. This certification represents a recurring certification made at the time any Order is placed under this Master Agreement. If the Contractor cannot certify this statement, attach a written explanation for review by the Lead State.

37. Governing Law and Venue

a. The procurement, evaluation, and award of the Master Agreement shall be governed by and construed in accordance with the laws of the Lead State sponsoring and administering the procurement. The construction and effect of the Master Agreement after award shall be governed by the law of the state serving as Lead State (in most cases also the Lead State). The construction and effect of any Participating Addendum or Order against the Master Agreement shall be governed by and construed in accordance with the laws of the Participating Entity's or Purchasing Entity's State.

b. Unless otherwise specified in the RFP, the venue for any protest, claim, dispute or action relating to the procurement, evaluation, and award is in the Lead State. Venue for any claim, dispute or action concerning the terms of the Master Agreement shall be in the state serving as Lead State. Venue for any claim, dispute, or action concerning any Order placed against the Master Agreement or the effect of a Participating Addendum shall be in the Purchasing Entity's State.

c. If a claim is brought in a federal forum, then it must be brought and adjudicated solely and exclusively within the United States District Court for (in decreasing order of priority): the Lead State for claims relating to the procurement, evaluation, award, or contract performance or administration if the Lead State is a party; the Participating State if a named party; the Participating Entity state if a named party; or the Purchasing Entity state if a named party.

d. This section is also not a waiver by the Participating State of any form of immunity, including but not limited to sovereign immunity and immunity based on the Eleventh Amendment to the Constitution of the United States.

40. Contract Provisions for Orders Utilizing Federal Funds: Pursuant to Appendix II to 2 Code of Federal Regulations (CFR) Part 200, Contract Provisions for Non-Federal Entity Contracts Under Federal Awards, Orders funded with federal funds may have

additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. These federal requirements may be proposed by Participating Entities in Participating Addenda and Purchasing Entities for incorporation in Orders placed under this master agreement.

42. NASPO ValuePoint Summary and Detailed Usage Reports: In addition to other reports that may be required by this solicitation, the Contractor shall provide the following NASPO ValuePoint reports.

a. Summary Sales Data. The Contractor shall submit quarterly sales reports directly to NASPO ValuePoint using the NASPO ValuePoint Quarterly Sales/Administrative Fee Reporting Tool found at http://www.naspo.org/WNCPO/Calculator.aspx. Any/all sales made under the contract shall be reported as cumulative totals by state. Even if Contractor experiences zero sales during a calendar quarter, a report is still required. Reports shall be due no later than 30 day following the end of the calendar quarter (as specified in the reporting tool).

b. Detailed Sales Data. Contractor shall also report detailed sales data by: (1) state; (2) entity/customer type, e.g. local government, higher education, K12, non-profit; (3) Purchasing Entity name; (4) Purchasing Entity bill-to and ship-to locations; (4) Purchasing Entity and Contractor Purchase Order identifier/number(s); (5) Purchase Order Type (e.g. sales order, credit, return, upgrade, determined by industry practices); (6) Purchase Order date; (7) Ship Date; (8) and line item description, including product number if used. The report shall be submitted in any form required by the solicitation. Reports are due on a quarterly basis and must be received by the Lead State and NASPO ValuePoint Cooperative Development Team no later than thirty (30) days after the end of the reporting period. Reports shall be delivered to the Lead State and to the NASPO ValuePoint Cooperative Development Team electronically through a designated portal, email, CD-Rom, flash drive or other method as determined by the Lead State and NASPO ValuePoint. Detailed sales data reports shall include sales information for all sales under Participating Addenda executed under this Master Agreement. The format for the detailed sales data report is in shown in Attachment F.

c. Reportable sales for the summary sales data report and detailed sales data report includes sales to employees for personal use where authorized by the solicitation and the Participating Addendum. Report data for employees should be limited to ONLY the state and entity they are participating under the authority of (state and agency, city, county, school district, etc.) and the amount of sales. No personal identification numbers, e.g. names, addresses, social security numbers or any other numerical identifier, may be submitted with any report.

d. Contractor shall provide the NASPO ValuePoint Cooperative Development Coordinator with an executive summary each quarter that includes, at a minimum, a list

of states with an active Participating Addendum, states that Contractor is in negotiations with and any PA roll out or implementation activities and issues. NASPO ValuePoint Cooperative Development Coordinator and Contractor will determine the format and content of the executive summary. The executive summary is due 30 days after the conclusion of each calendar quarter.

e. Timely submission of these reports is a material requirement of the Master Agreement. The recipient of the reports shall have exclusive ownership of the media containing the reports. The Lead State and NASPO ValuePoint shall have a perpetual, irrevocable, non-exclusive, royalty free, transferable right to display, modify, copy, and otherwise use reports, data and information provided under this section.

f. If requested by a Participating Entity, the Contractor must provide detailed sales data within the Participating State.

43. Entire Agreement: This Master Agreement, along with any attachment, contains the entire understanding of the parties hereto with respect to the Master Agreement unless a term is modified in a Participating Addendum with a Participating Entity. No click-through, or other end user terms and conditions or agreements required by the Contractor ("Additional Terms") provided with any Services hereunder shall be binding on Participating Entities or Purchasing Entities, even if use of such Services requires an affirmative "acceptance" of those Additional Terms before access is permitted.

Exhibit 1 to the Master Agreement: Software-as-a-Service

1. **Data Ownership:** The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. **Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

    a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

    b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

    c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

    d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

    e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. **Data Location:** The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. **Security Incident or Data Breach Notification:**

   a. Incident Response: Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the Purchasing Entity should be handled on an urgent as needed basis, as part of Contractor's communication and mitigation processes as mutually agreed upon, defined by law or contained in the Master Agreement.

   b. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

   c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. **Personal Data Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

   a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

   b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 48 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a Data Breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3)

document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

6. **Notification of Legal Requests**: If legally permissible, the Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law. .

7. **Termination and Suspension of Service**:

   a. In the event of a termination of the Master Agreement or applicable Participating Addendum, the Contractor shall implement an orderly return of purchasing entity's data in a CSV or another mutually agreeable format at a time agreed to by the parties or allow the Purchasing Entity to extract it's data and the subsequent secure disposal of purchasing entity's data.

   b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

   c. In the event of termination of any services or agreement in entirety, the Contractor shall not take any action to intentionally erase purchasing entity's data for a period of:

   - 10 days after the effective date of termination, if the termination is in accordance with the contract period
   - 30 days after the effective date of termination, if the termination is for convenience
   - • 60 days after the effective date of termination, if the termination is for cause

   After such period, the Contractor shall have no obligation to maintain or provide any purchasing entity's data and shall thereafter, unless legally prohibited, delete all purchasing entity's data in its systems or otherwise in its possession or under its control.

   d. The purchasing entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

   e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD,

backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. **Background Checks:** Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. **Access to Security Logs and Reports:** The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA agreed to by both the Contractor and the Purchasing Entity. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all public jurisdiction files related to this Master Agreement and applicable Participating Addendum.

10. **Contract Audit:** The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. **Data Center Audit:** The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. **Change Control and Advance Notice:** The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. **Security:** As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. **Non-disclosure and Separation of Duties:** The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. **Import and Export of Data:** The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. **Responsibilities and Uptime Guarantee**: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. **Subcontractor Disclosure**: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. **Right to Remove Individuals:** The Purchasing Entity shall have the right at any time to require that the Contractor remove from interaction with Purchasing Entity any Contractor representative who the Purchasing Entity believes is detrimental to its working relationship with the Contractor. The Purchasing Entity shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the Purchasing Entity signifies that a potential security violation exists with respect to the request, the Contractor shall immediately

remove such individual. The Contractor shall not assign the person to any aspect of the Master Agreement or future work orders without the Purchasing Entity's consent.

19. **Business Continuity and Disaster Recovery:** The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

20. **Compliance with Accessibility Standards**: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973, or any other state laws or administrative regulations identified by the Participating Entity.

21. **Web Services:** The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

22. **Encryption of Data at Rest:** The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data, unless the Purchasing Entity approves in writing for the storage of Personal Data on a Contractor portable device in order to accomplish work as defined in the statement of work.

23. **Subscription Terms**: Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for SaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 2 to the Master Agreement: Platform-as-a-Service

1. **Data Ownership:** The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. **Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

    a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

    b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

    c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

    d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

    e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. **Data Location:** The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. **Security Incident or Data Breach Notification:** The Contractor shall inform the Purchasing Entity of any security incident or data breach within the possession and control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

    a. Incident Response: The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Master Agreement, Participating Addendum, or SLA. Discussing security incidents with the Purchasing Entity should be handled on an urgent as-needed basis, as part of Contractor's communication and mitigation processes as mutually agreed, defined by law or contained in the Master Agreement, Participating Addendum, or SLA.

    b. Security Incident Reporting Requirements: Unless otherwise stipulated, the Contractor shall immediately report a security incident related to its service under the Master Agreement, Participating Addendum, or SLA to the appropriate Purchasing Entity.

    c. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any Purchasing Entity data that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate Purchasing Entity within 48 hours or sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner

5. **Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor.

    a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

6. **Notification of Legal Requests**: If legally permissible, the Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law.

7. **Termination and Suspension of Service**:

   a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

   b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

   c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

   d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

   e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of

Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. **Background Checks:**

   a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

   b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

   c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. **Access to Security Logs and Reports:**

   a. The Contractor shall provide reports on a schedule specified in the SLA to the Purchasing Entity in a format as specified in the SLA and agreed to by both the Contractor and the Purchasing Entity. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all Purchasing Entity files related to the Master Agreement, Participating Addendum, or SLA.

   b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. **Contract Audit:** The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.

11. **Data Center Audit**: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide an unredacted version of the audit report upon

request to a Purchasing Entity. The Contractor may remove its proprietary information from the unredacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

12. **Change Control and Advance Notice:** The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. **Security:** As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. **Non-disclosure and Separation of Duties:** The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. **Import and Export of Data:** The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.
16. **Responsibilities and Uptime Guarantee**: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.

17. **Subcontractor Disclosure**: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. **Business Continuity and Disaster Recovery:** The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. **Compliance with Accessibility Standards**: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973 or any other state laws or administrative regulations identified by the Participating Entity..

20. **Web Services:** The Contractor shall use Web services exclusively to interface with the Purchasing Entity's data in near real time.

21. **Encryption of Data at Rest:** The Contractor shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data as identified in the SLA, unless the Contractor presents a justifiable position that is approved by the Purchasing Entity that Personal Data, is required to be stored on a Contractor portable device in order to accomplish work as defined in the scope of work.

22. **Subscription Terms:** Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for PaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement.

Exhibit 3 to the Master Agreement: Infrastructure-as-a-Service

1. **Data Ownership:** The Purchasing Entity will own all right, title and interest in its data that is related to the Services provided by this Master Agreement. The Contractor shall not access Purchasing Entity user accounts or Purchasing Entity data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Master Agreement, Participating Addendum, SLA, and/or other contract documents, or (4) at the Purchasing Entity's written request.

Contractor shall not collect, access, or use user-specific Purchasing Entity Data except as strictly necessary to provide Service to the Purchasing Entity. No information regarding a Purchasing Entity's use of the Service may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this Master Agreement.

2. **Data Protection:** Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of Purchasing Entity information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Purchasing Entity information and comply with the following conditions:

    a. The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Data and Non-Public Data of similar kind.

    b. All data obtained by the Contractor in the performance of the Master Agreement shall become and remain the property of the Purchasing Entity.

    c. All Personal Data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the Personal Data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of the Master Agreement.

    d. Unless otherwise stipulated, the Contractor shall encrypt all Non-Public Data at rest and in transit. The Purchasing Entity shall identify data it deems as Non-Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the SLA.

    e. At no time shall any data or processes — that either belong to or are intended for the use of a Purchasing Entity or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the Purchasing Entity.

f. The Contractor shall not use any information collected in connection with the Services issued from this Master Agreement for any purpose other than fulfilling the Services.

3. **Data Location:** The Contractor shall provide its services to the Purchasing Entity and its end users solely from data centers in the U.S. Storage of Purchasing Entity data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store Purchasing Entity data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor shall permit its personnel and contractors to access Purchasing Entity data remotely only as required to provide technical support. The Contractor may provide technical user support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in a Participating Addendum.

4. **Security Incident or Data Breach Notification:** The Contractor shall inform the Purchasing Entity of any security incident or data breach related to Purchasing Entity's Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA. Such notice shall include, to the best of Contractor's knowledge at that time, the persons affected, their identities, and the Confidential Information and Data disclosed, or shall include if this information is unknown.

   a. Security Incident Reporting Requirements: The Contractor shall report a security incident to the Purchasing Entity identified contact immediately as soon as possible or promptly without out reasonable delay, or as defined in the SLA.

   b. Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any purchasing entity's content that is subject to applicable data breach notification law, the Contractor shall (1) as soon as possible or promptly without out reasonable delay notify the Purchasing Entity, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

5. **Breach Responsibilities:** This section only applies when a Data Breach occurs with respect to Personal Data within the possession or control of the Contractor and related to the service provided under the Master Agreement, Participating Addendum, or SLA.

   a. The Contractor, unless stipulated otherwise, shall immediately notify the appropriate Purchasing Entity identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

   b. The Contractor, unless stipulated otherwise, shall promptly notify the appropriate Purchasing Entity identified contact within 48 hours or sooner by telephone, unless shorter time is required by applicable law, if it has confirmed that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the Purchasing Entity as reasonably requested by the Purchasing Entity to investigate and resolve the Data Breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the Data Breach, including any post-incident

review of events and actions taken to make changes in business practices in providing the services, if necessary.

6. **Notification of Legal Requests:** If legally permissible, the Contractor shall contact the Purchasing Entity upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the Purchasing Entity's data under the Master Agreement, or which in any way might reasonably require access to the data of the Purchasing Entity. The Contractor shall not respond to subpoenas, service of process and other legal requests related to the Purchasing Entity without first notifying and obtaining the approval of the Purchasing Entity, unless prohibited by law.

7. **Termination and Suspension of Service:**

   a. In the event of an early termination of the Master Agreement, Participating or SLA, Contractor shall allow for the Purchasing Entity to retrieve its digital content and provide for the subsequent secure disposal of the Purchasing Entity's digital content.

   b. During any period of service suspension, the Contractor shall not take any action to intentionally erase or otherwise dispose of any of the Purchasing Entity's data.

   c. In the event of early termination of any Services or agreement in entirety, the Contractor shall not take any action to intentionally erase any Purchasing Entity's data for a period of 1) 45 days after the effective date of termination, if the termination is for convenience; or 2) 60 days after the effective date of termination, if the termination is for cause. After such day period, the Contractor shall have no obligation to maintain or provide any Purchasing Entity data and shall thereafter, unless legally prohibited, delete all Purchasing Entity data in its systems or otherwise in its possession or under its control. In the event of either termination for cause, the Contractor will impose no fees for access and retrieval of digital content to the Purchasing Entity.

   d. The Purchasing Entity shall be entitled to any post termination assistance generally made available with respect to the services, unless a unique data retrieval arrangement has been established as part of an SLA.

   e. Upon termination of the Services or the Agreement in its entirety, Contractor shall securely dispose of all Purchasing Entity's data in all of its forms, such as disk, CD/ DVD, backup tape and paper, unless stipulated otherwise by the Purchasing Entity. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST)-approved methods. Certificates of destruction shall be provided to the Purchasing Entity.

8. **Background Checks:**

   a. Upon the request of the Purchasing Entity, the Contractor shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Master Agreement who have been convicted of any crime of dishonesty,

including but not limited to criminal fraud, or otherwise convicted of any felony or misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Contractor shall promote and maintain an awareness of the importance of securing the Purchasing Entity's information among the Contractor's employees and agents.

b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

c. If any of the stated personnel providing services under a Participating Addendum is not acceptable to the Purchasing Entity in its sole opinion as a result of the background or criminal history investigation, the Purchasing Entity, in its' sole option shall have the right to either (1) request immediate replacement of the person, or (2) immediately terminate the Participating Addendum and any related service agreement.

9. **Access to Security Logs and Reports:**

   a. The Contractor shall provide reports on a schedule specified in the SLA to the Contractor directly related to the infrastructure that the Contractor controls upon which the Purchasing Entity's account resides. Unless otherwise agreed to in the SLA, the Contractor shall provide the public jurisdiction a history or all API calls for the Purchasing Entity account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Contractor. The report will be sufficient to enable the Purchasing Entity to perform security analysis, resource change tracking and compliance auditing

   b. The Contractor and the Purchasing Entity recognize that security responsibilities are shared. The Contractor is responsible for providing a secure infrastructure. The Purchasing Entity is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SLA.

10. **Contract Audit:** The Contractor shall allow the Purchasing Entity to audit conformance to the Master Agreement terms. The Purchasing Entity may perform this audit or contract with a third party at its discretion and at the Purchasing Entity's expense.
11. **Data Center Audit:** The Contractor shall perform an independent audit of its data centers at least annually and at its own expense, and provide an unredacted version of the audit report upon request. The Contractor may remove its proprietary information from the unredacted version. For example, a Service Organization Control (SOC) 2 audit report would be sufficient.

12. **Change Control and Advance Notice:** The Contractor shall give a minimum forty eight (48) hour advance notice (or as determined by a Purchasing Entity and included in the SLA) to the Purchasing Entity of any upgrades (e.g., major upgrades, minor upgrades, system changes) that

may impact service availability and performance. A major upgrade is a replacement of hardware, software or firmware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number.

Contractor will make updates and upgrades available to Purchasing Entity at no additional costs when Contractor makes such updates and upgrades generally available to its users.

No update, upgrade or other charge to the Service may decrease the Service's functionality, adversely affect Purchasing Entity's use of or access to the Service, or increase the cost of the Service to the Purchasing Entity.

Contractor will notify the Purchasing Entity at least sixty (60) days in advance prior to any major update or upgrade.

13. **Security:** As requested by a Purchasing Entity, the Contractor shall disclose its non-proprietary system security plans (SSP) or security processes and technical limitations to the Purchasing Entity such that adequate protection and flexibility can be attained between the Purchasing Entity and the Contractor. For example: virus checking and port sniffing — the Purchasing Entity and the Contractor shall understand each other's roles and responsibilities.

14. **Non-disclosure and Separation of Duties:** The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of Purchasing Entity data to that which is absolutely necessary to perform job duties.

15. **Import and Export of Data:** The Purchasing Entity shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor at any time during the term of Contractor's contract with the Purchasing Entity. This includes the ability for the Purchasing Entity to import or export data to/from other Contractors. Contractor shall specify if Purchasing Entity is required to provide its' own tools for this purpose, including the optional purchase of Contractors tools if Contractors applications are not able to provide this functionality directly.

16. **Responsibilities and Uptime Guarantee**: The Contractor shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the Contractor. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and provide service to customers as defined in the SLA.
17. **Subcontractor Disclosure**: Contractor shall identify all of its strategic business partners related to services provided under this Master Agreement, including but not limited to all subcontractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

18. **Business Continuity and Disaster Recovery:** The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the Purchasing Entity's recovery time objective (RTO) of XXX hours/days is met. (XXX hour/days shall be provided to Contractor by the Purchasing Entity.) Contractor must work with the Purchasing Entity to perform an annual Disaster Recovery test and take action to correct any issues detected during the test in a time frame mutually agreed between the Contractor and the Purchasing Entity.

19. **Subscription Terms:** Contractor grants to a Purchasing Entity a license to: (i) access and use the Service for its business purposes; (ii) for IaaS, use underlying software as embodied or used in the Service; and (iii) view, copy, upload and download (where applicable), and use Contractor's documentation.

No Contractor terms, including standard click through license or website terms or use of privacy policy, shall apply to Purchasing Entities unless such terms are included in this Master Agreement via amendment.

Attachment B – Identification of Service Models Matrix

Offerors must complete the following form to identify the service models your firm offers under this RFP. You may provide a list of the different SaaS, IaaS, and/or PaaS services that you offer, including the Categorization of Risk that you have the ability to store and secure. This document is to provide purchasing entities and eligible users a quick snap shot of the cloud solutions your firm provides.

Service Model:	Low Risk Data	Moderate Risk Data	High Risk Data	Deployment Models Offered:
Saas	Varies by Manufacturer Offer	Varies by Manufacturer Offer	Varies by Manufacturer Offer	AODocs, CA Technologies, DocuSign, FireEye, Google, QTS, Salesforce, SAP, ServiceNow, Virtru, VMware
IaaS	Varies by Manufacturer Offer	Varies by Manufacturer Offer	Varies by Manufacturer Offer	FireEye, Google, QTS, Virtustream, VMware
PaaS	Varies by Manufacturer Offer	Varies by Manufacturer Offer	Varies by Manufacturer Offer	Google, QTS, Salesforce, SAP, ServiceNow, Virtustream

Carahsoft's solution providers each have different forms and procedures for providing solutions and services with varying levels of data management for each solution. Please see Carahsoft's Technical Response for additional information regarding risk data management of low, moderate, and high risk data.

Attachment C – Cost Schedu

Solicitation Number CH16012
NASPO ValuePoint Cloud Solutions RF

Cloud Solutions By Category. Specify ***Discount Percent %*** C
each category. Highest discount will apply for products referenc
multiple categories. Provide a detailed product offering for each

Software as a Service Di

Infrastructure as a Service Di

Platform as a Services Di

Value Added Services Di

Additional Value Added Services:

Maintenance Services

Onsite Hourly Ra
Remote Hourly R

Professional Services

- **Deployment Services**
  Onsite Hourly Ra
  Remote Hourly R
- **Consulting/Advisory Services**
  Onsite Hourly Ra
  Remote Hourly R
- **Architectural Design Services**
  Onsite Hourly Ra
  Remote Hourly R
- **Statement of Work Services**
  Onsite Hourly Ra
  Remote Hourly R

Partner Services

Onsite Hourly Ra
Remote Hourly R

Training Deployment Services

Onsite Hourly R
Online Hourly R

Attachment C – Cost Schedule

Solicitation Number CH16012
NASPO ValuePoint Cloud Solutions RFP

Cloud Solutions By Category. Specify ***Discount Percent %*** Offered for products in each category. Highest discount will apply for products referenced in detail listings for multiple categories. Provide a detailed product offering for each category.

Software as a Service	**Discount % 0-21.60**
Infrastructure as a Service	**Discount % 0-10**
Platform as a Services	**Discount % 0-11**
Value Added Services	**Discount % 0-13**

Additional Value Added Services:

Maintenance Services	**Onsite Hourly Rate $ 250** **Remote Hourly Rate $ 175**
Professional Services	
• **Deployment Services**	**Onsite Hourly Rate $ 350** **Remote Hourly Rate $ 275**
• **Consulting/Advisory Services**	**Onsite Hourly Rate $ 300** **Remote Hourly Rate $ 225**
• **Architectural Design Services**	**Onsite Hourly Rate $ 300** **Remote Hourly Rate $ 225**
• **Statement of Work Services**	**Onsite Hourly Rate $ 250** **Remote Hourly Rate $ 175**
Partner Services	**Onsite Hourly Rate $ 250** **Remote Hourly Rate $ 175**
Training Deployment Services	**Onsite Hourly Rate $ 250** **Online Hourly Rate $ 175**

Manufacturer	Description	Vendor Part No	List Price	GSA Price
AODocs	AODOCS-TEAM-FOLDERS-12MO	AODocs Team Folders: 12 m	$ 36.00	$ 35.19
AODocs	AODOCS-DOCUMENT-MANAGEMENT-12MO	AODocs Document Manager	$ 72.00	$ 70.38
AODocs	AODOCS-TEAM-FOLDERS-1MO	AODocs Team Folders: 1 mo	$ 3.00	$ 2.93
AODocs	AODOCS-DOCUMENT-MANAGEMENT-1MO	AODocs Document Manager	$ 6.00	$ 5.87
AODocs	AODOCS-RETENTION-12MO	AODocs Retention Managem	$ 30.00	$ 29.33
AODocs	AODOCS-EMAIL-CONNECTOR-12MO	AODocs Email Connector 12	$ 30.00	$ 29.33
AODocs	AODOCS-MIGRATION-TOOL-12MO	AODocs Migration Tool 12 m	$ 20,000.00	$ 19,550.00
CA Technologies	CA Agile Central Enterprise Edition	ENTP-1YR-STD	$ 420.00	$ 403.20
CA Technologies	CA Flowdock Enterprise Add-on	FDE-SUB-OD-ADD	$ 108.00	$ 103.68
CA Technologies	CA Flowdock Enterprise Standalone	FDEP-SUB-OD	$ 108.00	$ 103.68
CA Technologies	CA Agile Central HP Integration	INT-SUB-OD-HP	$ 60.00	$ 57.60
CA Technologies	CA Agile Central IBM Integration	INT-SUB-OD-IBM	$ 60.00	$ 57.60
CA Technologies	CA Agile Central Quality Manager Module	QUAL-1YR-STD	$ 120.00	$ 115.20
CA Technologies	CA Agile Central Advanced Security and Administration	RAS-SUB-OD	$ 60.00	$ 57.60
CA Technologies	CA Idea Manager Fee	RIM-SUB-FEE	$ 1,000.00	$ 960.00
CA Technologies	CA Idea Manager	RIM-SUB-OD	$ 5,000.00	$ 4,800.00
CA Technologies	CA Portfolio Manager	RPM2-SUB-OD	$ 120.00	$ 115.20
CA Technologies	CA Quality Manager Product	RQMP-1YR-STD	$ 420.00	$ 403.20
CA Technologies	CA Time Tracker Module	RTT-1YR-STD	$ 120.00	$ 115.20
CA Technologies	CA Agile Central Unlimited Edition	UE-1YR-STD	$ 588.00	$ 564.48
CA Technologies	CA API Management SaaS Portal -Partner	APIMPR990	$ 30,000.00	$ 23,520.00
CA Technologies	CA API Management SaaS Gateway add-on -Partner	APIMSA990	$ 21,600.00	$ 16,934.40
CA Technologies	CA API Management SaaS Partner	APIMSP990	$ 78,000.00	$ 61,152.00
CA Technologies	CA App Synthetic Monitor 5 Minute Adv 10GB 10 Pack	APCA10990	$ 4,200.00	$ 4,200.00
CA Technologies	CA App Synthetic Monitor 5 Minute Adv 20GB 10 Pack	APCA20990	$ 6,360.00	$ 6,360.00
CA Technologies	CA App Synthetic Monitor 5 Minute Adv 40GB 10 Pack	APCA40990	$ 10,800.00	$ 10,800.00
CA Technologies	CA App Synthetic Monitor 1 Minute Basic 10 Pack	APCB10990	$ 7,560.00	$ 7,560.00
CA Technologies	CA App Synthetic Monitor 5 Minute Basic 50 Pack	APCB50990	$ 5,520.00	$ 5,520.00
CA Technologies	CA App Synthetic Monitor 10 Min RBM 20GB 1Pk	APCR20990	$ 4,080.00	$ 4,080.00
CA Technologies	CA App Synthetic Monitor 5 Min RBM 40GB 1Pk	APCR40990	$ 6,360.00	$ 6,360.00
CA Technologies	CA App Synthetic Monitor 15 Minute Adv 5GB 10 Pack	APMCA5990	$ 4,200.00	$ 4,200.00
CA Technologies	CA App Synthetic Monitor Adv Option	APMCMA990	$ 67,200.00	$ 67,200.00
CA Technologies	CA App Synthetic Monitor Intermediate Option	APMCMI990	$ 42,000.00	$ 42,000.00
CA Technologies	CA App Synthetic Monitor Intermediate Option	APMCMI990	$ 42,000.00	$ 42,000.00
CA Technologies	CA App Synthetic Monitor 5 Minute Basic Monitor 10 pack	NCUBMF990	$ 1,740.00	$ 1,740.00
CA Technologies	CA App Synthetic Monitor 5 Minute Basic Monitor 3 pack	NCUBMT990	$ 540.00	$ 540.00
CA Technologies	CA App Synthetic Monitor 5 Minute Advanced Monitor (10 GB) 1	NCUEAF990	$ 708.00	$ 708.00
CA Technologies	CA App Synthetic Monitor 1 Minute Basic Monitor 1	NCUEBM990	$ 1,080.00	$ 1,080.00
CA Technologies	CA App Synthetic Monitor 5 Minute Basic Monitor 25 pack	NCUEBP990	$ 3,900.00	$ 3,900.00
CA Technologies	CA App Synthetic Monitor 15 Minute Advanced Monitor (5 GB) 1	NCUEMA990	$ 348.00	$ 348.00
CA Technologies	CA App Synthetic Monitor 5 Minute Basic Monitor 1	NCUEMM990	$ 216.00	$ 216.00
CA Technologies	CA App Synthetic Monitor 10 Minute Basic Monitor 10 pack	NCUEMP990	$ 936.00	$ 936.00
CA Technologies	CA App Synthetic Monitor 10 Minute Basic Monitor 1	NCUETB990	$ 108.00	$ 108.00
CA Technologies	CA App Synthetic Monitor 10 Minute Basic Monitor 3 pack	NCUETP990	$ 288.00	$ 288.00
CA Technologies	CA App Synthetic Monitor 5 Minute Advanced Monitor (10 GB) 10 pack	NCUMAM990	$ 6,000.00	$ 6,000.00
CA Technologies	CA App Synthetic Monitor Corporate Bundle	NCUMCB990	$ 5,940.00	$ 5,940.00
CA Technologies	CA App Synthetic Monitor Enterprise Bundle	NCUMEB990	$ 18,000.00	$ 18,000.00

CA Technologies	CA App Synthetic Monitor 5 Minute Advanced Monitor (40 GB) 1	NCUMFA990	$ 1,800.00	$ 1,800.00
CA Technologies	CA App Synthetic Monitor 5 Minute Advanced Monitor (20 GB) 1	NCUMMA990	$ 1,080.00	$ 1,080.00
CA Technologies	CA App Synthetic Monitor Multi-Site Bundle	NCUMSB990	$ 1,188.00	$ 1,188.00
CA Technologies	CA Mobile App Analytics for Business Users SAAS	MBAABS565	$ 13.20	$ 11.22
CA Technologies	CA Mobile App Analytics for Consumer Users SAAS	MBAACS565	$ 0.48	$ 0.41
CA Technologies	*CA PPM SAAS Full Function User	CODSFF991	$ 720.00	$ 564.48
CA Technologies	*CA PPM SAAS Restricted User	CODSRU991	$ 360.00	$ 282.24
CA Technologies	*CA PPM SAAS VIEW ONLY USER (1000 User pack)	CODSVU991	$ 5,000.00	$ 3,920.03
CA Technologies	*CA PPM SAAS Sandbox Small Environment	CODSBX991	$ 30,000.00	$ 23,520.00
CA Technologies	*CA PPM SAAS Sandbox Near Production Environment	CODSB2991	$ 48,000.00	$ 37,632.00
DocuSign	3rd Party Solutions - Conga composer/Per Transaction - ADD ON	DS-3PS-CCT	$ 2.00	$ 1.95
DocuSign	3rd Party Solutions - Conga composer/Seat Per Year - ADD ON	DS-3PS-CCY	$ 180.00	$ 175.92
DocuSign	3rd Party Solutions - Dynamic Documents - ADD ON	DS-3PS-DD	$ 180.00	$ 175.92
DocuSign	3rd Party Solutions - eOriginal/Managed Transaction - ADD ON	DS-3PS-EMT	$ 1.00	$ 0.98
DocuSign	3rd Party Solutions - eOriginal/Transferred Transaction - ADD ON	DS-3PS-ETT	$ 5.00	$ 4.89
DocuSign	Additional - Fax Services - ADD ON	DS-AFS	$ 0.10	$ 0.10
DocuSign	DocuSign Authentication Option - ID Check - ADD ON	DS-AOID	$ 2.50	$ 2.44
DocuSign	DocuSign Authentication Option - Phone - ADD ON	DS-AOPhone	$ 0.75	$ 0.73
DocuSign	DocuSign Authentication Option - SMS - ADD ON	DS-AOSMS	$ 0.20	$ 0.20
DocuSign	Additonal - Retrieve - ADD ON	DS-AR	$ 5,000.00	$ 4,886.65
DocuSign	Customer Success Architects - Full time - SERVICE	DS-CSAF	$ 28,000.00	$ 27,365.24
DocuSign	Customer Success Architects - Half time - SERVICE	DS-CSAH	$ 18,000.00	$ 17,591.94
DocuSign	Customer Success Architects - Quarter time - SERVICE	DS-CSAQ	$ 10,000.00	$ 9,773.30
DocuSign	Docusign Digital Signatures - Express - ADD ON	DS-DSE	$ 1.50	$ 1.47
DocuSign	Docusign Digital Signatures - OpenTrust/Seat Per Year - ADD ON	DS-DSOTS	$ 144.00	$ 140.74
DocuSign	Docusign Digital Signatures - OpenTrust/Per Transaction - ADD ON	DS-DSOTT	$ 1.75	$ 1.71
DocuSign	Docusign Digital Signatures - SAFE Bio-Pharma - ADD ON	DS-DSSBP	$ 1.50	$ 1.47
DocuSign	Follow Up - TRAINING	DS-FUP	$ 295.00	$ 288.31
DocuSign	Microsoft Office 365 Quickstart Onboarding - TRAINING	DS-MO3QO	$ 295.00	$ 288.31
DocuSign	DocuSign for Office 365 Edition	DS-O3E	$ 120.00	$ 117.28
DocuSign	Powerforms - TRAINING	DS-PF	$ 295.00	$ 288.31
DocuSign	Professional Services - API Certification - SERVICE	DS-PS-APIC	$ 1,000.00	$ 977.33
DocuSign	Professional Services - Consulting - SERVICE	DS-PS-C	$ 295.00	$ 288.31
DocuSign	Professional Services - Department Strategic Assessment - SERVICE	DS-PS-DSA	$ 17,000.00	$ 16,614.61
DocuSign	Professional Services - Fast start API - SERVICE	DS-PS-FS	$ 18,000.00	$ 17,591.94
DocuSign	Professional Services - Full service API - SERVICE	DS-PS-FSAPI	$ 45,000.00	$ 43,979.85
DocuSign	Professional Services - Full service web console - SERVICE	DS-PS-FSERVWC	$ 30,000.00	$ 29,319.90
DocuSign	Professional Services - Full service Salesforce.com - SERVICE	DS-PS-FSSF	$ 35,000.00	$ 34,206.55
DocuSign	Professional Services - ProServ /Single Sign On - SERVICE	DS-PS-PSS	$ 2,500.00	$ 2,443.32
DocuSign	Professional Services - Q&A Bundle - SERVICE	DS-PS-QAB	$ 2,500.00	$ 2,443.32
DocuSign	Retrieve Training - TRAINING	DS-RT	$ 295.00	$ 288.31
DocuSign	Salesforce Admin - TRAINING	DS-SA	$ 295.00	$ 288.31
DocuSign	DocuSign System Automated Premium Edition	DS-SAPE	$ 5.00	$ 4.89
DocuSign	DocuSign for Salesforce Enterprise Editon	DS-SEE	$ 550.00	$ 537.53
DocuSign	Salesforce Installation & Configuration - TRAINING	DS-SIC	$ 295.00	$ 288.31
DocuSign	Web Console Admin - TRAINING	DS-WCA	$ 295.00	$ 288.31
DocuSign	Web Console Overview - TRAINING	DS-WCO	$ 295.00	$ 288.31
DocuSign	Web Console Template Setup - TRAINING	DS-WCTS	$ 295.00	$ 288.31
DocuSign	DocuSign Enterprise Edition Enterprise Premier (Support)	DS-EE-EP	$ 121.00	$ 118.26

DocuSign	DocuSign for Salesforce Enterprise Edition Enterprise Premier (Support)- Seats- USD- Annual	12000121S-EP	$ 121.00	$ 118.26
DocuSign	DocuSign for Salesforce Enterprise Editon Enterprise Premier (Support)	DS-SEE-EP	$ 121.00	$ 118.26
DocuSign	DocuSign Enterprise Edition Enterprise Premier (Support)- Seats-USD- Annual	12000111S-EP	$ 105.60	$ 103.21
DocuSign	DocuSign for Salesforce Enterprise Edition Premier (Support)- Seats- USD- Annual	12000121S-P	$ 82.50	$ 80.63
DocuSign	DocuSign for Salesforce Enterprise Editon Premier (Support)	DS-SEE-P	$ 82.50	$ 80.63
DocuSign	DocuSign for Salesforce Business Edition Enterprise Premier (Support)	12000321S-EP	$ 79.20	$ 77.40
DocuSign	DocuSign Enterprise Edition Premier (Support)- Seats-USD- Annual	12000111S-P	$ 72.00	$ 70.37
DocuSign	DocuSign for Salesforce Business Edition Premier (Support)	12000321S-P	$ 54.00	$ 52.78
DocuSign	DocuSign Enterprise Edition Premier (Support)	DS-EE-P	$ 54.00	$ 52.78
DocuSign	DocuSign for Salesforce Dynamic Documents Enterprise Premier (Support)- Seats- USD- Annual	12000232S-EP	$ 39.60	$ 38.70
DocuSign	DocuSign for Salesforce Dynamic Documents Premier (Support)- Seats- USD- Annual	12000232S-P	$ 27.00	$ 26.39
DocuSign	DocuSign for Office 365 Edition Enterprise Premier (Support)- Seat per Year	DS-O3E-EP	$ 26.40	$ 25.80
DocuSign	DocuSign for Office 365 Edition Premier (Support)- Seat per Year	DS-O3E-P	$ 18.00	$ 17.59
DocuSign	DocuSign Business Edition - SMS	200013	$ 2.00	$ 1.96
DocuSign	DocuSign for Salesforce Enterprise Edition Enterprise Premier (Support)- Envelopes- USD- Annual	12000121E-EP	$ 1.54	$ 1.52
DocuSign	DocuSign Business Edition ($/seat annually) 5+ seats	DS-BE	$ 360.00	$ 351.84
DocuSign	DocuSign for Salesforce Business Package ($/seat annually) 5+ seats	DS-SBP	$ 360.00	$ 351.84
DocuSign	DocuSign for Salesforce Enterprise Package ($/seat annually) 5+ seats	DS-SEP	$ 540.00	$ 527.76
DocuSign	DocuSign System Automated Standard Edition ($/envelope) 500 envelope allowance minimum	DS-SASE	$ 3.00	$ 2.93
DocuSign	DocuSign Enterprise Developer ($/app/year) $299/app/month	DS-ED	$ 3,588.00	$ 3,506.66
DocuSign	DocuSign Individual Developer ($/app/year) $9/app/month	DS-ID	$ 108.00	$ 105.55
DocuSign	DocuSign - Additional-Security Appliance - 40% uplift to annual Edition pricing -- Minimum 240000/year (requires product management approval)	DS-ASA	$ 240,000.00	$ 234,559.19
DocuSign	DocuSign - Additional-Connectors ($/user/year)	DS-AC	$ 144.00	$ 140.74
DocuSign	DocuSign - Professional Services -20 hr bundle Flat fee	DS-PSB	$ 5,000.00	$ 4,886.65
DocuSign	DocuSign - Strategic Value Assessments -SVA Corporate Flat fee	DS-SVA-C	$ 3,500.00	$ 3,420.65
DocuSign	DocuSign - Strategic Value Assessments -SVA Enterprise Flat fee	DS-SVA-E	$ 10,000.00	$ 9,773.30
DocuSign	DocuSign - Training-DS Transaction Rooms Broker Edition - Agent/User Training $/person	DS-TRBE-AUT	$ 295.00	$ 288.31
DocuSign	DocuSign - Training-DS Transaction Rooms Broker Edition - Admin/Account Setup $/person	DS-TRBE-AAU	$ 295.00	$ 288.31
DocuSign	DocuSign Enterprise Edition	DS-EE	$ 540.00	$ 527.76
DocuSign	Professional Services - Fast start Salesforce.com - SERVICE	DS-PS-FSS	$ 14,525.00	$ 14,195.72
DocuSign	Professional Services - Fast start web console - SERVICE	DS-PS-FSWC	$ 9,975.00	$ 9,748.87
DocuSign	DocuSign Enterprise Edition Enterprise Premier (Support)- Envelopes-USD- Annual	12000111E-EP	$ 1.32	$ 1.30
DocuSign	DocuSign System Automated Premium Edition Enterprise Premier (Support)	DS-SAPE-EP	$ 1.10	$ 1.09
DocuSign	DocuSign for Salesforce Enterprise Edition Premier (Support)- Envelopes- USD- Annual	12000121E-P	$ 1.05	$ 1.04
DocuSign	DocuSign Enterprise Edition Premier (Support)- Envelopes-USD- Annual	12000111E-P	$ 0.90	$ 0.89
DocuSign	DocuSign System Automated Premium Edition Premier (Support)	DS-SAPE-P	$ 0.75	$ 0.74
DocuSign	DocuSign Business Edition Enterprise Premier (Support)- SMS	200013-EP	$ 0.44	$ 0.44
DocuSign	DocuSign for Salesforce Dynamic Documents Enterprise Premier (Support)- Envelopes- USD- Annual	12000232E-EP	$ 0.44	$ 0.44
DocuSign	DocuSign Business Edition Premier (Support)- SMS	200013-P	$ 0.30	$ 0.30
DocuSign	DocuSign for Salesforce Dynamic Documents Premier (Support)- Envelopes- USD- Annual	12000232E-P	$ 0.30	$ 0.30
FireEye	Email Threat Prevention, Platinum Support 1 Year 1-249	ETP-000249-PTM1Y	$ 58.32	$ 50.74
FireEye	Email Threat Prevention, Platinum Support 2 Year 1-249	ETP-000249-PTM2Y	$ 116.64	$ 101.48
FireEye	Email Threat Prevention, Platinum Support 3 Year 1-249	ETP-000249-PTM3Y	$ 157.46	$ 136.99
FireEye	Email Threat Prevention, Platinum Support 4 Year 1-249	ETP-000249-PTM4Y	$ 209.95	$ 182.66
FireEye	Email Threat Prevention, Platinum Support 5 Year 1-249	ETP-000249-PTM5Y	$ 262.44	$ 228.32
FireEye	Email Threat Prevention, Government US 1 Year 1-249	ETP-000249-USG1Y	$ 58.32	$ 50.74
FireEye	Email Threat Prevention, Government US 2 Year 1-249	ETP-000249-USG2Y	$ 116.64	$ 101.48
FireEye	Email Threat Prevention, Government US 3 Year 1-249	ETP-000249-USG3Y	$ 157.46	$ 136.99
FireEye	Email Threat Prevention, Government US 4 Year 1-249	ETP-000249-USG4Y	$ 209.95	$ 182.66

FireEye	Email Threat Prevention, Government US 5 Year 1-249	ETP-000249-USG5Y	$ 262.44	$ 228.32
FireEye	Email Threat Prevention, Platinum Support 1 Year 250-499	ETP-000499-PTM1Y	$ 48.15	$ 41.89
FireEye	Email Threat Prevention, Platinum Support 2 Year 250-499	ETP-000499-PTM2Y	$ 96.30	$ 83.78
FireEye	Email Threat Prevention, Platinum Support 3 Year 250-499	ETP-000499-PTM3Y	$ 130.01	$ 113.11
FireEye	Email Threat Prevention, Platinum Support 4 Year 250-499	ETP-000499-PTM4Y	$ 173.34	$ 150.81
FireEye	Email Threat Prevention, Platinum Support 5 Year 250-499	ETP-000499-PTM5Y	$ 216.68	$ 188.51
FireEye	Email Threat Prevention, Government US 1 Year 250-499	ETP-000499-USG1Y	$ 48.15	$ 41.89
FireEye	Email Threat Prevention, Government US 2 Year 250-499	ETP-000499-USG2Y	$ 96.30	$ 83.78
FireEye	Email Threat Prevention, Government US 3 Year 250-499	ETP-000499-USG3Y	$ 130.01	$ 113.11
FireEye	Email Threat Prevention, Government US 4 Year 250-499	ETP-000499-USG4Y	$ 173.34	$ 150.81
FireEye	Email Threat Prevention, Government US 5 Year 250-499	ETP-000499-USG5Y	$ 216.68	$ 188.51
FireEye	Email Threat Prevention, Platinum Support 1 Year 500-749	ETP-000749-PTM1Y	$ 41.30	$ 35.93
FireEye	Email Threat Prevention, Platinum Support 2 Year 500-749	ETP-000749-PTM2Y	$ 82.60	$ 71.86
FireEye	Email Threat Prevention, Platinum Support 3 Year 500-749	ETP-000749-PTM3Y	$ 111.51	$ 97.01
FireEye	Email Threat Prevention, Platinum Support 4 Year 500-749	ETP-000749-PTM4Y	$ 148.68	$ 129.35
FireEye	Email Threat Prevention, Platinum Support 5 Year 500-749	ETP-000749-PTM5Y	$ 185.85	$ 161.69
FireEye	Email Threat Prevention, Government US 1 Year 500-749	ETP-000749-USG1Y	$ 41.30	$ 35.93
FireEye	Email Threat Prevention, Government US 2 Year 500-749	ETP-000749-USG2Y	$ 82.60	$ 71.86
FireEye	Email Threat Prevention, Government US 3 Year 500-749	ETP-000749-USG3Y	$ 111.51	$ 97.01
FireEye	Email Threat Prevention, Government US 4 Year 500-749	ETP-000749-USG4Y	$ 148.68	$ 129.35
FireEye	Email Threat Prevention, Government US 5 Year 500-749	ETP-000749-USG5Y	$ 185.85	$ 161.69
FireEye	Email Threat Prevention, Platinum Support 1 Year 750-999	ETP-000999-PTM1Y	$ 34.69	$ 30.18
FireEye	Email Threat Prevention, Platinum Support 2 Year 750-999	ETP-000999-PTM2Y	$ 69.38	$ 60.36
FireEye	Email Threat Prevention, Platinum Support 3 Year 750-999	ETP-000999-PTM3Y	$ 93.66	$ 81.48
FireEye	Email Threat Prevention, Platinum Support 4 Year 750-999	ETP-000999-PTM4Y	$ 124.88	$ 108.65
FireEye	Email Threat Prevention, Platinum Support 5 Year 750-999	ETP-000999-PTM5Y	$ 156.11	$ 135.82
FireEye	Email Threat Prevention, Government US 1 Year 750-999	ETP-000999-USG1Y	$ 34.69	$ 30.18
FireEye	Email Threat Prevention, Government US 2 Year 750-999	ETP-000999-USG2Y	$ 69.38	$ 60.36
FireEye	Email Threat Prevention, Government US 3 Year 750-999	ETP-000999-USG3Y	$ 93.66	$ 81.48
FireEye	Email Threat Prevention, Government US 4 Year 750-999	ETP-000999-USG4Y	$ 124.88	$ 108.65
FireEye	Email Threat Prevention, Government US 5 Year 750-999	ETP-000999-USG5Y	$ 156.11	$ 135.82
FireEye	Email Threat Prevention, Platinum Support 1 Year 1,000-1999	ETP-001999-PTM1Y	$ 31.46	$ 27.37
FireEye	Email Threat Prevention, Platinum Support 2 Year 1,000-1999	ETP-001999-PTM2Y	$ 62.92	$ 54.74
FireEye	Email Threat Prevention, Platinum Support 3 Year 1,000-1999	ETP-001999-PTM3Y	$ 84.94	$ 73.90
FireEye	Email Threat Prevention, Platinum Support 4 Year 1,000-1999	ETP-001999-PTM4Y	$ 113.26	$ 98.54
FireEye	Email Threat Prevention, Platinum Support 5 Year 1,000-1999	ETP-001999-PTM5Y	$ 141.57	$ 123.17
FireEye	Email Threat Prevention, Government US 1 Year 1,000-1999	ETP-001999-USG1Y	$ 31.46	$ 27.37
FireEye	Email Threat Prevention, Government US 2 Year 1,000-1999	ETP-001999-USG2Y	$ 62.92	$ 54.74
FireEye	Email Threat Prevention, Government US 3 Year 1,000-1999	ETP-001999-USG3Y	$ 84.94	$ 73.90
FireEye	Email Threat Prevention, Government US 4 Year 1,000-1999	ETP-001999-USG4Y	$ 113.26	$ 98.54
FireEye	Email Threat Prevention, Government US 5 Year 1,000-1999	ETP-001999-USG5Y	$ 141.57	$ 123.17
FireEye	Email Threat Prevention, Platinum Support 1 Year 2,000-4999	ETP-004999-PTM1Y	$ 28.64	$ 24.92
FireEye	Email Threat Prevention, Platinum Support 2 Year 2,000-4999	ETP-004999-PTM2Y	$ 57.28	$ 49.83
FireEye	Email Threat Prevention, Platinum Support 3 Year 2,000-4999	ETP-004999-PTM3Y	$ 77.33	$ 67.28
FireEye	Email Threat Prevention, Platinum Support 4 Year 2,000-4999	ETP-004999-PTM4Y	$ 103.10	$ 89.70
FireEye	Email Threat Prevention, Platinum Support 5 Year 2,000-4999	ETP-004999-PTM5Y	$ 128.88	$ 112.13
FireEye	Email Threat Prevention, Government US 1 Year 2,000-4999	ETP-004999-USG1Y	$ 28.64	$ 24.92
FireEye	Email Threat Prevention, Government US 2 Year 2,000-4999	ETP-004999-USG2Y	$ 57.28	$ 49.83
FireEye	Email Threat Prevention, Government US 3 Year 2,000-4999	ETP-004999-USG3Y	$ 77.33	$ 67.28

FireEye	Email Threat Prevention, Government US 4 Year 2,000-4999	ETP-004999-USG4Y	$ 103.10	$ 89.70
FireEye	Email Threat Prevention, Government US 5 Year 2,000-4999	ETP-004999-USG5Y	$ 128.88	$ 112.13
FireEye	Email Threat Prevention, Platinum Support 1 Year 5,000-9999	ETP-009999-PTM1Y	$ 25.51	$ 22.19
FireEye	Email Threat Prevention, Platinum Support 2 Year 5,000-9999	ETP-009999-PTM2Y	$ 51.02	$ 44.39
FireEye	Email Threat Prevention, Platinum Support 3 Year 5,000-9999	ETP-009999-PTM3Y	$ 68.88	$ 59.93
FireEye	Email Threat Prevention, Platinum Support 4 Year 5,000-9999	ETP-009999-PTM4Y	$ 91.84	$ 79.90
FireEye	Email Threat Prevention, Platinum Support 5 Year 5,000-9999	ETP-009999-PTM5Y	$ 114.80	$ 99.88
FireEye	Email Threat Prevention, Government US 1 Year 5,000-9999	ETP-009999-USG1Y	$ 25.51	$ 22.19
FireEye	Email Threat Prevention, Government US 2 Year 5,000-9999	ETP-009999-USG2Y	$ 51.02	$ 44.39
FireEye	Email Threat Prevention, Government US 3 Year 5,000-9999	ETP-009999-USG3Y	$ 68.88	$ 59.93
FireEye	Email Threat Prevention, Government US 4 Year 5,000-9999	ETP-009999-USG4Y	$ 91.84	$ 79.90
FireEye	Email Threat Prevention, Government US 5 Year 5,000-9999	ETP-009999-USG5Y	$ 114.80	$ 99.88
FireEye	Email Threat Prevention, Platinum Support 1 Year 10,000-19999	ETP-019999-PTM1Y	$ 22.02	$ 19.16
FireEye	Email Threat Prevention, Platinum Support 2 Year 10,000-19999	ETP-019999-PTM2Y	$ 44.04	$ 38.31
FireEye	Email Threat Prevention, Platinum Support 3 Year 10,000-19999	ETP-019999-PTM3Y	$ 59.45	$ 51.72
FireEye	Email Threat Prevention, Platinum Support 4 Year 10,000-19999	ETP-019999-PTM4Y	$ 79.27	$ 68.96
FireEye	Email Threat Prevention, Platinum Support 5 Year 10,000-19999	ETP-019999-PTM5Y	$ 99.09	$ 86.21
FireEye	Email Threat Prevention, Government US 1 Year 10,000-19999	ETP-019999-USG1Y	$ 22.02	$ 19.16
FireEye	Email Threat Prevention, Government US 2 Year 10,000-19999	ETP-019999-USG2Y	$ 44.04	$ 38.31
FireEye	Email Threat Prevention, Government US 3 Year 10,000-19999	ETP-019999-USG3Y	$ 59.45	$ 51.72
FireEye	Email Threat Prevention, Government US 4 Year 10,000-19999	ETP-019999-USG4Y	$ 79.27	$ 68.96
FireEye	Email Threat Prevention, Government US 5 Year 10,000-19999	ETP-019999-USG5Y	$ 99.09	$ 86.21
FireEye	Email Threat Prevention, Platinum Support 1 Year 20,000-49999	ETP-049999-PTM1Y	$ 20.76	$ 18.06
FireEye	Email Threat Prevention, Platinum Support 2 Year 20,000-49999	ETP-049999-PTM2Y	$ 41.52	$ 36.12
FireEye	Email Threat Prevention, Platinum Support 3 Year 20,000-49999	ETP-049999-PTM3Y	$ 56.05	$ 48.76
FireEye	Email Threat Prevention, Platinum Support 4 Year 20,000-49999	ETP-049999-PTM4Y	$ 74.74	$ 65.02
FireEye	Email Threat Prevention, Platinum Support 5 Year 20,000-49999	ETP-049999-PTM5Y	$ 93.42	$ 81.28
FireEye	Email Threat Prevention, Government US 1 Year 20,000-49999	ETP-049999-USG1Y	$ 20.76	$ 18.06
FireEye	Email Threat Prevention, Government US 2 Year 20,000-49999	ETP-049999-USG2Y	$ 41.52	$ 36.12
FireEye	Email Threat Prevention, Government US 3 Year 20,000-49999	ETP-049999-USG3Y	$ 56.05	$ 48.76
FireEye	Email Threat Prevention, Government US 4 Year 20,000-49999	ETP-049999-USG4Y	$ 74.74	$ 65.02
FireEye	Email Threat Prevention, Government US 5 Year 20,000-49999	ETP-049999-USG5Y	$ 93.42	$ 81.28
FireEye	Email Threat Prevention, Platinum Support 1 Year 50,000-74999	ETP-074999-PTM1Y	$ 18.75	$ 16.31
FireEye	Email Threat Prevention, Platinum Support 2 Year 50,000-74999	ETP-074999-PTM2Y	$ 37.50	$ 32.63
FireEye	Email Threat Prevention, Platinum Support 3 Year 50,000-74999	ETP-074999-PTM3Y	$ 50.63	$ 44.05
FireEye	Email Threat Prevention, Platinum Support 4 Year 50,000-74999	ETP-074999-PTM4Y	$ 67.50	$ 58.73
FireEye	Email Threat Prevention, Platinum Support 5 Year 50,000-74999	ETP-074999-PTM5Y	$ 84.38	$ 73.41
FireEye	Email Threat Prevention, Government US 1 Year 50,000-74999	ETP-074999-USG1Y	$ 18.75	$ 16.31
FireEye	Email Threat Prevention, Government US 2 Year 50,000-74999	ETP-074999-USG2Y	$ 37.50	$ 32.63
FireEye	Email Threat Prevention, Government US 3 Year 50,000-74999	ETP-074999-USG3Y	$ 50.63	$ 44.05
FireEye	Email Threat Prevention, Government US 4 Year 50,000-74999	ETP-074999-USG4Y	$ 67.50	$ 58.73
FireEye	Email Threat Prevention, Government US 5 Year 50,000-74999	ETP-074999-USG5Y	$ 84.38	$ 73.41
FireEye	Email Threat Prevention, Platinum Support 1 Year 75,000-99999	ETP-099999-PTM1Y	$ 16.22	$ 14.11
FireEye	Email Threat Prevention, Platinum Support 2 Year 75,000-99999	ETP-099999-PTM2Y	$ 32.44	$ 28.22
FireEye	Email Threat Prevention, Platinum Support 3 Year 75,000-99999	ETP-099999-PTM3Y	$ 43.79	$ 38.10
FireEye	Email Threat Prevention, Platinum Support 4 Year 75,000-99999	ETP-099999-PTM4Y	$ 58.39	$ 50.80
FireEye	Email Threat Prevention, Platinum Support 5 Year 75,000-99999	ETP-099999-PTM5Y	$ 72.99	$ 63.50
FireEye	Email Threat Prevention, Government US 1 Year 75,000-99999	ETP-099999-USG1Y	$ 16.22	$ 14.11
FireEye	Email Threat Prevention, Government US 2 Year 75,000-99999	ETP-099999-USG2Y	$ 32.44	$ 28.22

FireEye	Email Threat Prevention, Government US 3 Year 75,000-99999	ETP-099999-USG3Y	$ 43.79	$ 38.10
FireEye	Email Threat Prevention, Government US 4 Year 75,000-99999	ETP-099999-USG4Y	$ 58.39	$ 50.80
FireEye	Email Threat Prevention, Government US 5 Year 75,000-99999	ETP-099999-USG5Y	$ 72.99	$ 63.50
FireEye	Email Threat Prevention, Platinum Support 1 Year 100,000-199999	ETP-199999-PTM1Y	$ 14.26	$ 12.41
FireEye	Email Threat Prevention, Platinum Support 2 Year 100,000-199999	ETP-199999-PTM2Y	$ 28.52	$ 24.81
FireEye	Email Threat Prevention, Platinum Support 3 Year 100,000-199999	ETP-199999-PTM3Y	$ 38.50	$ 33.50
FireEye	Email Threat Prevention, Platinum Support 4 Year 100,000-199999	ETP-199999-PTM4Y	$ 51.34	$ 44.67
FireEye	Email Threat Prevention, Platinum Support 5 Year 100,000-199999	ETP-199999-PTM5Y	$ 64.17	$ 55.83
FireEye	Email Threat Prevention, Government US 1 Year 100,000-199999	ETP-199999-USG1Y	$ 14.26	$ 12.41
FireEye	Email Threat Prevention, Government US 2 Year 100,000-199999	ETP-199999-USG2Y	$ 28.52	$ 24.81
FireEye	Email Threat Prevention, Government US 3 Year 100,000-199999	ETP-199999-USG3Y	$ 38.50	$ 33.50
FireEye	Email Threat Prevention, Government US 4 Year 100,000-199999	ETP-199999-USG4Y	$ 51.34	$ 44.67
FireEye	Email Threat Prevention, Government US 5 Year 100,000-199999	ETP-199999-USG5Y	$ 64.17	$ 55.83
FireEye	Email Threat Prevention, Platinum Support 1 Year 200,000+	ETP-200000+PTM1Y	$ 13.46	$ 11.71
FireEye	Email Threat Prevention, Platinum Support 2 Year 200,000+	ETP-200000+PTM2Y	$ 26.92	$ 23.42
FireEye	Email Threat Prevention, Platinum Support 3 Year 200,000+	ETP-200000+PTM3Y	$ 36.34	$ 31.62
FireEye	Email Threat Prevention, Platinum Support 4 Year 200,000+	ETP-200000+PTM4Y	$ 48.46	$ 42.16
FireEye	Email Threat Prevention, Platinum Support 5 Year 200,000+	ETP-200000+PTM5Y	$ 60.57	$ 52.70
FireEye	Email Threat Prevention, Government US 1 Year 200,000+	ETP-200000+USG1Y	$ 13.46	$ 11.71
FireEye	Email Threat Prevention, Government US 2 Year 200,000+	ETP-200000+USG2Y	$ 26.92	$ 23.42
FireEye	Email Threat Prevention, Government US 3 Year 200,000+	ETP-200000+USG3Y	$ 36.34	$ 31.62
FireEye	Email Threat Prevention, Government US 4 Year 200,000+	ETP-200000+USG4Y	$ 48.46	$ 42.16
FireEye	Email Threat Prevention, Government US 5 Year 200,000+	ETP-200000+USG5Y	$ 60.57	$ 52.70
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 1-249	ETP-A-000249-CAG1Y	$ 71.95	$ 62.60
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 1-249	ETP-A-000249-CAG2Y	$ 134.55	$ 117.06
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 1-249	ETP-A-000249-CAG3Y	$ 194.27	$ 169.01
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 1-249	ETP-A-000249-CAG4Y	$ 259.02	$ 225.35
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 1-249	ETP-A-000249-CAG5Y	$ 323.78	$ 281.69
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 1-249	ETP-A-000249-CAP1Y	$ 75.00	$ 65.25
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 1-249	ETP-A-000249-CAP2Y	$ 140.25	$ 122.02
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 1-249	ETP-A-000249-CAP3Y	$ 202.50	$ 176.18
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 1-249	ETP-A-000249-CAP4Y	$ 270.00	$ 234.90
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 1-249	ETP-A-000249-CAP5Y	$ 337.50	$ 293.63
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 1-249	ETP-A-000249-PPL1Y	$ 13.62	$ 11.85
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 1-249	ETP-A-000249-PPL2Y	$ 140.25	$ 122.02
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 1-249	ETP-A-000249-PPL3Y	$ 202.50	$ 176.18
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 1-249	ETP-A-000249-PPL4Y	$ 270.00	$ 234.90
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 1-249	ETP-A-000249-PPL5Y	$ 337.50	$ 293.63
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 1-249	ETP-A-000249-PTM1Y	$ 26.24	$ 22.83
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 1-249	ETP-A-000249-PTM2Y	$ 134.55	$ 117.06
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 1-249	ETP-A-000249-PTM3Y	$ 194.27	$ 169.01
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 1-249	ETP-A-000249-PTM4Y	$ 259.02	$ 225.35
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 1-249	ETP-A-000249-PTM5Y	$ 323.78	$ 281.69
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 1-249	ETP-A-000249-USG1Y	$ 71.95	$ 62.60
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 1-249	ETP-A-000249-USG2Y	$ 134.55	$ 117.06
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 1-249	ETP-A-000249-USG3Y	$ 194.27	$ 169.01
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 1-249	ETP-A-000249-USG4Y	$ 259.02	$ 225.35
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 1-249	ETP-A-000249-USG5Y	$ 323.78	$ 281.69
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 1-249	ETP-A-000249-USP1Y	$ 75.00	$ 65.25

FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 1-249	ETP-A-000249-USP2Y	$ 140.25	$ 122.02
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 1-249	ETP-A-000249-USP3Y	$ 202.50	$ 176.18
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 1-249	ETP-A-000249-USP4Y	$ 270.00	$ 234.90
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 1-249	ETP-A-000249-USP5Y	$ 337.50	$ 293.63
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 250-499	ETP-A-000499-CAG1Y	$ 35.96	$ 31.29
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 250-499	ETP-A-000499-CAG2Y	$ 67.24	$ 58.50
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 250-499	ETP-A-000499-CAG3Y	$ 97.09	$ 84.47
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 250-499	ETP-A-000499-CAG4Y	$ 129.46	$ 112.63
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 250-499	ETP-A-000499-CAG5Y	$ 161.82	$ 140.78
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 250-499	ETP-A-000499-CAP1Y	$ 37.48	$ 32.61
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 250-499	ETP-A-000499-CAP2Y	$ 70.09	$ 60.98
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 250-499	ETP-A-000499-CAP3Y	$ 101.20	$ 88.04
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 250-499	ETP-A-000499-CAP4Y	$ 134.93	$ 117.39
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 250-499	ETP-A-000499-CAP5Y	$ 168.66	$ 146.73
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 250-499	ETP-A-000499-PPL1Y	$ 11.26	$ 9.80
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 250-499	ETP-A-000499-PPL2Y	$ 70.09	$ 60.98
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 250-499	ETP-A-000499-PPL3Y	$ 101.20	$ 88.04
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 250-499	ETP-A-000499-PPL4Y	$ 134.93	$ 117.39
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 250-499	ETP-A-000499-PPL5Y	$ 168.66	$ 146.73
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 250-499	ETP-A-000499-PTM1Y	$ 21.67	$ 18.85
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 250-499	ETP-A-000499-PTM2Y	$ 67.24	$ 58.50
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 250-499	ETP-A-000499-PTM3Y	$ 97.09	$ 84.47
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 250-499	ETP-A-000499-PTM4Y	$ 129.46	$ 112.63
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 250-499	ETP-A-000499-PTM5Y	$ 161.82	$ 140.78
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 250-499	ETP-A-000499-USG1Y	$ 35.96	$ 31.29
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 250-499	ETP-A-000499-USG2Y	$ 67.24	$ 58.50
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 250-499	ETP-A-000499-USG3Y	$ 97.09	$ 84.47
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 250-499	ETP-A-000499-USG4Y	$ 129.46	$ 112.63
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 250-499	ETP-A-000499-USG5Y	$ 161.82	$ 140.78
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 250-499	ETP-A-000499-USP1Y	$ 37.48	$ 32.61
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 250-499	ETP-A-000499-USP2Y	$ 70.09	$ 60.98
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 250-499	ETP-A-000499-USP3Y	$ 101.20	$ 88.04
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 250-499	ETP-A-000499-USP4Y	$ 134.93	$ 117.39
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 250-499	ETP-A-000499-USP5Y	$ 168.66	$ 146.73
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 500-749	ETP-A-000749-CAG1Y	$ 29.76	$ 25.89
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 500-749	ETP-A-000749-CAG2Y	$ 55.65	$ 48.42
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 500-749	ETP-A-000749-CAG3Y	$ 80.35	$ 69.90
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 500-749	ETP-A-000749-CAG4Y	$ 107.14	$ 93.21
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 500-749	ETP-A-000749-CAG5Y	$ 133.92	$ 116.51
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 500-749	ETP-A-000749-CAP1Y	$ 31.02	$ 26.99
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 500-749	ETP-A-000749-CAP2Y	$ 58.00	$ 50.46
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 500-749	ETP-A-000749-CAP3Y	$ 83.75	$ 72.86
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 500-749	ETP-A-000749-CAP4Y	$ 111.67	$ 97.15
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 500-749	ETP-A-000749-CAP5Y	$ 139.59	$ 121.44
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 500-749	ETP-A-000749-PPL1Y	$ 9.66	$ 8.40
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 500-749	ETP-A-000749-PPL2Y	$ 58.00	$ 50.46
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 500-749	ETP-A-000749-PPL3Y	$ 83.75	$ 72.86
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 500-749	ETP-A-000749-PPL4Y	$ 111.67	$ 97.15
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 500-749	ETP-A-000749-PPL5Y	$ 139.59	$ 121.44

FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 500-749	ETP-A-000749-PTM1Y	$ 18.59	$ 16.17
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 500-749	ETP-A-000749-PTM2Y	$ 55.65	$ 48.42
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 500-749	ETP-A-000749-PTM3Y	$ 80.35	$ 69.90
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 500-749	ETP-A-000749-PTM4Y	$ 107.14	$ 93.21
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 500-749	ETP-A-000749-PTM5Y	$ 133.92	$ 116.51
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 500-749	ETP-A-000749-USG1Y	$ 29.76	$ 25.89
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 500-749	ETP-A-000749-USG2Y	$ 55.65	$ 48.42
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 500-749	ETP-A-000749-USG3Y	$ 80.35	$ 69.90
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 500-749	ETP-A-000749-USG4Y	$ 107.14	$ 93.21
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 500-749	ETP-A-000749-USG5Y	$ 133.92	$ 116.51
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 500-749	ETP-A-000749-USP1Y	$ 31.02	$ 26.99
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 500-749	ETP-A-000749-USP2Y	$ 58.00	$ 50.46
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 500-749	ETP-A-000749-USP3Y	$ 83.75	$ 72.86
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 500-749	ETP-A-000749-USP4Y	$ 111.67	$ 97.15
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 500-749	ETP-A-000749-USP5Y	$ 139.59	$ 121.44
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 750-999	ETP-A-000999-CAG1Y	$ 29.03	$ 25.26
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 750-999	ETP-A-000999-CAG2Y	$ 54.28	$ 47.22
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 750-999	ETP-A-000999-CAG3Y	$ 78.38	$ 68.19
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 750-999	ETP-A-000999-CAG4Y	$ 104.51	$ 90.92
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 750-999	ETP-A-000999-CAG5Y	$ 130.64	$ 113.66
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 750-999	ETP-A-000999-CAP1Y	$ 30.26	$ 26.33
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 750-999	ETP-A-000999-CAP2Y	$ 56.58	$ 49.22
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 750-999	ETP-A-000999-CAP3Y	$ 81.70	$ 71.08
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 750-999	ETP-A-000999-CAP4Y	$ 108.94	$ 94.78
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 750-999	ETP-A-000999-CAP5Y	$ 136.17	$ 118.47
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 750-999	ETP-A-000999-PPL1Y	$ 8.11	$ 7.06
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 750-999	ETP-A-000999-PPL2Y	$ 56.58	$ 49.22
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 750-999	ETP-A-000999-PPL3Y	$ 81.70	$ 71.08
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 750-999	ETP-A-000999-PPL4Y	$ 108.94	$ 94.78
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 750-999	ETP-A-000999-PPL5Y	$ 136.17	$ 118.47
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 750-999	ETP-A-000999-PTM1Y	$ 15.61	$ 13.58
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 750-999	ETP-A-000999-PTM2Y	$ 54.28	$ 47.22
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 750-999	ETP-A-000999-PTM3Y	$ 78.38	$ 68.19
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 750-999	ETP-A-000999-PTM4Y	$ 104.51	$ 90.92
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 750-999	ETP-A-000999-PTM5Y	$ 130.64	$ 113.66
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 750-999	ETP-A-000999-USG1Y	$ 29.03	$ 25.26
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 750-999	ETP-A-000999-USG2Y	$ 54.28	$ 47.22
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 750-999	ETP-A-000999-USG3Y	$ 78.38	$ 68.19
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 750-999	ETP-A-000999-USG4Y	$ 104.51	$ 90.92
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 750-999	ETP-A-000999-USG5Y	$ 130.64	$ 113.66
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 750-999	ETP-A-000999-USP1Y	$ 30.26	$ 26.33
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 750-999	ETP-A-000999-USP2Y	$ 56.58	$ 49.22
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 750-999	ETP-A-000999-USP3Y	$ 81.70	$ 71.08
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 750-999	ETP-A-000999-USP4Y	$ 108.94	$ 94.78
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 750-999	ETP-A-000999-USP5Y	$ 136.17	$ 118.47
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 1,000-1999	ETP-A-001999-CAG1Y	$ 22.35	$ 19.44
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 1,000-1999	ETP-A-001999-CAG2Y	$ 41.79	$ 36.36
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 1,000-1999	ETP-A-001999-CAG3Y	$ 60.35	$ 52.50
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 1,000-1999	ETP-A-001999-CAG4Y	$ 80.46	$ 70.00

FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 1,000-1999	ETP-A-001999-CAG5Y	$ 100.58	$ 87.50
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 1,000-1999	ETP-A-001999-CAP1Y	$ 23.29	$ 20.26
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 1,000-1999	ETP-A-001999-CAP2Y	$ 43.56	$ 37.90
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 1,000-1999	ETP-A-001999-CAP3Y	$ 62.88	$ 54.71
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 1,000-1999	ETP-A-001999-CAP4Y	$ 83.84	$ 72.94
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 1,000-1999	ETP-A-001999-CAP5Y	$ 104.81	$ 91.18
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 1,000-1999	ETP-A-001999-PPL1Y	$ 7.35	$ 6.39
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 1,000-1999	ETP-A-001999-PPL2Y	$ 43.56	$ 37.90
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 1,000-1999	ETP-A-001999-PPL3Y	$ 62.88	$ 54.71
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 1,000-1999	ETP-A-001999-PPL4Y	$ 83.84	$ 72.94
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 1,000-1999	ETP-A-001999-PPL5Y	$ 104.81	$ 91.18
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 1,000-1999	ETP-A-001999-PTM1Y	$ 14.16	$ 12.32
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 1,000-1999	ETP-A-001999-PTM2Y	$ 41.79	$ 36.36
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 1,000-1999	ETP-A-001999-PTM3Y	$ 60.35	$ 52.50
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 1,000-1999	ETP-A-001999-PTM4Y	$ 80.46	$ 70.00
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 1,000-1999	ETP-A-001999-PTM5Y	$ 100.58	$ 87.50
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 1,000-1999	ETP-A-001999-USG1Y	$ 22.35	$ 19.44
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 1,000-1999	ETP-A-001999-USG2Y	$ 41.79	$ 36.36
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 1,000-1999	ETP-A-001999-USG3Y	$ 60.35	$ 52.50
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 1,000-1999	ETP-A-001999-USG4Y	$ 80.46	$ 70.00
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 1,000-1999	ETP-A-001999-USG5Y	$ 100.58	$ 87.50
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 1,000-1999	ETP-A-001999-USP1Y	$ 23.29	$ 20.26
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 1,000-1999	ETP-A-001999-USP2Y	$ 43.56	$ 37.90
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 1,000-1999	ETP-A-001999-USP3Y	$ 62.88	$ 54.71
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 1,000-1999	ETP-A-001999-USP4Y	$ 83.84	$ 72.94
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 1,000-1999	ETP-A-001999-USP5Y	$ 104.81	$ 91.18
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 2,000-4999	ETP-A-004999-CAG1Y	$ 16.67	$ 14.50
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 2,000-4999	ETP-A-004999-CAG2Y	$ 31.17	$ 27.12
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 2,000-4999	ETP-A-004999-CAG3Y	$ 45.01	$ 39.16
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 2,000-4999	ETP-A-004999-CAG4Y	$ 60.01	$ 52.21
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 2,000-4999	ETP-A-004999-CAG5Y	$ 75.02	$ 65.27
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 2,000-4999	ETP-A-004999-CAP1Y	$ 17.38	$ 15.12
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 2,000-4999	ETP-A-004999-CAP2Y	$ 32.49	$ 28.27
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 2,000-4999	ETP-A-004999-CAP3Y	$ 46.93	$ 40.83
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 2,000-4999	ETP-A-004999-CAP4Y	$ 62.57	$ 54.44
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 2,000-4999	ETP-A-004999-CAP5Y	$ 78.21	$ 68.04
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 2,000-4999	ETP-A-004999-PPL1Y	$ 6.70	$ 5.83
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 2,000-4999	ETP-A-004999-PPL2Y	$ 32.49	$ 28.27
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 2,000-4999	ETP-A-004999-PPL3Y	$ 46.93	$ 40.83
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 2,000-4999	ETP-A-004999-PPL4Y	$ 62.57	$ 54.44
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 2,000-4999	ETP-A-004999-PPL5Y	$ 78.21	$ 68.04
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 2,000-4999	ETP-A-004999-PTM1Y	$ 12.89	$ 11.21
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 2,000-4999	ETP-A-004999-PTM2Y	$ 31.17	$ 27.12
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 2,000-4999	ETP-A-004999-PTM3Y	$ 45.01	$ 39.16
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 2,000-4999	ETP-A-004999-PTM4Y	$ 60.01	$ 52.21
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 2,000-4999	ETP-A-004999-PTM5Y	$ 75.02	$ 65.27
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 2,000-4999	ETP-A-004999-USG1Y	$ 16.67	$ 14.50
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 2,000-4999	ETP-A-004999-USG2Y	$ 31.17	$ 27.12
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 2,000-4999	ETP-A-004999-USG3Y	$ 45.01	$ 39.16

FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 2,000-4999	ETP-A-004999-USG4Y	$ 60.01	$ 52.21
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 2,000-4999	ETP-A-004999-USG5Y	$ 75.02	$ 65.27
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 2,000-4999	ETP-A-004999-USP1Y	$ 17.38	$ 15.12
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 2,000-4999	ETP-A-004999-USP2Y	$ 32.49	$ 28.27
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 2,000-4999	ETP-A-004999-USP3Y	$ 46.93	$ 40.83
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 2,000-4999	ETP-A-004999-USP4Y	$ 62.57	$ 54.44
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 2,000-4999	ETP-A-004999-USP5Y	$ 78.21	$ 68.04
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 5,000-9999	ETP-A-009999-CAG1Y	$ 14.75	$ 12.83
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 5,000-9999	ETP-A-009999-CAG2Y	$ 27.57	$ 23.99
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 5,000-9999	ETP-A-009999-CAG3Y	$ 39.83	$ 34.65
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 5,000-9999	ETP-A-009999-CAG4Y	$ 53.10	$ 46.20
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 5,000-9999	ETP-A-009999-CAG5Y	$ 66.38	$ 57.75
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 5,000-9999	ETP-A-009999-CAP1Y	$ 15.37	$ 13.37
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 5,000-9999	ETP-A-009999-CAP2Y	$ 28.74	$ 25.00
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 5,000-9999	ETP-A-009999-CAP3Y	$ 41.50	$ 36.11
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 5,000-9999	ETP-A-009999-CAP4Y	$ 55.33	$ 48.14
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 5,000-9999	ETP-A-009999-CAP5Y	$ 69.17	$ 60.18
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 5,000-9999	ETP-A-009999-PPL1Y	$ 8.29	$ 7.21
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 5,000-9999	ETP-A-009999-PPL2Y	$ 28.74	$ 25.00
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 5,000-9999	ETP-A-009999-PPL3Y	$ 41.50	$ 36.11
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 5,000-9999	ETP-A-009999-PPL4Y	$ 55.33	$ 48.14
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 5,000-9999	ETP-A-009999-PPL5Y	$ 69.17	$ 60.18
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 5,000-9999	ETP-A-009999-PTM1Y	$ 13.71	$ 11.93
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 5,000-9999	ETP-A-009999-PTM2Y	$ 27.57	$ 23.99
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 5,000-9999	ETP-A-009999-PTM3Y	$ 39.83	$ 34.65
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 5,000-9999	ETP-A-009999-PTM4Y	$ 53.10	$ 46.20
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 5,000-9999	ETP-A-009999-PTM5Y	$ 66.38	$ 57.75
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 5,000-9999	ETP-A-009999-USG1Y	$ 14.75	$ 12.83
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 5,000-9999	ETP-A-009999-USG2Y	$ 27.57	$ 23.99
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 5,000-9999	ETP-A-009999-USG3Y	$ 39.83	$ 34.65
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 5,000-9999	ETP-A-009999-USG4Y	$ 53.10	$ 46.20
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 5,000-9999	ETP-A-009999-USG5Y	$ 66.38	$ 57.75
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 5,000-9999	ETP-A-009999-USP1Y	$ 15.37	$ 13.37
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 5,000-9999	ETP-A-009999-USP2Y	$ 28.74	$ 25.00
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 5,000-9999	ETP-A-009999-USP3Y	$ 41.50	$ 36.11
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 5,000-9999	ETP-A-009999-USP4Y	$ 55.33	$ 48.14
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 5,000-9999	ETP-A-009999-USP5Y	$ 69.17	$ 60.18
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 10,000-19999	ETP-A-019999-CAG1Y	$ 12.89	$ 11.21
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 10,000-19999	ETP-A-019999-CAG2Y	$ 24.11	$ 20.98
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 10,000-19999	ETP-A-019999-CAG3Y	$ 34.80	$ 30.28
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 10,000-19999	ETP-A-019999-CAG4Y	$ 46.40	$ 40.37
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 10,000-19999	ETP-A-019999-CAG5Y	$ 58.01	$ 50.47
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 10,000-19999	ETP-A-019999-CAP1Y	$ 13.44	$ 11.69
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 10,000-19999	ETP-A-019999-CAP2Y	$ 25.13	$ 21.86
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 10,000-19999	ETP-A-019999-CAP3Y	$ 36.29	$ 31.57
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 10,000-19999	ETP-A-019999-CAP4Y	$ 48.38	$ 42.09
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 10,000-19999	ETP-A-019999-CAP5Y	$ 60.48	$ 52.62
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 10,000-19999	ETP-A-019999-PPL1Y	$ 6.07	$ 5.28
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 10,000-19999	ETP-A-019999-PPL2Y	$ 25.13	$ 21.86

FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 10,000-19999	ETP-A-019999-PPL3Y	$ 36.29	$ 31.57
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 10,000-19999	ETP-A-019999-PPL4Y	$ 48.38	$ 42.09
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 10,000-19999	ETP-A-019999-PPL5Y	$ 60.48	$ 52.62
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 10,000-19999	ETP-A-019999-PTM1Y	$ 10.79	$ 9.39
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 10,000-19999	ETP-A-019999-PTM2Y	$ 24.11	$ 20.98
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 10,000-19999	ETP-A-019999-PTM3Y	$ 34.80	$ 30.28
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 10,000-19999	ETP-A-019999-PTM4Y	$ 46.40	$ 40.37
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 10,000-19999	ETP-A-019999-PTM5Y	$ 58.01	$ 50.47
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 10,000-19999	ETP-A-019999-USG1Y	$ 12.89	$ 11.21
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 10,000-19999	ETP-A-019999-USG2Y	$ 24.11	$ 20.98
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 10,000-19999	ETP-A-019999-USG3Y	$ 34.80	$ 30.28
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 10,000-19999	ETP-A-019999-USG4Y	$ 46.40	$ 40.37
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 10,000-19999	ETP-A-019999-USG5Y	$ 58.01	$ 50.47
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 10,000-19999	ETP-A-019999-USP1Y	$ 13.44	$ 11.69
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 10,000-19999	ETP-A-019999-USP2Y	$ 25.13	$ 21.86
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 10,000-19999	ETP-A-019999-USP3Y	$ 36.29	$ 31.57
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 10,000-19999	ETP-A-019999-USP4Y	$ 48.38	$ 42.09
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 10,000-19999	ETP-A-019999-USP5Y	$ 60.48	$ 52.62
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 20,000-49999	ETP-A-049999-CAG1Y	$ 11.55	$ 10.05
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 20,000-49999	ETP-A-049999-CAG2Y	$ 21.67	$ 18.85
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 20,000-49999	ETP-A-049999-CAG3Y	$ 31.19	$ 27.14
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 20,000-49999	ETP-A-049999-CAG4Y	$ 41.58	$ 36.17
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 20,000-49999	ETP-A-049999-CAG5Y	$ 51.98	$ 45.22
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 20,000-49999	ETP-A-049999-CAP1Y	$ 12.04	$ 10.47
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 20,000-49999	ETP-A-049999-CAP2Y	$ 22.59	$ 19.65
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 20,000-49999	ETP-A-049999-CAP3Y	$ 32.51	$ 28.28
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 20,000-49999	ETP-A-049999-CAP4Y	$ 43.34	$ 37.71
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 20,000-49999	ETP-A-049999-CAP5Y	$ 54.18	$ 47.14
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 20,000-49999	ETP-A-049999-PPL1Y	$ 4.85	$ 4.22
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 20,000-49999	ETP-A-049999-PPL2Y	$ 22.50	$ 19.58
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 20,000-49999	ETP-A-049999-PPL3Y	$ 32.51	$ 28.28
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 20,000-49999	ETP-A-049999-PPL4Y	$ 43.34	$ 37.71
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 20,000-49999	ETP-A-049999-PPL5Y	$ 54.18	$ 47.14
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 20,000-49999	ETP-A-049999-PTM1Y	$ 9.34	$ 8.13
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 20,000-49999	ETP-A-049999-PTM2Y	$ 21.59	$ 18.78
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 20,000-49999	ETP-A-049999-PTM3Y	$ 31.19	$ 27.14
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 20,000-49999	ETP-A-049999-PTM4Y	$ 41.58	$ 36.17
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 20,000-49999	ETP-A-049999-PTM5Y	$ 51.98	$ 45.22
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 20,000-49999	ETP-A-049999-USG1Y	$ 11.55	$ 10.05
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 20,000-49999	ETP-A-049999-USG2Y	$ 21.67	$ 18.85
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 20,000-49999	ETP-A-049999-USG3Y	$ 31.19	$ 27.14
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 20,000-49999	ETP-A-049999-USG4Y	$ 41.58	$ 36.17
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 20,000-49999	ETP-A-049999-USG5Y	$ 51.98	$ 45.22
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 20,000-49999	ETP-A-049999-USP1Y	$ 12.04	$ 10.47
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 20,000-49999	ETP-A-049999-USP2Y	$ 22.59	$ 19.65
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 20,000-49999	ETP-A-049999-USP3Y	$ 32.51	$ 28.28
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 20,000-49999	ETP-A-049999-USP4Y	$ 43.34	$ 37.71
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 20,000-49999	ETP-A-049999-USP5Y	$ 54.18	$ 47.14
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 50,000-74999	ETP-A-074999-CAG1Y	$ 11.84	$ 10.30

FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 50,000-74999	ETP-A-074999-CAG2Y	$ 22.18	$ 19.30
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 50,000-74999	ETP-A-074999-CAG3Y	$ 31.97	$ 27.81
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 50,000-74999	ETP-A-074999-CAG4Y	$ 42.62	$ 37.08
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 50,000-74999	ETP-A-074999-CAG5Y	$ 53.28	$ 46.35
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 50,000-74999	ETP-A-074999-CAP1Y	$ 12.34	$ 10.74
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 50,000-74999	ETP-A-074999-CAP2Y	$ 23.13	$ 20.12
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 50,000-74999	ETP-A-074999-CAP3Y	$ 33.32	$ 28.99
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 50,000-74999	ETP-A-074999-CAP4Y	$ 44.42	$ 38.65
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 50,000-74999	ETP-A-074999-CAP5Y	$ 55.53	$ 48.31
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 50,000-74999	ETP-A-074999-PPL1Y	$ 4.76	$ 4.14
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 50,000-74999	ETP-A-074999-PPL2Y	$ 23.06	$ 20.06
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 50,000-74999	ETP-A-074999-PPL3Y	$ 33.32	$ 28.99
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 50,000-74999	ETP-A-074999-PPL4Y	$ 44.42	$ 38.65
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 50,000-74999	ETP-A-074999-PPL5Y	$ 55.53	$ 48.31
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 50,000-74999	ETP-A-074999-PTM1Y	$ 8.80	$ 7.66
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 50,000-74999	ETP-A-074999-PTM2Y	$ 22.14	$ 19.26
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 50,000-74999	ETP-A-074999-PTM3Y	$ 31.97	$ 27.81
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 50,000-74999	ETP-A-074999-PTM4Y	$ 42.62	$ 37.08
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 50,000-74999	ETP-A-074999-PTM5Y	$ 53.28	$ 46.35
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 50,000-74999	ETP-A-074999-USG1Y	$ 11.84	$ 10.30
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 50,000-74999	ETP-A-074999-USG2Y	$ 22.18	$ 19.30
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 50,000-74999	ETP-A-074999-USG3Y	$ 31.97	$ 27.81
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 50,000-74999	ETP-A-074999-USG4Y	$ 42.62	$ 37.08
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 50,000-74999	ETP-A-074999-USG5Y	$ 53.28	$ 46.35
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 50,000-74999	ETP-A-074999-USP1Y	$ 12.34	$ 10.74
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 50,000-74999	ETP-A-074999-USP2Y	$ 23.13	$ 20.12
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 50,000-74999	ETP-A-074999-USP3Y	$ 33.32	$ 28.99
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 50,000-74999	ETP-A-074999-USP4Y	$ 44.42	$ 38.65
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 50,000-74999	ETP-A-074999-USP5Y	$ 55.53	$ 48.31
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 75,000-99999	ETP-A-099999-CAG1Y	$ 12.39	$ 10.78
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 75,000-99999	ETP-A-099999-CAG2Y	$ 23.16	$ 20.15
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 75,000-99999	ETP-A-099999-CAG3Y	$ 33.45	$ 29.10
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 75,000-99999	ETP-A-099999-CAG4Y	$ 44.60	$ 38.80
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 75,000-99999	ETP-A-099999-CAG5Y	$ 55.76	$ 48.51
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 75,000-99999	ETP-A-099999-CAP1Y	$ 12.91	$ 11.23
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 75,000-99999	ETP-A-099999-CAP2Y	$ 24.14	$ 21.00
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 75,000-99999	ETP-A-099999-CAP3Y	$ 34.86	$ 30.33
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 75,000-99999	ETP-A-099999-CAP4Y	$ 46.48	$ 40.44
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 75,000-99999	ETP-A-099999-CAP5Y	$ 58.10	$ 50.55
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 75,000-99999	ETP-A-099999-PPL1Y	$ 4.76	$ 4.14
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 75,000-99999	ETP-A-099999-PPL2Y	$ 24.14	$ 21.00
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 75,000-99999	ETP-A-099999-PPL3Y	$ 34.86	$ 30.33
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 75,000-99999	ETP-A-099999-PPL4Y	$ 46.48	$ 40.44
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 75,000-99999	ETP-A-099999-PPL5Y	$ 58.10	$ 50.55
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 75,000-99999	ETP-A-099999-PTM1Y	$ 8.22	$ 7.15
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 75,000-99999	ETP-A-099999-PTM2Y	$ 23.16	$ 20.15
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 75,000-99999	ETP-A-099999-PTM3Y	$ 33.45	$ 29.10
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 75,000-99999	ETP-A-099999-PTM4Y	$ 44.60	$ 38.80
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 75,000-99999	ETP-A-099999-PTM5Y	$ 55.76	$ 48.51

FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 75,000-99999	ETP-A-099999-USG1Y	$ 12.39	$ 10.78
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 75,000-99999	ETP-A-099999-USG2Y	$ 23.16	$ 20.15
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 75,000-99999	ETP-A-099999-USG3Y	$ 33.45	$ 29.10
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 75,000-99999	ETP-A-099999-USG4Y	$ 44.60	$ 38.80
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 75,000-99999	ETP-A-099999-USG5Y	$ 55.76	$ 48.51
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 75,000-99999	ETP-A-099999-USP1Y	$ 12.91	$ 11.23
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 75,000-99999	ETP-A-099999-USP2Y	$ 24.14	$ 21.00
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 75,000-99999	ETP-A-099999-USP3Y	$ 34.86	$ 30.33
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 75,000-99999	ETP-A-099999-USP4Y	$ 46.48	$ 40.44
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 75,000-99999	ETP-A-099999-USP5Y	$ 58.10	$ 50.55
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 100,000-199999	ETP-A-199999-CAG1Y	$ 10.78	$ 9.38
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 100,000-199999	ETP-A-199999-CAG2Y	$ 20.15	$ 17.53
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 100,000-199999	ETP-A-199999-CAG3Y	$ 29.11	$ 25.33
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 100,000-199999	ETP-A-199999-CAG4Y	$ 38.81	$ 33.76
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 100,000-199999	ETP-A-199999-CAG5Y	$ 48.51	$ 42.20
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 100,000-199999	ETP-A-199999-CAP1Y	$ 11.23	$ 9.77
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 100,000-199999	ETP-A-199999-CAP2Y	$ 21.01	$ 18.28
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 100,000-199999	ETP-A-199999-CAP3Y	$ 30.32	$ 26.38
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 100,000-199999	ETP-A-199999-CAP4Y	$ 40.43	$ 35.17
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 100,000-199999	ETP-A-199999-CAP5Y	$ 50.54	$ 43.97
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 100,000-199999	ETP-A-199999-PPL1Y	$ 3.50	$ 3.05
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 100,000-199999	ETP-A-199999-PPL2Y	$ 21.09	$ 18.35
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 100,000-199999	ETP-A-199999-PPL3Y	$ 30.48	$ 26.52
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 100,000-199999	ETP-A-199999-PPL4Y	$ 40.64	$ 35.36
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 100,000-199999	ETP-A-199999-PPL5Y	$ 50.81	$ 44.20
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 100,000-199999	ETP-A-199999-PTM1Y	$ 6.58	$ 5.72
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 100,000-199999	ETP-A-199999-PTM2Y	$ 20.25	$ 17.62
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 100,000-199999	ETP-A-199999-PTM3Y	$ 29.24	$ 25.44
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 100,000-199999	ETP-A-199999-PTM4Y	$ 38.99	$ 33.92
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 100,000-199999	ETP-A-199999-PTM5Y	$ 48.74	$ 42.40
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 100,000-199999	ETP-A-199999-USG1Y	$ 10.78	$ 9.38
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 100,000-199999	ETP-A-199999-USG2Y	$ 20.15	$ 17.53
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 100,000-199999	ETP-A-199999-USG3Y	$ 29.11	$ 25.33
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 100,000-199999	ETP-A-199999-USG4Y	$ 38.81	$ 33.76
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 100,000-199999	ETP-A-199999-USG5Y	$ 48.51	$ 42.20
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 100,000-199999	ETP-A-199999-USP1Y	$ 11.23	$ 9.77
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 100,000-199999	ETP-A-199999-USP2Y	$ 21.01	$ 18.28
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 100,000-199999	ETP-A-199999-USP3Y	$ 30.32	$ 26.38
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 100,000-199999	ETP-A-199999-USP4Y	$ 40.43	$ 35.17
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 100,000-199999	ETP-A-199999-USP5Y	$ 50.54	$ 43.97
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 1 Year 200,000+	ETP-A-200000+CAG1Y	$ 10.42	$ 9.07
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 2 Year 200,000+	ETP-A-200000+CAG2Y	$ 19.49	$ 16.96
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 3 Year 200,000+	ETP-A-200000+CAG3Y	$ 28.13	$ 24.47
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 4 Year 200,000+	ETP-A-200000+CAG4Y	$ 37.51	$ 32.63
FireEye	AV/AS Add-on for ETP Cloud & Gov CA 5 Year 200,000+	ETP-A-200000+CAG5Y	$ 46.89	$ 40.79
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 200,000+	ETP-A-200000+CAP1Y	$ 10.86	$ 9.45
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 200,000+	ETP-A-200000+CAP2Y	$ 20.30	$ 17.66
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 200,000+	ETP-A-200000+CAP3Y	$ 29.32	$ 25.51
FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 200,000+	ETP-A-200000+CAP4Y	$ 39.10	$ 34.02

FireEye	AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 200,000+	ETP-A-200000+CAP5Y	$ 48.87	$ 42.52
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 200,000+	ETP-A-200000+PPL1Y	$ 3.13	$ 2.72
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 200,000+	ETP-A-200000+PPL2Y	$ 20.32	$ 17.68
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 200,000+	ETP-A-200000+PPL3Y	$ 29.38	$ 25.56
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 200,000+	ETP-A-200000+PPL4Y	$ 39.17	$ 34.08
FireEye	AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 200,000+	ETP-A-200000+PPL5Y	$ 48.96	$ 42.60
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 200,000+	ETP-A-200000+PTM1Y	$ 6.04	$ 5.25
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 200,000+	ETP-A-200000+PTM2Y	$ 19.51	$ 16.97
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 200,000+	ETP-A-200000+PTM3Y	$ 28.16	$ 24.50
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 200,000+	ETP-A-200000+PTM4Y	$ 37.55	$ 32.67
FireEye	AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 200,000+	ETP-A-200000+PTM5Y	$ 46.94	$ 40.84
FireEye	AV/AS Add-on for ETP Cloud & Gov US 1 Year 200,000+	ETP-A-200000+USG1Y	$ 10.42	$ 9.07
FireEye	AV/AS Add-on for ETP Cloud & Gov US 2 Year 200,000+	ETP-A-200000+USG2Y	$ 19.49	$ 16.96
FireEye	AV/AS Add-on for ETP Cloud & Gov US 3 Year 200,000+	ETP-A-200000+USG3Y	$ 28.13	$ 24.47
FireEye	AV/AS Add-on for ETP Cloud & Gov US 4 Year 200,000+	ETP-A-200000+USG4Y	$ 37.51	$ 32.63
FireEye	AV/AS Add-on for ETP Cloud & Gov US 5 Year 200,000+	ETP-A-200000+USG5Y	$ 46.89	$ 40.79
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 200,000+	ETP-A-200000+USP1Y	$ 10.86	$ 9.45
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 200,000+	ETP-A-200000+USP2Y	$ 20.30	$ 17.66
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 200,000+	ETP-A-200000+USP3Y	$ 29.32	$ 25.51
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 200,000+	ETP-A-200000+USP4Y	$ 39.10	$ 34.02
FireEye	AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 200,000+	ETP-A-200000+USP5Y	$ 48.87	$ 42.52
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 1-249	ETP-C-000249-CAG1Y	$ 84.56	$ 73.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 1-249	ETP-C-000249-CAG2Y	$ 169.12	$ 147.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 1-249	ETP-C-000249-CAG3Y	$ 228.31	$ 198.63
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 1-249	ETP-C-000249-CAG4Y	$ 304.42	$ 264.85
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 1-249	ETP-C-000249-CAG5Y	$ 380.52	$ 331.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 1-249	ETP-C-000249-CAP1Y	$ 88.14	$ 76.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 1-249	ETP-C-000249-CAP2Y	$ 176.28	$ 153.36
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 1-249	ETP-C-000249-CAP3Y	$ 237.98	$ 207.04
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 1-249	ETP-C-000249-CAP4Y	$ 317.30	$ 276.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 1-249	ETP-C-000249-CAP5Y	$ 396.63	$ 345.07
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 1-249	ETP-C-000249-PPL1Y	$ 88.14	$ 76.68
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 1-249	ETP-C-000249-PPL2Y	$ 176.28	$ 153.36
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 1-249	ETP-C-000249-PPL3Y	$ 237.98	$ 207.04
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 1-249	ETP-C-000249-PPL4Y	$ 317.30	$ 276.05
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 1-249	ETP-C-000249-PPL5Y	$ 396.63	$ 345.07
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 1-249	ETP-C-000249-PTM1Y	$ 84.56	$ 73.57
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 1-249	ETP-C-000249-PTM2Y	$ 169.12	$ 147.13
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 1-249	ETP-C-000249-PTM3Y	$ 228.31	$ 198.63
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 1-249	ETP-C-000249-PTM4Y	$ 304.42	$ 264.85
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 1-249	ETP-C-000249-PTM5Y	$ 380.52	$ 331.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 1-249	ETP-C-000249-USG1Y	$ 84.56	$ 73.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 1-249	ETP-C-000249-USG2Y	$ 169.12	$ 147.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 1-249	ETP-C-000249-USG3Y	$ 228.31	$ 198.63
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 1-249	ETP-C-000249-USG4Y	$ 304.42	$ 264.85
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 1-249	ETP-C-000249-USG5Y	$ 380.52	$ 331.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 1-249	ETP-C-000249-USP1Y	$ 88.14	$ 76.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 1-249	ETP-C-000249-USP2Y	$ 176.28	$ 153.36
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 1-249	ETP-C-000249-USP3Y	$ 237.98	$ 207.04

FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 1-249	ETP-C-000249-USP4Y	$ 317.30	$ 276.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 1-249	ETP-C-000249-USP5Y	$ 396.63	$ 345.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 250-499	ETP-C-000499-CAG1Y	$ 69.82	$ 60.74
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 250-499	ETP-C-000499-CAG2Y	$ 139.64	$ 121.49
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 250-499	ETP-C-000499-CAG3Y	$ 188.51	$ 164.00
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 250-499	ETP-C-000499-CAG4Y	$ 251.35	$ 218.67
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 250-499	ETP-C-000499-CAG5Y	$ 314.19	$ 273.35
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 250-499	ETP-C-000499-CAP1Y	$ 72.78	$ 63.32
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 250-499	ETP-C-000499-CAP2Y	$ 145.56	$ 126.64
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 250-499	ETP-C-000499-CAP3Y	$ 196.51	$ 170.96
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 250-499	ETP-C-000499-CAP4Y	$ 262.01	$ 227.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 250-499	ETP-C-000499-CAP5Y	$ 327.51	$ 284.93
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 250-499	ETP-C-000499-PPL1Y	$ 72.78	$ 63.32
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 250-499	ETP-C-000499-PPL2Y	$ 145.56	$ 126.64
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 250-499	ETP-C-000499-PPL3Y	$ 196.51	$ 170.96
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 250-499	ETP-C-000499-PPL4Y	$ 262.01	$ 227.95
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 250-499	ETP-C-000499-PPL5Y	$ 327.51	$ 284.93
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 250-499	ETP-C-000499-PTM1Y	$ 69.82	$ 60.74
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 250-499	ETP-C-000499-PTM2Y	$ 139.64	$ 121.49
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 250-499	ETP-C-000499-PTM3Y	$ 188.51	$ 164.00
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 250-499	ETP-C-000499-PTM4Y	$ 251.35	$ 218.67
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 250-499	ETP-C-000499-PTM5Y	$ 314.19	$ 273.35
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 250-499	ETP-C-000499-USG1Y	$ 69.82	$ 60.74
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 250-499	ETP-C-000499-USG2Y	$ 139.64	$ 121.49
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 250-499	ETP-C-000499-USG3Y	$ 188.51	$ 164.00
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 250-499	ETP-C-000499-USG4Y	$ 251.35	$ 218.67
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 250-499	ETP-C-000499-USG5Y	$ 314.19	$ 273.35
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 250-499	ETP-C-000499-USP1Y	$ 72.78	$ 63.32
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 250-499	ETP-C-000499-USP2Y	$ 145.56	$ 126.64
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 250-499	ETP-C-000499-USP3Y	$ 196.51	$ 170.96
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 250-499	ETP-C-000499-USP4Y	$ 262.01	$ 227.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 250-499	ETP-C-000499-USP5Y	$ 327.51	$ 284.93
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 500-749	ETP-C-000749-CAG1Y	$ 59.89	$ 52.10
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 500-749	ETP-C-000749-CAG2Y	$ 119.78	$ 104.21
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 500-749	ETP-C-000749-CAG3Y	$ 161.70	$ 140.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 500-749	ETP-C-000749-CAG4Y	$ 215.60	$ 187.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 500-749	ETP-C-000749-CAG5Y	$ 269.51	$ 234.47
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 500-749	ETP-C-000749-CAP1Y	$ 62.43	$ 54.31
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 500-749	ETP-C-000749-CAP2Y	$ 124.86	$ 108.63
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 500-749	ETP-C-000749-CAP3Y	$ 168.56	$ 146.65
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 500-749	ETP-C-000749-CAP4Y	$ 224.75	$ 195.53
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 500-749	ETP-C-000749-CAP5Y	$ 280.94	$ 244.42
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 500-749	ETP-C-000749-PPL1Y	$ 62.43	$ 54.31
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 500-749	ETP-C-000749-PPL2Y	$ 124.86	$ 108.63
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 500-749	ETP-C-000749-PPL3Y	$ 168.56	$ 146.65
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 500-749	ETP-C-000749-PPL4Y	$ 224.75	$ 195.53
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 500-749	ETP-C-000749-PPL5Y	$ 280.94	$ 244.42
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 500-749	ETP-C-000749-PTM1Y	$ 59.89	$ 52.10
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 500-749	ETP-C-000749-PTM2Y	$ 119.78	$ 104.21

FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 500-749	ETP-C-000749-PTM3Y	$ 161.70	$ 140.68
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 500-749	ETP-C-000749-PTM4Y	$ 215.60	$ 187.57
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 500-749	ETP-C-000749-PTM5Y	$ 269.51	$ 234.47
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 500-749	ETP-C-000749-USG1Y	$ 59.89	$ 52.10
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 500-749	ETP-C-000749-USG2Y	$ 119.78	$ 104.21
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 500-749	ETP-C-000749-USG3Y	$ 161.70	$ 140.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 500-749	ETP-C-000749-USG4Y	$ 215.60	$ 187.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 500-749	ETP-C-000749-USG5Y	$ 269.51	$ 234.47
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 500-749	ETP-C-000749-USP1Y	$ 62.43	$ 54.31
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 500-749	ETP-C-000749-USP2Y	$ 124.86	$ 108.63
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 500-749	ETP-C-000749-USP3Y	$ 168.56	$ 146.65
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 500-749	ETP-C-000749-USP4Y	$ 224.75	$ 195.53
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 500-749	ETP-C-000749-USP5Y	$ 280.94	$ 244.42
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 750-999	ETP-C-000999-CAG1Y	$ 50.30	$ 43.76
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 750-999	ETP-C-000999-CAG2Y	$ 100.60	$ 87.52
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 750-999	ETP-C-000999-CAG3Y	$ 135.81	$ 118.15
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 750-999	ETP-C-000999-CAG4Y	$ 181.08	$ 157.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 750-999	ETP-C-000999-CAG5Y	$ 226.35	$ 196.92
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 750-999	ETP-C-000999-CAP1Y	$ 52.43	$ 45.61
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 750-999	ETP-C-000999-CAP2Y	$ 104.86	$ 91.23
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 750-999	ETP-C-000999-CAP3Y	$ 141.56	$ 123.16
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 750-999	ETP-C-000999-CAP4Y	$ 188.75	$ 164.21
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 750-999	ETP-C-000999-CAP5Y	$ 235.94	$ 205.27
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 750-999	ETP-C-000999-PPL1Y	$ 52.43	$ 45.61
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 750-999	ETP-C-000999-PPL2Y	$ 104.86	$ 91.23
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 750-999	ETP-C-000999-PPL3Y	$ 141.56	$ 123.16
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 750-999	ETP-C-000999-PPL4Y	$ 188.75	$ 164.21
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 750-999	ETP-C-000999-PPL5Y	$ 235.94	$ 205.27
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 750-999	ETP-C-000999-PTM1Y	$ 50.30	$ 43.76
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 750-999	ETP-C-000999-PTM2Y	$ 100.60	$ 87.52
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 750-999	ETP-C-000999-PTM3Y	$ 135.81	$ 118.15
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 750-999	ETP-C-000999-PTM4Y	$ 181.08	$ 157.54
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 750-999	ETP-C-000999-PTM5Y	$ 226.35	$ 196.92
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 750-999	ETP-C-000999-USG1Y	$ 50.30	$ 43.76
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 750-999	ETP-C-000999-USG2Y	$ 100.60	$ 87.52
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 750-999	ETP-C-000999-USG3Y	$ 135.81	$ 118.15
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 750-999	ETP-C-000999-USG4Y	$ 181.08	$ 157.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 750-999	ETP-C-000999-USG5Y	$ 226.35	$ 196.92
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 750-999	ETP-C-000999-USP1Y	$ 52.43	$ 45.61
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 750-999	ETP-C-000999-USP2Y	$ 104.86	$ 91.23
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 750-999	ETP-C-000999-USP3Y	$ 141.56	$ 123.16
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 750-999	ETP-C-000999-USP4Y	$ 188.75	$ 164.21
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 750-999	ETP-C-000999-USP5Y	$ 235.94	$ 205.27
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 1,000-1999	ETP-C-001999-CAG1Y	$ 45.62	$ 39.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 1,000-1999	ETP-C-001999-CAG2Y	$ 91.24	$ 79.38
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 1,000-1999	ETP-C-001999-CAG3Y	$ 123.17	$ 107.16
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 1,000-1999	ETP-C-001999-CAG4Y	$ 164.23	$ 142.88
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 1,000-1999	ETP-C-001999-CAG5Y	$ 205.29	$ 178.60
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 1,000-1999	ETP-C-001999-CAP1Y	$ 47.55	$ 41.37

FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 1,000-1999	ETP-C-001999-CAP2Y	$ 95.10	$ 82.74
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 1,000-1999	ETP-C-001999-CAP3Y	$ 128.39	$ 111.70
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 1,000-1999	ETP-C-001999-CAP4Y	$ 171.18	$ 148.93
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 1,000-1999	ETP-C-001999-CAP5Y	$ 213.98	$ 186.16
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 1,000-1999	ETP-C-001999-PPL1Y	$ 47.55	$ 41.37
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 1,000-1999	ETP-C-001999-PPL2Y	$ 95.10	$ 82.74
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 1,000-1999	ETP-C-001999-PPL3Y	$ 128.39	$ 111.70
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 1,000-1999	ETP-C-001999-PPL4Y	$ 171.18	$ 148.93
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 1,000-1999	ETP-C-001999-PPL5Y	$ 213.98	$ 186.16
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 1,000-1999	ETP-C-001999-PTM1Y	$ 45.62	$ 39.69
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 1,000-1999	ETP-C-001999-PTM2Y	$ 91.24	$ 79.38
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 1,000-1999	ETP-C-001999-PTM3Y	$ 123.17	$ 107.16
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 1,000-1999	ETP-C-001999-PTM4Y	$ 164.23	$ 142.88
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 1,000-1999	ETP-C-001999-PTM5Y	$ 205.29	$ 178.60
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 1,000-1999	ETP-C-001999-USG1Y	$ 45.62	$ 39.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 1,000-1999	ETP-C-001999-USG2Y	$ 91.24	$ 79.38
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 1,000-1999	ETP-C-001999-USG3Y	$ 123.17	$ 107.16
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 1,000-1999	ETP-C-001999-USG4Y	$ 164.23	$ 142.88
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 1,000-1999	ETP-C-001999-USG5Y	$ 205.29	$ 178.60
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 1,000-1999	ETP-C-001999-USP1Y	$ 47.55	$ 41.37
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 1,000-1999	ETP-C-001999-USP2Y	$ 95.10	$ 82.74
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 1,000-1999	ETP-C-001999-USP3Y	$ 128.39	$ 111.70
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 1,000-1999	ETP-C-001999-USP4Y	$ 171.18	$ 148.93
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 1,000-1999	ETP-C-001999-USP5Y	$ 213.98	$ 186.16
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 2,000-4999	ETP-C-004999-CAG1Y	$ 41.53	$ 36.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 2,000-4999	ETP-C-004999-CAG2Y	$ 83.06	$ 72.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 2,000-4999	ETP-C-004999-CAG3Y	$ 112.13	$ 97.55
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 2,000-4999	ETP-C-004999-CAG4Y	$ 149.51	$ 130.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 2,000-4999	ETP-C-004999-CAG5Y	$ 186.89	$ 162.59
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 2,000-4999	ETP-C-004999-CAP1Y	$ 43.29	$ 37.66
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 2,000-4999	ETP-C-004999-CAP2Y	$ 86.58	$ 75.32
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 2,000-4999	ETP-C-004999-CAP3Y	$ 116.88	$ 101.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 2,000-4999	ETP-C-004999-CAP4Y	$ 155.84	$ 135.58
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 2,000-4999	ETP-C-004999-CAP5Y	$ 194.81	$ 169.48
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 2,000-4999	ETP-C-004999-PPL1Y	$ 43.29	$ 37.66
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 2,000-4999	ETP-C-004999-PPL2Y	$ 86.58	$ 75.32
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 2,000-4999	ETP-C-004999-PPL3Y	$ 116.88	$ 101.69
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 2,000-4999	ETP-C-004999-PPL4Y	$ 155.84	$ 135.58
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 2,000-4999	ETP-C-004999-PPL5Y	$ 194.81	$ 169.48
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 2,000-4999	ETP-C-004999-PTM1Y	$ 41.53	$ 36.13
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 2,000-4999	ETP-C-004999-PTM2Y	$ 83.06	$ 72.26
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 2,000-4999	ETP-C-004999-PTM3Y	$ 112.13	$ 97.55
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 2,000-4999	ETP-C-004999-PTM4Y	$ 149.51	$ 130.07
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 2,000-4999	ETP-C-004999-PTM5Y	$ 186.89	$ 162.59
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 2,000-4999	ETP-C-004999-USG1Y	$ 41.53	$ 36.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 2,000-4999	ETP-C-004999-USG2Y	$ 83.06	$ 72.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 2,000-4999	ETP-C-004999-USG3Y	$ 112.13	$ 97.55
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 2,000-4999	ETP-C-004999-USG4Y	$ 149.51	$ 130.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 2,000-4999	ETP-C-004999-USG5Y	$ 186.89	$ 162.59

FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 2,000-4999	ETP-C-004999-USP1Y	$ 43.29	$ 37.66
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 2,000-4999	ETP-C-004999-USP2Y	$ 86.58	$ 75.32
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 2,000-4999	ETP-C-004999-USP3Y	$ 116.88	$ 101.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 2,000-4999	ETP-C-004999-USP4Y	$ 155.84	$ 135.58
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 2,000-4999	ETP-C-004999-USP5Y	$ 194.81	$ 169.48
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 5,000-9999	ETP-C-009999-CAG1Y	$ 39.22	$ 34.12
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 5,000-9999	ETP-C-009999-CAG2Y	$ 78.44	$ 68.24
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 5,000-9999	ETP-C-009999-CAG3Y	$ 105.89	$ 92.12
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 5,000-9999	ETP-C-009999-CAG4Y	$ 141.19	$ 122.84
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 5,000-9999	ETP-C-009999-CAG5Y	$ 176.49	$ 153.55
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 5,000-9999	ETP-C-009999-CAP1Y	$ 40.88	$ 35.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 5,000-9999	ETP-C-009999-CAP2Y	$ 81.76	$ 71.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 5,000-9999	ETP-C-009999-CAP3Y	$ 110.38	$ 96.03
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 5,000-9999	ETP-C-009999-CAP4Y	$ 147.17	$ 128.04
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 5,000-9999	ETP-C-009999-CAP5Y	$ 183.96	$ 160.05
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 5,000-9999	ETP-C-009999-PPL1Y	$ 40.88	$ 35.57
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 5,000-9999	ETP-C-009999-PPL2Y	$ 81.76	$ 71.13
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 5,000-9999	ETP-C-009999-PPL3Y	$ 110.38	$ 96.03
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 5,000-9999	ETP-C-009999-PPL4Y	$ 147.17	$ 128.04
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 5,000-9999	ETP-C-009999-PPL5Y	$ 183.96	$ 160.05
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 5,000-9999	ETP-C-009999-PTM1Y	$ 39.22	$ 34.12
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 5,000-9999	ETP-C-009999-PTM2Y	$ 78.44	$ 68.24
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 5,000-9999	ETP-C-009999-PTM3Y	$ 105.89	$ 92.12
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 5,000-9999	ETP-C-009999-PTM4Y	$ 141.19	$ 122.84
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 5,000-9999	ETP-C-009999-PTM5Y	$ 176.49	$ 153.55
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 5,000-9999	ETP-C-009999-USG1Y	$ 39.22	$ 34.12
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 5,000-9999	ETP-C-009999-USG2Y	$ 78.44	$ 68.24
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 5,000-9999	ETP-C-009999-USG3Y	$ 105.89	$ 92.12
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 5,000-9999	ETP-C-009999-USG4Y	$ 141.19	$ 122.84
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 5,000-9999	ETP-C-009999-USG5Y	$ 176.49	$ 153.55
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 5,000-9999	ETP-C-009999-USP1Y	$ 40.88	$ 35.57
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 5,000-9999	ETP-C-009999-USP2Y	$ 81.76	$ 71.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 5,000-9999	ETP-C-009999-USP3Y	$ 110.38	$ 96.03
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 5,000-9999	ETP-C-009999-USP4Y	$ 147.17	$ 128.04
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 5,000-9999	ETP-C-009999-USP5Y	$ 183.96	$ 160.05
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 10,000-19999	ETP-C-019999-CAG1Y	$ 32.81	$ 28.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 10,000-19999	ETP-C-019999-CAG2Y	$ 65.62	$ 57.09
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 10,000-19999	ETP-C-019999-CAG3Y	$ 88.59	$ 77.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 10,000-19999	ETP-C-019999-CAG4Y	$ 118.12	$ 102.76
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 10,000-19999	ETP-C-019999-CAG5Y	$ 147.65	$ 128.46
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 10,000-19999	ETP-C-019999-CAP1Y	$ 34.20	$ 29.75
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 10,000-19999	ETP-C-019999-CAP2Y	$ 68.40	$ 59.51
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 10,000-19999	ETP-C-019999-CAP3Y	$ 92.34	$ 80.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 10,000-19999	ETP-C-019999-CAP4Y	$ 123.12	$ 107.11
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 10,000-19999	ETP-C-019999-CAP5Y	$ 153.90	$ 133.89
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 10,000-19999	ETP-C-019999-PPL1Y	$ 34.20	$ 29.75
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 10,000-19999	ETP-C-019999-PPL2Y	$ 68.40	$ 59.51
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 10,000-19999	ETP-C-019999-PPL3Y	$ 92.34	$ 80.34
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 10,000-19999	ETP-C-019999-PPL4Y	$ 123.12	$ 107.11

FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 10,000-19999	ETP-C-019999-PPL5Y	$ 153.90	$ 133.89
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 10,000-19999	ETP-C-019999-PTM1Y	$ 32.81	$ 28.54
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 10,000-19999	ETP-C-019999-PTM2Y	$ 65.62	$ 57.09
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 10,000-19999	ETP-C-019999-PTM3Y	$ 88.59	$ 77.07
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 10,000-19999	ETP-C-019999-PTM4Y	$ 118.12	$ 102.76
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 10,000-19999	ETP-C-019999-PTM5Y	$ 147.65	$ 128.46
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 10,000-19999	ETP-C-019999-USG1Y	$ 32.81	$ 28.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 10,000-19999	ETP-C-019999-USG2Y	$ 65.62	$ 57.09
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 10,000-19999	ETP-C-019999-USG3Y	$ 88.59	$ 77.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 10,000-19999	ETP-C-019999-USG4Y	$ 118.12	$ 102.76
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 10,000-19999	ETP-C-019999-USG5Y	$ 147.65	$ 128.46
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 10,000-19999	ETP-C-019999-USP1Y	$ 34.20	$ 29.75
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 10,000-19999	ETP-C-019999-USP2Y	$ 68.40	$ 59.51
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 10,000-19999	ETP-C-019999-USP3Y	$ 92.34	$ 80.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 10,000-19999	ETP-C-019999-USP4Y	$ 123.12	$ 107.11
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 10,000-19999	ETP-C-019999-USP5Y	$ 153.90	$ 133.89
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 20,000-49999	ETP-C-049999-CAG1Y	$ 30.10	$ 26.19
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 20,000-49999	ETP-C-049999-CAG2Y	$ 60.20	$ 52.37
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 20,000-49999	ETP-C-049999-CAG3Y	$ 81.27	$ 70.70
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 20,000-49999	ETP-C-049999-CAG4Y	$ 108.36	$ 94.27
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 20,000-49999	ETP-C-049999-CAG5Y	$ 135.45	$ 117.84
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 20,000-49999	ETP-C-049999-CAP1Y	$ 31.38	$ 27.30
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 20,000-49999	ETP-C-049999-CAP2Y	$ 62.76	$ 54.60
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 20,000-49999	ETP-C-049999-CAP3Y	$ 84.73	$ 73.72
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 20,000-49999	ETP-C-049999-CAP4Y	$ 112.97	$ 98.28
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 20,000-49999	ETP-C-049999-CAP5Y	$ 141.21	$ 122.85
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 20,000-49999	ETP-C-049999-PPL1Y	$ 31.38	$ 27.30
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 20,000-49999	ETP-C-049999-PPL2Y	$ 62.76	$ 54.60
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 20,000-49999	ETP-C-049999-PPL3Y	$ 84.73	$ 73.72
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 20,000-49999	ETP-C-049999-PPL4Y	$ 112.97	$ 98.28
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 20,000-49999	ETP-C-049999-PPL5Y	$ 141.21	$ 122.85
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 20,000-49999	ETP-C-049999-PTM1Y	$ 30.10	$ 26.19
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 20,000-49999	ETP-C-049999-PTM2Y	$ 60.20	$ 52.37
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 20,000-49999	ETP-C-049999-PTM3Y	$ 81.27	$ 70.70
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 20,000-49999	ETP-C-049999-PTM4Y	$ 108.36	$ 94.27
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 20,000-49999	ETP-C-049999-PTM5Y	$ 135.45	$ 117.84
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 20,000-49999	ETP-C-049999-USG1Y	$ 30.10	$ 26.19
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 20,000-49999	ETP-C-049999-USG2Y	$ 60.20	$ 52.37
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 20,000-49999	ETP-C-049999-USG3Y	$ 81.27	$ 70.70
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 20,000-49999	ETP-C-049999-USG4Y	$ 108.36	$ 94.27
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 20,000-49999	ETP-C-049999-USG5Y	$ 135.45	$ 117.84
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 20,000-49999	ETP-C-049999-USP1Y	$ 31.38	$ 27.30
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 20,000-49999	ETP-C-049999-USP2Y	$ 62.76	$ 54.60
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 20,000-49999	ETP-C-049999-USP3Y	$ 84.73	$ 73.72
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 20,000-49999	ETP-C-049999-USP4Y	$ 112.97	$ 98.28
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 20,000-49999	ETP-C-049999-USP5Y	$ 141.21	$ 122.85
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 50,000-74999	ETP-C-074999-CAG1Y	$ 27.55	$ 23.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 50,000-74999	ETP-C-074999-CAG2Y	$ 55.10	$ 47.94
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 50,000-74999	ETP-C-074999-CAG3Y	$ 74.39	$ 64.72

FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 50,000-74999	ETP-C-074999-CAG4Y	$ 99.18	$ 86.29
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 50,000-74999	ETP-C-074999-CAG5Y	$ 123.98	$ 107.86
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 50,000-74999	ETP-C-074999-CAP1Y	$ 28.72	$ 24.99
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 50,000-74999	ETP-C-074999-CAP2Y	$ 57.44	$ 49.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 50,000-74999	ETP-C-074999-CAP3Y	$ 77.54	$ 67.46
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 50,000-74999	ETP-C-074999-CAP4Y	$ 103.39	$ 89.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 50,000-74999	ETP-C-074999-CAP5Y	$ 129.24	$ 112.44
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 50,000-74999	ETP-C-074999-PPL1Y	$ 28.72	$ 24.99
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 50,000-74999	ETP-C-074999-PPL2Y	$ 57.44	$ 49.97
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 50,000-74999	ETP-C-074999-PPL3Y	$ 77.54	$ 67.46
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 50,000-74999	ETP-C-074999-PPL4Y	$ 103.39	$ 89.95
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 50,000-74999	ETP-C-074999-PPL5Y	$ 129.24	$ 112.44
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 50,000-74999	ETP-C-074999-PTM1Y	$ 27.55	$ 23.97
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 50,000-74999	ETP-C-074999-PTM2Y	$ 55.10	$ 47.94
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 50,000-74999	ETP-C-074999-PTM3Y	$ 74.39	$ 64.72
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 50,000-74999	ETP-C-074999-PTM4Y	$ 99.18	$ 86.29
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 50,000-74999	ETP-C-074999-PTM5Y	$ 123.98	$ 107.86
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 50,000-74999	ETP-C-074999-USG1Y	$ 27.55	$ 23.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 50,000-74999	ETP-C-074999-USG2Y	$ 55.10	$ 47.94
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 50,000-74999	ETP-C-074999-USG3Y	$ 74.39	$ 64.72
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 50,000-74999	ETP-C-074999-USG4Y	$ 99.18	$ 86.29
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 50,000-74999	ETP-C-074999-USG5Y	$ 123.98	$ 107.86
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 50,000-74999	ETP-C-074999-USP1Y	$ 28.72	$ 24.99
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 50,000-74999	ETP-C-074999-USP2Y	$ 57.44	$ 49.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 50,000-74999	ETP-C-074999-USP3Y	$ 77.54	$ 67.46
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 50,000-74999	ETP-C-074999-USP4Y	$ 103.39	$ 89.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 50,000-74999	ETP-C-074999-USP5Y	$ 129.24	$ 112.44
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 75,000-99999	ETP-C-099999-CAG1Y	$ 24.44	$ 21.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 75,000-99999	ETP-C-099999-CAG2Y	$ 48.88	$ 42.53
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 75,000-99999	ETP-C-099999-CAG3Y	$ 65.99	$ 57.41
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 75,000-99999	ETP-C-099999-CAG4Y	$ 87.98	$ 76.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 75,000-99999	ETP-C-099999-CAG5Y	$ 109.98	$ 95.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 75,000-99999	ETP-C-099999-CAP1Y	$ 25.48	$ 22.17
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 75,000-99999	ETP-C-099999-CAP2Y	$ 50.96	$ 44.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 75,000-99999	ETP-C-099999-CAP3Y	$ 68.80	$ 59.86
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 75,000-99999	ETP-C-099999-CAP4Y	$ 91.73	$ 79.81
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 75,000-99999	ETP-C-099999-CAP5Y	$ 114.66	$ 99.75
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 75,000-99999	ETP-C-099999-PPL1Y	$ 25.48	$ 22.17
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 75,000-99999	ETP-C-099999-PPL2Y	$ 50.96	$ 44.34
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 75,000-99999	ETP-C-099999-PPL3Y	$ 68.80	$ 59.86
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 75,000-99999	ETP-C-099999-PPL4Y	$ 91.73	$ 79.81
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 75,000-99999	ETP-C-099999-PPL5Y	$ 114.66	$ 99.75
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 75,000-99999	ETP-C-099999-PTM1Y	$ 24.44	$ 21.26
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 75,000-99999	ETP-C-099999-PTM2Y	$ 48.88	$ 42.53
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 75,000-99999	ETP-C-099999-PTM3Y	$ 65.99	$ 57.41
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 75,000-99999	ETP-C-099999-PTM4Y	$ 87.98	$ 76.54
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 75,000-99999	ETP-C-099999-PTM5Y	$ 109.98	$ 95.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 75,000-99999	ETP-C-099999-USG1Y	$ 24.44	$ 21.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 75,000-99999	ETP-C-099999-USG2Y	$ 48.88	$ 42.53

FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 75,000-99999	ETP-C-099999-USG3Y	$ 65.99	$ 57.41
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 75,000-99999	ETP-C-099999-USG4Y	$ 87.98	$ 76.54
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 75,000-99999	ETP-C-099999-USG5Y	$ 109.98	$ 95.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 75,000-99999	ETP-C-099999-USP1Y	$ 25.48	$ 22.17
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 75,000-99999	ETP-C-099999-USP2Y	$ 50.96	$ 44.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 75,000-99999	ETP-C-099999-USP3Y	$ 68.80	$ 59.86
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 75,000-99999	ETP-C-099999-USP4Y	$ 91.73	$ 79.81
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 75,000-99999	ETP-C-099999-USP5Y	$ 114.66	$ 99.75
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 100,000-199999	ETP-C-199999-CAG1Y	$ 20.84	$ 18.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 100,000-199999	ETP-C-199999-CAG2Y	$ 41.68	$ 36.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 100,000-199999	ETP-C-199999-CAG3Y	$ 56.27	$ 48.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 100,000-199999	ETP-C-199999-CAG4Y	$ 75.02	$ 65.27
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 100,000-199999	ETP-C-199999-CAG5Y	$ 93.78	$ 81.59
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 100,000-199999	ETP-C-199999-CAP1Y	$ 21.72	$ 18.90
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 100,000-199999	ETP-C-199999-CAP2Y	$ 43.44	$ 37.79
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 100,000-199999	ETP-C-199999-CAP3Y	$ 58.64	$ 51.02
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 100,000-199999	ETP-C-199999-CAP4Y	$ 78.19	$ 68.03
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 100,000-199999	ETP-C-199999-CAP5Y	$ 97.74	$ 85.03
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 100,000-199999	ETP-C-199999-PPL1Y	$ 21.72	$ 18.90
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 100,000-199999	ETP-C-199999-PPL2Y	$ 43.44	$ 37.79
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 100,000-199999	ETP-C-199999-PPL3Y	$ 58.64	$ 51.02
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 100,000-199999	ETP-C-199999-PPL4Y	$ 78.19	$ 68.03
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 100,000-199999	ETP-C-199999-PPL5Y	$ 97.74	$ 85.03
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 100,000-199999	ETP-C-199999-PTM1Y	$ 20.84	$ 18.13
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 100,000-199999	ETP-C-199999-PTM2Y	$ 41.68	$ 36.26
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 100,000-199999	ETP-C-199999-PTM3Y	$ 56.27	$ 48.95
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 100,000-199999	ETP-C-199999-PTM4Y	$ 75.02	$ 65.27
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 100,000-199999	ETP-C-199999-PTM5Y	$ 93.78	$ 81.59
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 100,000-199999	ETP-C-199999-USG1Y	$ 20.84	$ 18.13
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 100,000-199999	ETP-C-199999-USG2Y	$ 41.68	$ 36.26
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 100,000-199999	ETP-C-199999-USG3Y	$ 56.27	$ 48.95
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 100,000-199999	ETP-C-199999-USG4Y	$ 75.02	$ 65.27
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 100,000-199999	ETP-C-199999-USG5Y	$ 93.78	$ 81.59
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 100,000-199999	ETP-C-199999-USP1Y	$ 21.72	$ 18.90
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 100,000-199999	ETP-C-199999-USP2Y	$ 43.44	$ 37.79
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 100,000-199999	ETP-C-199999-USP3Y	$ 58.64	$ 51.02
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 100,000-199999	ETP-C-199999-USP4Y	$ 78.19	$ 68.03
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 100,000-199999	ETP-C-199999-USP5Y	$ 97.74	$ 85.03
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 200,000+	ETP-C-200000+CAG1Y	$ 19.50	$ 16.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 200,000+	ETP-C-200000+CAG2Y	$ 39.00	$ 33.93
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 200,000+	ETP-C-200000+CAG3Y	$ 52.65	$ 45.81
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 200,000+	ETP-C-200000+CAG4Y	$ 70.20	$ 61.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 200,000+	ETP-C-200000+CAG5Y	$ 87.75	$ 76.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 200,000+	ETP-C-200000+CAP1Y	$ 20.33	$ 17.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 200,000+	ETP-C-200000+CAP2Y	$ 40.66	$ 35.37
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 200,000+	ETP-C-200000+CAP3Y	$ 54.89	$ 47.75
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 200,000+	ETP-C-200000+CAP4Y	$ 73.19	$ 63.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 200,000+	ETP-C-200000+CAP5Y	$ 91.49	$ 79.60
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 200,000+	ETP-C-200000+PPL1Y	$ 20.33	$ 17.69

FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 200,000+	ETP-C-200000+PPL2Y	$ 40.66	$ 35.37
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 200,000+	ETP-C-200000+PPL3Y	$ 54.89	$ 47.75
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 200,000+	ETP-C-200000+PPL4Y	$ 73.19	$ 63.68
FireEye	Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 200,000+	ETP-C-200000+PPL5Y	$ 91.49	$ 79.60
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 200,000+	ETP-C-200000+PTM1Y	$ 19.50	$ 16.97
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 200,000+	ETP-C-200000+PTM2Y	$ 39.00	$ 33.93
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 200,000+	ETP-C-200000+PTM3Y	$ 52.65	$ 45.81
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 200,000+	ETP-C-200000+PTM4Y	$ 70.20	$ 61.07
FireEye	Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 200,000+	ETP-C-200000+PTM5Y	$ 87.75	$ 76.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 200,000+	ETP-C-200000+USG1Y	$ 19.50	$ 16.97
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 200,000+	ETP-C-200000+USG2Y	$ 39.00	$ 33.93
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 200,000+	ETP-C-200000+USG3Y	$ 52.65	$ 45.81
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 200,000+	ETP-C-200000+USG4Y	$ 70.20	$ 61.07
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 200,000+	ETP-C-200000+USG5Y	$ 87.75	$ 76.34
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 200,000+	ETP-C-200000+USP1Y	$ 20.33	$ 17.69
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 200,000+	ETP-C-200000+USP2Y	$ 40.66	$ 35.37
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 200,000+	ETP-C-200000+USP3Y	$ 54.89	$ 47.75
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 200,000+	ETP-C-200000+USP4Y	$ 73.19	$ 63.68
FireEye	Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 200,000+	ETP-C-200000+USP5Y	$ 91.49	$ 79.60
FireEye	EVL Email Threat Prevention	EVL-EC-ETP	$ -	$ -
FireEye	EVL AV/AS Add-on for ETP Cloud with AV/AS	EVL-EC-ETP-A	$ -	$ -
FireEye	EVL Email Threat Prevention Cloud with AV/AS	EVL-EC-ETP-C	$ -	$ -
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 1-249	RN-ETP-000249-PTM1Y	$ 58.32	$ 50.74
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 1-249	RN-ETP-000249-PTM3Y	$ 157.46	$ 136.99
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 1-249	RN-ETP-000249-PTM4Y	$ 209.95	$ 182.66
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 1-249	RN-ETP-000249-PTM5Y	$ 262.44	$ 228.32
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 1-249	RN-ETP-000249-USG1Y	$ 58.32	$ 50.74
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 1-249	RN-ETP-000249-USG3Y	$ 157.46	$ 136.99
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 1-249	RN-ETP-000249-USG4Y	$ 209.95	$ 182.66
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 1-249	RN-ETP-000249-USG5Y	$ 262.44	$ 228.32
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 250-499	RN-ETP-000499-PTM1Y	$ 48.15	$ 41.89
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 250-499	RN-ETP-000499-PTM3Y	$ 130.01	$ 113.11
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 250-499	RN-ETP-000499-PTM4Y	$ 173.34	$ 150.81
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 250-499	RN-ETP-000499-PTM5Y	$ 216.68	$ 188.51
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 250-499	RN-ETP-000499-USG1Y	$ 48.15	$ 41.89
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 250-499	RN-ETP-000499-USG3Y	$ 130.01	$ 113.11
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 250-499	RN-ETP-000499-USG4Y	$ 173.34	$ 150.81
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 250-499	RN-ETP-000499-USG5Y	$ 216.68	$ 188.51
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 500-749	RN-ETP-000749-PTM1Y	$ 41.30	$ 35.93
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 500-749	RN-ETP-000749-PTM3Y	$ 111.51	$ 97.01
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 500-749	RN-ETP-000749-PTM4Y	$ 148.68	$ 129.35
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 500-749	RN-ETP-000749-PTM5Y	$ 185.85	$ 161.69
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 500-749	RN-ETP-000749-USG1Y	$ 41.30	$ 35.93
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 500-749	RN-ETP-000749-USG3Y	$ 111.51	$ 97.01
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 500-749	RN-ETP-000749-USG4Y	$ 148.68	$ 129.35
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 500-749	RN-ETP-000749-USG5Y	$ 185.85	$ 161.69
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 750-999	RN-ETP-000999-PTM1Y	$ 34.69	$ 30.18
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 750-999	RN-ETP-000999-PTM3Y	$ 93.66	$ 81.48
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 750-999	RN-ETP-000999-PTM4Y	$ 124.88	$ 108.65

FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 750-999	RN-ETP-000999-PTM5Y	$ 156.11	$ 135.82
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 750-999	RN-ETP-000999-USG1Y	$ 34.69	$ 30.18
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 750-999	RN-ETP-000999-USG3Y	$ 93.66	$ 81.48
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 750-999	RN-ETP-000999-USG4Y	$ 124.88	$ 108.65
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 750-999	RN-ETP-000999-USG5Y	$ 156.11	$ 135.82
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 1,000-1999	RN-ETP-001999-PTM1Y	$ 31.46	$ 27.37
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 1,000-1999	RN-ETP-001999-PTM3Y	$ 84.94	$ 73.90
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 1,000-1999	RN-ETP-001999-PTM4Y	$ 113.26	$ 98.54
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 1,000-1999	RN-ETP-001999-PTM5Y	$ 141.57	$ 123.17
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 1,000-1999	RN-ETP-001999-USG1Y	$ 31.46	$ 27.37
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 1,000-1999	RN-ETP-001999-USG3Y	$ 84.94	$ 73.90
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 1,000-1999	RN-ETP-001999-USG4Y	$ 113.26	$ 98.54
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 1,000-1999	RN-ETP-001999-USG5Y	$ 141.57	$ 123.17
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 2,000-4999	RN-ETP-004999-PTM1Y	$ 28.64	$ 24.92
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 2,000-4999	RN-ETP-004999-PTM3Y	$ 77.33	$ 67.28
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 2,000-4999	RN-ETP-004999-PTM4Y	$ 103.10	$ 89.70
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 2,000-4999	RN-ETP-004999-PTM5Y	$ 128.88	$ 112.13
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 2,000-4999	RN-ETP-004999-USG1Y	$ 28.64	$ 24.92
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 2,000-4999	RN-ETP-004999-USG3Y	$ 77.33	$ 67.28
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 2,000-4999	RN-ETP-004999-USG4Y	$ 103.10	$ 89.70
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 2,000-4999	RN-ETP-004999-USG5Y	$ 128.88	$ 112.13
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 5,000-9999	RN-ETP-009999-PTM1Y	$ 25.51	$ 22.19
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 5,000-9999	RN-ETP-009999-PTM3Y	$ 68.88	$ 59.93
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 5,000-9999	RN-ETP-009999-PTM4Y	$ 91.84	$ 79.90
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 5,000-9999	RN-ETP-009999-PTM5Y	$ 114.80	$ 99.88
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 5,000-9999	RN-ETP-009999-USG1Y	$ 25.51	$ 22.19
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 5,000-9999	RN-ETP-009999-USG3Y	$ 68.88	$ 59.93
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 5,000-9999	RN-ETP-009999-USG4Y	$ 91.84	$ 79.90
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 5,000-9999	RN-ETP-009999-USG5Y	$ 114.80	$ 99.88
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 10,000-19999	RN-ETP-019999-PTM1Y	$ 22.02	$ 19.16
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 10,000-19999	RN-ETP-019999-PTM3Y	$ 59.45	$ 51.72
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 10,000-19999	RN-ETP-019999-PTM4Y	$ 79.27	$ 68.96
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 10,000-19999	RN-ETP-019999-PTM5Y	$ 99.09	$ 86.21
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 10,000-19999	RN-ETP-019999-USG1Y	$ 22.02	$ 19.16
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 10,000-19999	RN-ETP-019999-USG3Y	$ 59.45	$ 51.72
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 10,000-19999	RN-ETP-019999-USG4Y	$ 79.27	$ 68.96
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 10,000-19999	RN-ETP-019999-USG5Y	$ 99.09	$ 86.21
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 20,000-49999	RN-ETP-049999-PTM1Y	$ 20.76	$ 18.06
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 20,000-49999	RN-ETP-049999-PTM3Y	$ 56.05	$ 48.76
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 20,000-49999	RN-ETP-049999-PTM4Y	$ 74.74	$ 65.02
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 20,000-49999	RN-ETP-049999-PTM5Y	$ 93.42	$ 81.28
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 20,000-49999	RN-ETP-049999-USG1Y	$ 20.76	$ 18.06
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 20,000-49999	RN-ETP-049999-USG3Y	$ 56.05	$ 48.76
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 20,000-49999	RN-ETP-049999-USG4Y	$ 74.74	$ 65.02
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 20,000-49999	RN-ETP-049999-USG5Y	$ 93.42	$ 81.28
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 50,000-74999	RN-ETP-074999-PTM1Y	$ 18.75	$ 16.31
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 50,000-74999	RN-ETP-074999-PTM3Y	$ 50.63	$ 44.05
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 50,000-74999	RN-ETP-074999-PTM4Y	$ 67.50	$ 58.73
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 50,000-74999	RN-ETP-074999-PTM5Y	$ 84.38	$ 73.41

FireEye	Renewal-Email Threat Prevention, Government US 1 Year 50,000-74999	RN-ETP-074999-USG1Y	$ 18.75	$ 16.31
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 50,000-74999	RN-ETP-074999-USG3Y	$ 50.63	$ 44.05
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 50,000-74999	RN-ETP-074999-USG4Y	$ 67.50	$ 58.73
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 50,000-74999	RN-ETP-074999-USG5Y	$ 84.38	$ 73.41
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 75,000-99999	RN-ETP-099999-PTM1Y	$ 16.22	$ 14.11
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 75,000-99999	RN-ETP-099999-PTM3Y	$ 43.79	$ 38.10
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 75,000-99999	RN-ETP-099999-PTM4Y	$ 58.39	$ 50.80
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 75,000-99999	RN-ETP-099999-PTM5Y	$ 72.99	$ 63.50
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 75,000-99999	RN-ETP-099999-USG1Y	$ 16.22	$ 14.11
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 75,000-99999	RN-ETP-099999-USG3Y	$ 43.79	$ 38.10
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 75,000-99999	RN-ETP-099999-USG4Y	$ 58.39	$ 50.80
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 75,000-99999	RN-ETP-099999-USG5Y	$ 72.99	$ 63.50
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 100,000-199999	RN-ETP-199999-PTM1Y	$ 14.26	$ 12.41
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 100,000-199999	RN-ETP-199999-PTM3Y	$ 38.50	$ 33.50
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 100,000-199999	RN-ETP-199999-PTM4Y	$ 51.34	$ 44.67
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 100,000-199999	RN-ETP-199999-PTM5Y	$ 64.17	$ 55.83
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 100,000-199999	RN-ETP-199999-USG1Y	$ 14.26	$ 12.41
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 100,000-199999	RN-ETP-199999-USG3Y	$ 38.50	$ 33.50
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 100,000-199999	RN-ETP-199999-USG4Y	$ 51.34	$ 44.67
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 100,000-199999	RN-ETP-199999-USG5Y	$ 64.17	$ 55.83
FireEye	Renewal-Email Threat Prevention, Platinum Support 1 Year 200,000+	RN-ETP-200000+PTM1Y	$ 13.46	$ 11.71
FireEye	Renewal-Email Threat Prevention, Platinum Support 3 Year 200,000+	RN-ETP-200000+PTM3Y	$ 36.34	$ 31.62
FireEye	Renewal-Email Threat Prevention, Platinum Support 4 Year 200,000+	RN-ETP-200000+PTM4Y	$ 48.46	$ 42.16
FireEye	Renewal-Email Threat Prevention, Platinum Support 5 Year 200,000+	RN-ETP-200000+PTM5Y	$ 60.57	$ 52.70
FireEye	Renewal-Email Threat Prevention, Government US 1 Year 200,000+	RN-ETP-200000+USG1Y	$ 13.46	$ 11.71
FireEye	Renewal-Email Threat Prevention, Government US 3 Year 200,000+	RN-ETP-200000+USG3Y	$ 36.34	$ 31.62
FireEye	Renewal-Email Threat Prevention, Government US 4 Year 200,000+	RN-ETP-200000+USG4Y	$ 48.46	$ 42.16
FireEye	Renewal-Email Threat Prevention, Government US 5 Year 200,000+	RN-ETP-200000+USG5Y	$ 60.57	$ 52.70
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 1-249	RN-ETP-A-000249-CAG1Y	$ 71.95	$ 62.60
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 1-249	RN-ETP-A-000249-CAG2Y	$ 134.55	$ 117.06
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 1-249	RN-ETP-A-000249-CAG3Y	$ 194.27	$ 169.01
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 1-249	RN-ETP-A-000249-CAG4Y	$ 259.02	$ 225.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 1-249	RN-ETP-A-000249-CAG5Y	$ 323.78	$ 281.69
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 1-249	RN-ETP-A-000249-CAP1Y	$ 75.00	$ 65.25
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 1-249	RN-ETP-A-000249-CAP2Y	$ 140.25	$ 122.02
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 1-249	RN-ETP-A-000249-CAP3Y	$ 202.50	$ 176.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 1-249	RN-ETP-A-000249-CAP4Y	$ 270.00	$ 234.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 1-249	RN-ETP-A-000249-CAP5Y	$ 337.50	$ 293.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 1-249	RN-ETP-A-000249-PPL1Y	$ 13.62	$ 11.85
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 1-249	RN-ETP-A-000249-PPL2Y	$ 140.25	$ 122.02
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 1-249	RN-ETP-A-000249-PPL3Y	$ 202.50	$ 176.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 1-249	RN-ETP-A-000249-PPL4Y	$ 270.00	$ 234.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 1-249	RN-ETP-A-000249-PPL5Y	$ 337.50	$ 293.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 1-249	RN-ETP-A-000249-PTM1Y	$ 26.24	$ 22.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 1-249	RN-ETP-A-000249-PTM2Y	$ 134.55	$ 117.06
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 1-249	RN-ETP-A-000249-PTM3Y	$ 194.27	$ 169.01
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 1-249	RN-ETP-A-000249-PTM4Y	$ 259.02	$ 225.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 1-249	RN-ETP-A-000249-PTM5Y	$ 323.78	$ 281.69
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 1-249	RN-ETP-A-000249-USG1Y	$ 71.95	$ 62.60

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 1-249	RN-ETP-A-000249-USG2Y	$ 134.55	$ 117.06
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 1-249	RN-ETP-A-000249-USG3Y	$ 194.27	$ 169.01
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 1-249	RN-ETP-A-000249-USG4Y	$ 259.02	$ 225.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 1-249	RN-ETP-A-000249-USG5Y	$ 323.78	$ 281.69
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 1-249	RN-ETP-A-000249-USP1Y	$ 75.00	$ 65.25
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 1-249	RN-ETP-A-000249-USP2Y	$ 140.25	$ 122.02
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 1-249	RN-ETP-A-000249-USP3Y	$ 202.50	$ 176.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 1-249	RN-ETP-A-000249-USP4Y	$ 270.00	$ 234.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 1-249	RN-ETP-A-000249-USP5Y	$ 337.50	$ 293.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 250-499	RN-ETP-A-000499-CAG1Y	$ 35.96	$ 31.29
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 250-499	RN-ETP-A-000499-CAG2Y	$ 67.24	$ 58.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 250-499	RN-ETP-A-000499-CAG3Y	$ 97.09	$ 84.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 250-499	RN-ETP-A-000499-CAG4Y	$ 129.46	$ 112.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 250-499	RN-ETP-A-000499-CAG5Y	$ 161.82	$ 140.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 250-499	RN-ETP-A-000499-CAP1Y	$ 37.48	$ 32.61
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 250-499	RN-ETP-A-000499-CAP2Y	$ 70.09	$ 60.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 250-499	RN-ETP-A-000499-CAP3Y	$ 101.20	$ 88.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 250-499	RN-ETP-A-000499-CAP4Y	$ 134.93	$ 117.39
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 250-499	RN-ETP-A-000499-CAP5Y	$ 168.66	$ 146.73
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 250-499	RN-ETP-A-000499-PPL1Y	$ 11.26	$ 9.80
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 250-499	RN-ETP-A-000499-PPL2Y	$ 70.09	$ 60.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 250-499	RN-ETP-A-000499-PPL3Y	$ 101.20	$ 88.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 250-499	RN-ETP-A-000499-PPL4Y	$ 134.93	$ 117.39
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 250-499	RN-ETP-A-000499-PPL5Y	$ 168.66	$ 146.73
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 250-499	RN-ETP-A-000499-PTM1Y	$ 21.67	$ 18.85
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 250-499	RN-ETP-A-000499-PTM2Y	$ 67.24	$ 58.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 250-499	RN-ETP-A-000499-PTM3Y	$ 97.09	$ 84.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 250-499	RN-ETP-A-000499-PTM4Y	$ 129.46	$ 112.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 250-499	RN-ETP-A-000499-PTM5Y	$ 161.82	$ 140.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 250-499	RN-ETP-A-000499-USG1Y	$ 35.96	$ 31.29
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 250-499	RN-ETP-A-000499-USG2Y	$ 67.24	$ 58.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 250-499	RN-ETP-A-000499-USG3Y	$ 97.09	$ 84.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 250-499	RN-ETP-A-000499-USG4Y	$ 129.46	$ 112.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 250-499	RN-ETP-A-000499-USG5Y	$ 161.82	$ 140.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 250-499	RN-ETP-A-000499-USP1Y	$ 37.48	$ 32.61
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 250-499	RN-ETP-A-000499-USP2Y	$ 70.09	$ 60.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 250-499	RN-ETP-A-000499-USP3Y	$ 101.20	$ 88.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 250-499	RN-ETP-A-000499-USP4Y	$ 134.93	$ 117.39
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 250-499	RN-ETP-A-000499-USP5Y	$ 168.66	$ 146.73
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 500-749	RN-ETP-A-000749-CAG1Y	$ 29.76	$ 25.89
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 500-749	RN-ETP-A-000749-CAG2Y	$ 55.65	$ 48.42
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 500-749	RN-ETP-A-000749-CAG3Y	$ 80.35	$ 69.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 500-749	RN-ETP-A-000749-CAG4Y	$ 107.14	$ 93.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 500-749	RN-ETP-A-000749-CAG5Y	$ 133.92	$ 116.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 500-749	RN-ETP-A-000749-CAP1Y	$ 31.02	$ 26.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 500-749	RN-ETP-A-000749-CAP2Y	$ 58.00	$ 50.46
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 500-749	RN-ETP-A-000749-CAP3Y	$ 83.75	$ 72.86
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 500-749	RN-ETP-A-000749-CAP4Y	$ 111.67	$ 97.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 500-749	RN-ETP-A-000749-CAP5Y	$ 139.59	$ 121.44

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 500-749	RN-ETP-A-000749-PPL1Y	$ 9.66	$ 8.40
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 500-749	RN-ETP-A-000749-PPL2Y	$ 58.00	$ 50.46
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 500-749	RN-ETP-A-000749-PPL3Y	$ 83.75	$ 72.86
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 500-749	RN-ETP-A-000749-PPL4Y	$ 111.67	$ 97.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 500-749	RN-ETP-A-000749-PPL5Y	$ 139.59	$ 121.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 500-749	RN-ETP-A-000749-PTM1Y	$ 18.59	$ 16.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 500-749	RN-ETP-A-000749-PTM2Y	$ 55.65	$ 48.42
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 500-749	RN-ETP-A-000749-PTM3Y	$ 80.35	$ 69.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 500-749	RN-ETP-A-000749-PTM4Y	$ 107.14	$ 93.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 500-749	RN-ETP-A-000749-PTM5Y	$ 133.92	$ 116.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 500-749	RN-ETP-A-000749-USG1Y	$ 29.76	$ 25.89
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 500-749	RN-ETP-A-000749-USG2Y	$ 55.65	$ 48.42
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 500-749	RN-ETP-A-000749-USG3Y	$ 80.35	$ 69.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 500-749	RN-ETP-A-000749-USG4Y	$ 107.14	$ 93.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 500-749	RN-ETP-A-000749-USG5Y	$ 133.92	$ 116.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 500-749	RN-ETP-A-000749-USP1Y	$ 31.02	$ 26.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 500-749	RN-ETP-A-000749-USP2Y	$ 58.00	$ 50.46
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 500-749	RN-ETP-A-000749-USP3Y	$ 83.75	$ 72.86
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 500-749	RN-ETP-A-000749-USP4Y	$ 111.67	$ 97.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 500-749	RN-ETP-A-000749-USP5Y	$ 139.59	$ 121.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 750-999	RN-ETP-A-000999-CAG1Y	$ 29.03	$ 25.26
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 750-999	RN-ETP-A-000999-CAG2Y	$ 54.28	$ 47.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 750-999	RN-ETP-A-000999-CAG3Y	$ 78.38	$ 68.19
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 750-999	RN-ETP-A-000999-CAG4Y	$ 104.51	$ 90.92
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 750-999	RN-ETP-A-000999-CAG5Y	$ 130.64	$ 113.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 750-999	RN-ETP-A-000999-CAP1Y	$ 30.26	$ 26.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 750-999	RN-ETP-A-000999-CAP2Y	$ 56.58	$ 49.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 750-999	RN-ETP-A-000999-CAP3Y	$ 81.70	$ 71.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 750-999	RN-ETP-A-000999-CAP4Y	$ 108.94	$ 94.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 750-999	RN-ETP-A-000999-CAP5Y	$ 136.17	$ 118.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 750-999	RN-ETP-A-000999-PPL1Y	$ 8.11	$ 7.06
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 750-999	RN-ETP-A-000999-PPL2Y	$ 56.58	$ 49.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 750-999	RN-ETP-A-000999-PPL3Y	$ 81.70	$ 71.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 750-999	RN-ETP-A-000999-PPL4Y	$ 108.94	$ 94.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 750-999	RN-ETP-A-000999-PPL5Y	$ 136.17	$ 118.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 750-999	RN-ETP-A-000999-PTM1Y	$ 15.61	$ 13.58
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 750-999	RN-ETP-A-000999-PTM2Y	$ 54.28	$ 47.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 750-999	RN-ETP-A-000999-PTM3Y	$ 78.38	$ 68.19
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 750-999	RN-ETP-A-000999-PTM4Y	$ 104.51	$ 90.92
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 750-999	RN-ETP-A-000999-PTM5Y	$ 130.64	$ 113.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 750-999	RN-ETP-A-000999-USG1Y	$ 29.03	$ 25.26
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 750-999	RN-ETP-A-000999-USG2Y	$ 54.28	$ 47.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 750-999	RN-ETP-A-000999-USG3Y	$ 78.38	$ 68.19
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 750-999	RN-ETP-A-000999-USG4Y	$ 104.51	$ 90.92
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 750-999	RN-ETP-A-000999-USG5Y	$ 130.64	$ 113.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 750-999	RN-ETP-A-000999-USP1Y	$ 30.26	$ 26.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 750-999	RN-ETP-A-000999-USP2Y	$ 56.58	$ 49.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 750-999	RN-ETP-A-000999-USP3Y	$ 81.70	$ 71.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 750-999	RN-ETP-A-000999-USP4Y	$ 108.94	$ 94.78

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 750-999	RN-ETP-A-000999-USP5Y	$ 136.17	$ 118.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 1,000-1999	RN-ETP-A-001999-CAG1Y	$ 22.35	$ 19.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 1,000-1999	RN-ETP-A-001999-CAG2Y	$ 41.79	$ 36.36
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 1,000-1999	RN-ETP-A-001999-CAG3Y	$ 60.35	$ 52.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 1,000-1999	RN-ETP-A-001999-CAG4Y	$ 80.46	$ 70.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 1,000-1999	RN-ETP-A-001999-CAG5Y	$ 100.58	$ 87.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 1,000-1999	RN-ETP-A-001999-CAP1Y	$ 23.29	$ 20.26
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 1,000-1999	RN-ETP-A-001999-CAP2Y	$ 43.56	$ 37.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 1,000-1999	RN-ETP-A-001999-CAP3Y	$ 62.88	$ 54.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 1,000-1999	RN-ETP-A-001999-CAP4Y	$ 83.84	$ 72.94
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 1,000-1999	RN-ETP-A-001999-CAP5Y	$ 104.81	$ 91.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 1,000-1999	RN-ETP-A-001999-PPL1Y	$ 7.35	$ 6.39
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 1,000-1999	RN-ETP-A-001999-PPL2Y	$ 43.56	$ 37.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 1,000-1999	RN-ETP-A-001999-PPL3Y	$ 62.88	$ 54.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 1,000-1999	RN-ETP-A-001999-PPL4Y	$ 83.84	$ 72.94
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 1,000-1999	RN-ETP-A-001999-PPL5Y	$ 104.81	$ 91.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 1,000-1999	RN-ETP-A-001999-PTM1Y	$ 14.16	$ 12.32
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 1,000-1999	RN-ETP-A-001999-PTM2Y	$ 41.79	$ 36.36
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 1,000-1999	RN-ETP-A-001999-PTM3Y	$ 60.35	$ 52.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 1,000-1999	RN-ETP-A-001999-PTM4Y	$ 80.46	$ 70.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 1,000-1999	RN-ETP-A-001999-PTM5Y	$ 100.58	$ 87.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 1,000-1999	RN-ETP-A-001999-USG1Y	$ 22.35	$ 19.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 1,000-1999	RN-ETP-A-001999-USG2Y	$ 41.79	$ 36.36
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 1,000-1999	RN-ETP-A-001999-USG3Y	$ 60.35	$ 52.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 1,000-1999	RN-ETP-A-001999-USG4Y	$ 80.46	$ 70.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 1,000-1999	RN-ETP-A-001999-USG5Y	$ 100.58	$ 87.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 1,000-1999	RN-ETP-A-001999-USP1Y	$ 23.29	$ 20.26
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 1,000-1999	RN-ETP-A-001999-USP2Y	$ 43.56	$ 37.90
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 1,000-1999	RN-ETP-A-001999-USP3Y	$ 62.88	$ 54.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 1,000-1999	RN-ETP-A-001999-USP4Y	$ 83.84	$ 72.94
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 1,000-1999	RN-ETP-A-001999-USP5Y	$ 104.81	$ 91.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 2,000-4999	RN-ETP-A-004999-CAG1Y	$ 16.67	$ 14.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 2,000-4999	RN-ETP-A-004999-CAG2Y	$ 31.17	$ 27.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 2,000-4999	RN-ETP-A-004999-CAG3Y	$ 45.01	$ 39.16
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 2,000-4999	RN-ETP-A-004999-CAG4Y	$ 60.01	$ 52.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 2,000-4999	RN-ETP-A-004999-CAG5Y	$ 75.02	$ 65.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 2,000-4999	RN-ETP-A-004999-CAP1Y	$ 17.38	$ 15.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 2,000-4999	RN-ETP-A-004999-CAP2Y	$ 32.49	$ 28.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 2,000-4999	RN-ETP-A-004999-CAP3Y	$ 46.93	$ 40.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 2,000-4999	RN-ETP-A-004999-CAP4Y	$ 62.57	$ 54.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 2,000-4999	RN-ETP-A-004999-CAP5Y	$ 78.21	$ 68.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 2,000-4999	RN-ETP-A-004999-PPL1Y	$ 6.70	$ 5.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 2,000-4999	RN-ETP-A-004999-PPL2Y	$ 32.49	$ 28.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 2,000-4999	RN-ETP-A-004999-PPL3Y	$ 46.93	$ 40.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 2,000-4999	RN-ETP-A-004999-PPL4Y	$ 62.57	$ 54.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 2,000-4999	RN-ETP-A-004999-PPL5Y	$ 78.21	$ 68.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 2,000-4999	RN-ETP-A-004999-PTM1Y	$ 12.89	$ 11.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 2,000-4999	RN-ETP-A-004999-PTM2Y	$ 31.17	$ 27.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 2,000-4999	RN-ETP-A-004999-PTM3Y	$ 45.01	$ 39.16

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 2,000-4999	RN-ETP-A-004999-PTM4Y	$ 60.01	$ 52.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 2,000-4999	RN-ETP-A-004999-PTM5Y	$ 75.02	$ 65.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 2,000-4999	RN-ETP-A-004999-USG1Y	$ 16.67	$ 14.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 2,000-4999	RN-ETP-A-004999-USG2Y	$ 31.17	$ 27.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 2,000-4999	RN-ETP-A-004999-USG3Y	$ 45.01	$ 39.16
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 2,000-4999	RN-ETP-A-004999-USG4Y	$ 60.01	$ 52.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 2,000-4999	RN-ETP-A-004999-USG5Y	$ 75.02	$ 65.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 2,000-4999	RN-ETP-A-004999-USP1Y	$ 17.38	$ 15.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 2,000-4999	RN-ETP-A-004999-USP2Y	$ 32.49	$ 28.27
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 2,000-4999	RN-ETP-A-004999-USP3Y	$ 46.93	$ 40.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 2,000-4999	RN-ETP-A-004999-USP4Y	$ 62.57	$ 54.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 2,000-4999	RN-ETP-A-004999-USP5Y	$ 78.21	$ 68.04
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 5,000-9999	RN-ETP-A-009999-CAG1Y	$ 14.75	$ 12.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 5,000-9999	RN-ETP-A-009999-CAG2Y	$ 27.57	$ 23.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 5,000-9999	RN-ETP-A-009999-CAG3Y	$ 39.83	$ 34.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 5,000-9999	RN-ETP-A-009999-CAG4Y	$ 53.10	$ 46.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 5,000-9999	RN-ETP-A-009999-CAG5Y	$ 66.38	$ 57.75
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 5,000-9999	RN-ETP-A-009999-CAP1Y	$ 15.37	$ 13.37
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 5,000-9999	RN-ETP-A-009999-CAP2Y	$ 28.74	$ 25.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 5,000-9999	RN-ETP-A-009999-CAP3Y	$ 41.50	$ 36.11
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 5,000-9999	RN-ETP-A-009999-CAP4Y	$ 55.33	$ 48.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 5,000-9999	RN-ETP-A-009999-CAP5Y	$ 69.17	$ 60.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 5,000-9999	RN-ETP-A-009999-PPL1Y	$ 8.29	$ 7.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 5,000-9999	RN-ETP-A-009999-PPL2Y	$ 28.74	$ 25.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 5,000-9999	RN-ETP-A-009999-PPL3Y	$ 41.50	$ 36.11
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 5,000-9999	RN-ETP-A-009999-PPL4Y	$ 55.33	$ 48.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 5,000-9999	RN-ETP-A-009999-PPL5Y	$ 69.17	$ 60.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 5,000-9999	RN-ETP-A-009999-PTM1Y	$ 13.71	$ 11.93
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 5,000-9999	RN-ETP-A-009999-PTM2Y	$ 27.57	$ 23.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 5,000-9999	RN-ETP-A-009999-PTM3Y	$ 39.83	$ 34.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 5,000-9999	RN-ETP-A-009999-PTM4Y	$ 53.10	$ 46.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 5,000-9999	RN-ETP-A-009999-PTM5Y	$ 66.38	$ 57.75
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 5,000-9999	RN-ETP-A-009999-USG1Y	$ 14.75	$ 12.83
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 5,000-9999	RN-ETP-A-009999-USG2Y	$ 27.57	$ 23.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 5,000-9999	RN-ETP-A-009999-USG3Y	$ 39.83	$ 34.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 5,000-9999	RN-ETP-A-009999-USG4Y	$ 53.10	$ 46.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 5,000-9999	RN-ETP-A-009999-USG5Y	$ 66.38	$ 57.75
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 5,000-9999	RN-ETP-A-009999-USP1Y	$ 15.37	$ 13.37
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 5,000-9999	RN-ETP-A-009999-USP2Y	$ 28.74	$ 25.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 5,000-9999	RN-ETP-A-009999-USP3Y	$ 41.50	$ 36.11
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 5,000-9999	RN-ETP-A-009999-USP4Y	$ 55.33	$ 48.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 5,000-9999	RN-ETP-A-009999-USP5Y	$ 69.17	$ 60.18
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 10,000-19999	RN-ETP-A-019999-CAG1Y	$ 12.89	$ 11.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 10,000-19999	RN-ETP-A-019999-CAG2Y	$ 24.11	$ 20.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 10,000-19999	RN-ETP-A-019999-CAG3Y	$ 34.80	$ 30.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 10,000-19999	RN-ETP-A-019999-CAG4Y	$ 46.40	$ 40.37
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 10,000-19999	RN-ETP-A-019999-CAG5Y	$ 58.01	$ 50.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 10,000-19999	RN-ETP-A-019999-CAP1Y	$ 13.44	$ 11.69
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 10,000-19999	RN-ETP-A-019999-CAP2Y	$ 25.13	$ 21.86

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 10,000-19999	RN-ETP-A-019999-CAP3Y	$ 36.29	$ 31.57
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 10,000-19999	RN-ETP-A-019999-CAP4Y	$ 48.38	$ 42.09
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 10,000-19999	RN-ETP-A-019999-CAP5Y	$ 60.48	$ 52.62
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 10,000-19999	RN-ETP-A-019999-PPL1Y	$ 6.07	$ 5.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 10,000-19999	RN-ETP-A-019999-PPL2Y	$ 25.13	$ 21.86
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 10,000-19999	RN-ETP-A-019999-PPL3Y	$ 36.29	$ 31.57
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 10,000-19999	RN-ETP-A-019999-PPL4Y	$ 48.38	$ 42.09
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 10,000-19999	RN-ETP-A-019999-PPL5Y	$ 60.48	$ 52.62
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 10,000-19999	RN-ETP-A-019999-PTM1Y	$ 10.79	$ 9.39
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 10,000-19999	RN-ETP-A-019999-PTM2Y	$ 24.11	$ 20.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 10,000-19999	RN-ETP-A-019999-PTM3Y	$ 34.80	$ 30.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 10,000-19999	RN-ETP-A-019999-PTM4Y	$ 46.40	$ 40.37
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 10,000-19999	RN-ETP-A-019999-PTM5Y	$ 58.01	$ 50.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 10,000-19999	RN-ETP-A-019999-USG1Y	$ 12.89	$ 11.21
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 10,000-19999	RN-ETP-A-019999-USG2Y	$ 24.11	$ 20.98
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 10,000-19999	RN-ETP-A-019999-USG3Y	$ 34.80	$ 30.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 10,000-19999	RN-ETP-A-019999-USG4Y	$ 46.40	$ 40.37
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 10,000-19999	RN-ETP-A-019999-USG5Y	$ 58.01	$ 50.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 10,000-19999	RN-ETP-A-019999-USP1Y	$ 13.44	$ 11.69
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 10,000-19999	RN-ETP-A-019999-USP2Y	$ 25.13	$ 21.86
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 10,000-19999	RN-ETP-A-019999-USP3Y	$ 36.29	$ 31.57
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 10,000-19999	RN-ETP-A-019999-USP4Y	$ 48.38	$ 42.09
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 10,000-19999	RN-ETP-A-019999-USP5Y	$ 60.48	$ 52.62
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 20,000-49999	RN-ETP-A-049999-CAG1Y	$ 11.55	$ 10.05
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 20,000-49999	RN-ETP-A-049999-CAG2Y	$ 21.67	$ 18.85
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 20,000-49999	RN-ETP-A-049999-CAG3Y	$ 31.19	$ 27.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 20,000-49999	RN-ETP-A-049999-CAG4Y	$ 41.58	$ 36.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 20,000-49999	RN-ETP-A-049999-CAG5Y	$ 51.98	$ 45.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 20,000-49999	RN-ETP-A-049999-CAP1Y	$ 12.04	$ 10.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 20,000-49999	RN-ETP-A-049999-CAP2Y	$ 22.59	$ 19.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 20,000-49999	RN-ETP-A-049999-CAP3Y	$ 32.51	$ 28.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 20,000-49999	RN-ETP-A-049999-CAP4Y	$ 43.34	$ 37.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 20,000-49999	RN-ETP-A-049999-CAP5Y	$ 54.18	$ 47.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 20,000-49999	RN-ETP-A-049999-PPL1Y	$ 4.85	$ 4.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 20,000-49999	RN-ETP-A-049999-PPL2Y	$ 22.50	$ 19.58
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 20,000-49999	RN-ETP-A-049999-PPL3Y	$ 32.51	$ 28.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 20,000-49999	RN-ETP-A-049999-PPL4Y	$ 43.34	$ 37.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 20,000-49999	RN-ETP-A-049999-PPL5Y	$ 54.18	$ 47.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 20,000-49999	RN-ETP-A-049999-PTM1Y	$ 9.34	$ 8.13
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 20,000-49999	RN-ETP-A-049999-PTM2Y	$ 21.59	$ 18.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 20,000-49999	RN-ETP-A-049999-PTM3Y	$ 31.19	$ 27.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 20,000-49999	RN-ETP-A-049999-PTM4Y	$ 41.58	$ 36.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 20,000-49999	RN-ETP-A-049999-PTM5Y	$ 51.98	$ 45.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 20,000-49999	RN-ETP-A-049999-USG1Y	$ 11.55	$ 10.05
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 20,000-49999	RN-ETP-A-049999-USG2Y	$ 21.67	$ 18.85
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 20,000-49999	RN-ETP-A-049999-USG3Y	$ 31.19	$ 27.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 20,000-49999	RN-ETP-A-049999-USG4Y	$ 41.58	$ 36.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 20,000-49999	RN-ETP-A-049999-USG5Y	$ 51.98	$ 45.22
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 20,000-49999	RN-ETP-A-049999-USP1Y	$ 12.04	$ 10.47

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 20,000-49999	RN-ETP-A-049999-USP2Y	$ 22.59	$ 19.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 20,000-49999	RN-ETP-A-049999-USP3Y	$ 32.51	$ 28.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 20,000-49999	RN-ETP-A-049999-USP4Y	$ 43.34	$ 37.71
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 20,000-49999	RN-ETP-A-049999-USP5Y	$ 54.18	$ 47.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 50,000-74999	RN-ETP-A-074999-CAG1Y	$ 11.84	$ 10.30
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 50,000-74999	RN-ETP-A-074999-CAG2Y	$ 22.18	$ 19.30
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 50,000-74999	RN-ETP-A-074999-CAG3Y	$ 31.97	$ 27.81
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 50,000-74999	RN-ETP-A-074999-CAG4Y	$ 42.62	$ 37.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 50,000-74999	RN-ETP-A-074999-CAG5Y	$ 53.28	$ 46.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 50,000-74999	RN-ETP-A-074999-CAP1Y	$ 12.34	$ 10.74
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 50,000-74999	RN-ETP-A-074999-CAP2Y	$ 23.13	$ 20.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 50,000-74999	RN-ETP-A-074999-CAP3Y	$ 33.32	$ 28.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 50,000-74999	RN-ETP-A-074999-CAP4Y	$ 44.42	$ 38.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 50,000-74999	RN-ETP-A-074999-CAP5Y	$ 55.53	$ 48.31
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 50,000-74999	RN-ETP-A-074999-PPL1Y	$ 4.76	$ 4.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 50,000-74999	RN-ETP-A-074999-PPL2Y	$ 23.06	$ 20.06
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 50,000-74999	RN-ETP-A-074999-PPL3Y	$ 33.32	$ 28.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 50,000-74999	RN-ETP-A-074999-PPL4Y	$ 44.42	$ 38.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 50,000-74999	RN-ETP-A-074999-PPL5Y	$ 55.53	$ 48.31
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 50,000-74999	RN-ETP-A-074999-PTM1Y	$ 8.80	$ 7.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 50,000-74999	RN-ETP-A-074999-PTM2Y	$ 22.14	$ 19.26
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 50,000-74999	RN-ETP-A-074999-PTM3Y	$ 31.97	$ 27.81
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 50,000-74999	RN-ETP-A-074999-PTM4Y	$ 42.62	$ 37.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 50,000-74999	RN-ETP-A-074999-PTM5Y	$ 53.28	$ 46.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 50,000-74999	RN-ETP-A-074999-USG1Y	$ 11.84	$ 10.30
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 50,000-74999	RN-ETP-A-074999-USG2Y	$ 22.18	$ 19.30
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 50,000-74999	RN-ETP-A-074999-USG3Y	$ 31.97	$ 27.81
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 50,000-74999	RN-ETP-A-074999-USG4Y	$ 42.62	$ 37.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 50,000-74999	RN-ETP-A-074999-USG5Y	$ 53.28	$ 46.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 50,000-74999	RN-ETP-A-074999-USP1Y	$ 12.34	$ 10.74
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 50,000-74999	RN-ETP-A-074999-USP2Y	$ 23.13	$ 20.12
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 50,000-74999	RN-ETP-A-074999-USP3Y	$ 33.32	$ 28.99
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 50,000-74999	RN-ETP-A-074999-USP4Y	$ 44.42	$ 38.65
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 50,000-74999	RN-ETP-A-074999-USP5Y	$ 55.53	$ 48.31
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 75,000-99999	RN-ETP-A-099999-CAG1Y	$ 12.39	$ 10.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 75,000-99999	RN-ETP-A-099999-CAG2Y	$ 23.16	$ 20.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 75,000-99999	RN-ETP-A-099999-CAG3Y	$ 33.45	$ 29.10
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 75,000-99999	RN-ETP-A-099999-CAG4Y	$ 44.60	$ 38.80
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 75,000-99999	RN-ETP-A-099999-CAG5Y	$ 55.76	$ 48.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 75,000-99999	RN-ETP-A-099999-CAP1Y	$ 12.91	$ 11.23
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 75,000-99999	RN-ETP-A-099999-CAP2Y	$ 24.14	$ 21.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 75,000-99999	RN-ETP-A-099999-CAP3Y	$ 34.86	$ 30.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 75,000-99999	RN-ETP-A-099999-CAP4Y	$ 46.48	$ 40.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 75,000-99999	RN-ETP-A-099999-CAP5Y	$ 58.10	$ 50.55
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 75,000-99999	RN-ETP-A-099999-PPL1Y	$ 4.76	$ 4.14
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 75,000-99999	RN-ETP-A-099999-PPL2Y	$ 24.14	$ 21.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 75,000-99999	RN-ETP-A-099999-PPL3Y	$ 34.86	$ 30.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 75,000-99999	RN-ETP-A-099999-PPL4Y	$ 46.48	$ 40.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 75,000-99999	RN-ETP-A-099999-PPL5Y	$ 58.10	$ 50.55

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 75,000-99999	RN-ETP-A-099999-PTM1Y	$ 8.22	$ 7.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 75,000-99999	RN-ETP-A-099999-PTM2Y	$ 23.16	$ 20.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 75,000-99999	RN-ETP-A-099999-PTM3Y	$ 33.45	$ 29.10
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 75,000-99999	RN-ETP-A-099999-PTM4Y	$ 44.60	$ 38.80
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 75,000-99999	RN-ETP-A-099999-PTM5Y	$ 55.76	$ 48.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 75,000-99999	RN-ETP-A-099999-USG1Y	$ 12.39	$ 10.78
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 75,000-99999	RN-ETP-A-099999-USG2Y	$ 23.16	$ 20.15
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 75,000-99999	RN-ETP-A-099999-USG3Y	$ 33.45	$ 29.10
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 75,000-99999	RN-ETP-A-099999-USG4Y	$ 44.60	$ 38.80
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 75,000-99999	RN-ETP-A-099999-USG5Y	$ 55.76	$ 48.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 75,000-99999	RN-ETP-A-099999-USP1Y	$ 12.91	$ 11.23
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 75,000-99999	RN-ETP-A-099999-USP2Y	$ 24.14	$ 21.00
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 75,000-99999	RN-ETP-A-099999-USP3Y	$ 34.86	$ 30.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 75,000-99999	RN-ETP-A-099999-USP4Y	$ 46.48	$ 40.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 75,000-99999	RN-ETP-A-099999-USP5Y	$ 58.10	$ 50.55
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 100,000-199999	RN-ETP-A-199999-CAG1Y	$ 10.78	$ 9.38
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 100,000-199999	RN-ETP-A-199999-CAG2Y	$ 20.15	$ 17.53
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 100,000-199999	RN-ETP-A-199999-CAG3Y	$ 29.11	$ 25.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 100,000-199999	RN-ETP-A-199999-CAG4Y	$ 38.81	$ 33.76
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 100,000-199999	RN-ETP-A-199999-CAG5Y	$ 48.51	$ 42.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 100,000-199999	RN-ETP-A-199999-CAP1Y	$ 11.23	$ 9.77
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 100,000-199999	RN-ETP-A-199999-CAP2Y	$ 21.01	$ 18.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 100,000-199999	RN-ETP-A-199999-CAP3Y	$ 30.32	$ 26.38
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 100,000-199999	RN-ETP-A-199999-CAP4Y	$ 40.43	$ 35.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 100,000-199999	RN-ETP-A-199999-CAP5Y	$ 50.54	$ 43.97
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 100,000-199999	RN-ETP-A-199999-PPL1Y	$ 3.50	$ 3.05
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 100,000-199999	RN-ETP-A-199999-PPL2Y	$ 21.09	$ 18.35
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 100,000-199999	RN-ETP-A-199999-PPL3Y	$ 30.48	$ 26.52
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 100,000-199999	RN-ETP-A-199999-PPL4Y	$ 40.64	$ 35.36
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 100,000-199999	RN-ETP-A-199999-PPL5Y	$ 50.81	$ 44.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 100,000-199999	RN-ETP-A-199999-PTM1Y	$ 6.58	$ 5.72
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 100,000-199999	RN-ETP-A-199999-PTM2Y	$ 20.25	$ 17.62
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 100,000-199999	RN-ETP-A-199999-PTM3Y	$ 29.24	$ 25.44
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 100,000-199999	RN-ETP-A-199999-PTM4Y	$ 38.99	$ 33.92
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 100,000-199999	RN-ETP-A-199999-PTM5Y	$ 48.74	$ 42.40
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 100,000-199999	RN-ETP-A-199999-USG1Y	$ 10.78	$ 9.38
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 100,000-199999	RN-ETP-A-199999-USG2Y	$ 20.15	$ 17.53
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 100,000-199999	RN-ETP-A-199999-USG3Y	$ 29.11	$ 25.33
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 100,000-199999	RN-ETP-A-199999-USG4Y	$ 38.81	$ 33.76
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 100,000-199999	RN-ETP-A-199999-USG5Y	$ 48.51	$ 42.20
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 100,000-199999	RN-ETP-A-199999-USP1Y	$ 11.23	$ 9.77
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 100,000-199999	RN-ETP-A-199999-USP2Y	$ 21.01	$ 18.28
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 100,000-199999	RN-ETP-A-199999-USP3Y	$ 30.32	$ 26.38
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 100,000-199999	RN-ETP-A-199999-USP4Y	$ 40.43	$ 35.17
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 100,000-199999	RN-ETP-A-199999-USP5Y	$ 50.54	$ 43.97
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 1 Year 200,000+	RN-ETP-A-200000+CAG1Y	$ 10.42	$ 9.07
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 2 Year 200,000+	RN-ETP-A-200000+CAG2Y	$ 19.49	$ 16.96
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 3 Year 200,000+	RN-ETP-A-200000+CAG3Y	$ 28.13	$ 24.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 4 Year 200,000+	RN-ETP-A-200000+CAG4Y	$ 37.51	$ 32.63

FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA 5 Year 200,000+	RN-ETP-A-200000+CAG5Y	$ 46.89	$ 40.79
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 1 Year 200,000+	RN-ETP-A-200000+CAP1Y	$ 10.86	$ 9.45
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 2 Year 200,000+	RN-ETP-A-200000+CAP2Y	$ 20.30	$ 17.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 3 Year 200,000+	RN-ETP-A-200000+CAP3Y	$ 29.32	$ 25.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 4 Year 200,000+	RN-ETP-A-200000+CAP4Y	$ 39.10	$ 34.02
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov CA Plat Prio Plus 5 Year 200,000+	RN-ETP-A-200000+CAP5Y	$ 48.87	$ 42.52
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 1 Year 200,000+	RN-ETP-A-200000+PPL1Y	$ 3.13	$ 2.72
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 2 Year 200,000+	RN-ETP-A-200000+PPL2Y	$ 20.32	$ 17.68
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 3 Year 200,000+	RN-ETP-A-200000+PPL3Y	$ 29.38	$ 25.56
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 4 Year 200,000+	RN-ETP-A-200000+PPL4Y	$ 39.17	$ 34.08
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Plat Prio Plus Support 5 Year 200,000+	RN-ETP-A-200000+PPL5Y	$ 48.96	$ 42.60
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 1 Year 200,000+	RN-ETP-A-200000+PTM1Y	$ 6.04	$ 5.25
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 2 Year 200,000+	RN-ETP-A-200000+PTM2Y	$ 19.51	$ 16.97
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 3 Year 200,000+	RN-ETP-A-200000+PTM3Y	$ 28.16	$ 24.50
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 4 Year 200,000+	RN-ETP-A-200000+PTM4Y	$ 37.55	$ 32.67
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Platinum Support 5 Year 200,000+	RN-ETP-A-200000+PTM5Y	$ 46.94	$ 40.84
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 1 Year 200,000+	RN-ETP-A-200000+USG1Y	$ 10.42	$ 9.07
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 2 Year 200,000+	RN-ETP-A-200000+USG2Y	$ 19.49	$ 16.96
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 3 Year 200,000+	RN-ETP-A-200000+USG3Y	$ 28.13	$ 24.47
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 4 Year 200,000+	RN-ETP-A-200000+USG4Y	$ 37.51	$ 32.63
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US 5 Year 200,000+	RN-ETP-A-200000+USG5Y	$ 46.89	$ 40.79
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 1 Year 200,000+	RN-ETP-A-200000+USP1Y	$ 10.86	$ 9.45
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 2 Year 200,000+	RN-ETP-A-200000+USP2Y	$ 20.30	$ 17.66
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 3 Year 200,000+	RN-ETP-A-200000+USP3Y	$ 29.32	$ 25.51
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 4 Year 200,000+	RN-ETP-A-200000+USP4Y	$ 39.10	$ 34.02
FireEye	Renewal-AV/AS Add-on for ETP Cloud & Gov US Plat Prio Plus 5 Year 200,000+	RN-ETP-A-200000+USP5Y	$ 48.87	$ 42.52
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 1-249	RN-ETP-C-000249-CAG1Y	$ 84.56	$ 73.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 1-249	RN-ETP-C-000249-CAG2Y	$ 169.12	$ 147.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 1-249	RN-ETP-C-000249-CAG3Y	$ 228.31	$ 198.63
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 1-249	RN-ETP-C-000249-CAG4Y	$ 304.42	$ 264.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 1-249	RN-ETP-C-000249-CAG5Y	$ 380.52	$ 331.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 1-249	RN-ETP-C-000249-CAP1Y	$ 88.14	$ 76.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 1-249	RN-ETP-C-000249-CAP2Y	$ 176.28	$ 153.36
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 1-249	RN-ETP-C-000249-CAP3Y	$ 237.98	$ 207.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 1-249	RN-ETP-C-000249-CAP4Y	$ 317.30	$ 276.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 1-249	RN-ETP-C-000249-CAP5Y	$ 396.63	$ 345.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 1-249	RN-ETP-C-000249-PPL1Y	$ 88.14	$ 76.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 1-249	RN-ETP-C-000249-PPL2Y	$ 176.28	$ 153.36
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 1-249	RN-ETP-C-000249-PPL3Y	$ 237.98	$ 207.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 1-249	RN-ETP-C-000249-PPL4Y	$ 317.30	$ 276.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 1-249	RN-ETP-C-000249-PPL5Y	$ 396.63	$ 345.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 1-249	RN-ETP-C-000249-PTM1Y	$ 84.56	$ 73.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 1-249	RN-ETP-C-000249-PTM2Y	$ 169.12	$ 147.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 1-249	RN-ETP-C-000249-PTM3Y	$ 228.31	$ 198.63
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 1-249	RN-ETP-C-000249-PTM4Y	$ 304.42	$ 264.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 1-249	RN-ETP-C-000249-PTM5Y	$ 380.52	$ 331.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 1-249	RN-ETP-C-000249-USG1Y	$ 84.56	$ 73.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 1-249	RN-ETP-C-000249-USG2Y	$ 169.12	$ 147.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 1-249	RN-ETP-C-000249-USG3Y	$ 228.31	$ 198.63

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 1-249	RN-ETP-C-000249-USG4Y	$ 304.42	$ 264.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 1-249	RN-ETP-C-000249-USG5Y	$ 380.52	$ 331.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 1-249	RN-ETP-C-000249-USP1Y	$ 88.14	$ 76.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 1-249	RN-ETP-C-000249-USP2Y	$ 176.28	$ 153.36
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 1-249	RN-ETP-C-000249-USP3Y	$ 237.98	$ 207.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 1-249	RN-ETP-C-000249-USP4Y	$ 317.30	$ 276.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 1-249	RN-ETP-C-000249-USP5Y	$ 396.63	$ 345.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 250-499	RN-ETP-C-000499-CAG1Y	$ 69.82	$ 60.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 250-499	RN-ETP-C-000499-CAG2Y	$ 139.64	$ 121.49
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 250-499	RN-ETP-C-000499-CAG3Y	$ 188.51	$ 164.00
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 250-499	RN-ETP-C-000499-CAG4Y	$ 251.35	$ 218.67
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 250-499	RN-ETP-C-000499-CAG5Y	$ 314.19	$ 273.35
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 250-499	RN-ETP-C-000499-CAP1Y	$ 72.78	$ 63.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 250-499	RN-ETP-C-000499-CAP2Y	$ 145.56	$ 126.64
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 250-499	RN-ETP-C-000499-CAP3Y	$ 196.51	$ 170.96
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 250-499	RN-ETP-C-000499-CAP4Y	$ 262.01	$ 227.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 250-499	RN-ETP-C-000499-CAP5Y	$ 327.51	$ 284.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 250-499	RN-ETP-C-000499-PPL1Y	$ 72.78	$ 63.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 250-499	RN-ETP-C-000499-PPL2Y	$ 145.56	$ 126.64
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 250-499	RN-ETP-C-000499-PPL3Y	$ 196.51	$ 170.96
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 250-499	RN-ETP-C-000499-PPL4Y	$ 262.01	$ 227.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 250-499	RN-ETP-C-000499-PPL5Y	$ 327.51	$ 284.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 250-499	RN-ETP-C-000499-PTM1Y	$ 69.82	$ 60.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 250-499	RN-ETP-C-000499-PTM2Y	$ 139.64	$ 121.49
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 250-499	RN-ETP-C-000499-PTM3Y	$ 188.51	$ 164.00
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 250-499	RN-ETP-C-000499-PTM4Y	$ 251.35	$ 218.67
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 250-499	RN-ETP-C-000499-PTM5Y	$ 314.19	$ 273.35
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 250-499	RN-ETP-C-000499-USG1Y	$ 69.82	$ 60.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 250-499	RN-ETP-C-000499-USG2Y	$ 139.64	$ 121.49
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 250-499	RN-ETP-C-000499-USG3Y	$ 188.51	$ 164.00
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 250-499	RN-ETP-C-000499-USG4Y	$ 251.35	$ 218.67
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 250-499	RN-ETP-C-000499-USG5Y	$ 314.19	$ 273.35
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 250-499	RN-ETP-C-000499-USP1Y	$ 72.78	$ 63.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 250-499	RN-ETP-C-000499-USP2Y	$ 145.56	$ 126.64
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 250-499	RN-ETP-C-000499-USP3Y	$ 196.51	$ 170.96
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 250-499	RN-ETP-C-000499-USP4Y	$ 262.01	$ 227.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 250-499	RN-ETP-C-000499-USP5Y	$ 327.51	$ 284.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 500-749	RN-ETP-C-000749-CAG1Y	$ 59.89	$ 52.10
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 500-749	RN-ETP-C-000749-CAG2Y	$ 119.78	$ 104.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 500-749	RN-ETP-C-000749-CAG3Y	$ 161.70	$ 140.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 500-749	RN-ETP-C-000749-CAG4Y	$ 215.60	$ 187.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 500-749	RN-ETP-C-000749-CAG5Y	$ 269.51	$ 234.47
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 500-749	RN-ETP-C-000749-CAP1Y	$ 62.43	$ 54.31
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 500-749	RN-ETP-C-000749-CAP2Y	$ 124.86	$ 108.63
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 500-749	RN-ETP-C-000749-CAP3Y	$ 168.56	$ 146.65
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 500-749	RN-ETP-C-000749-CAP4Y	$ 224.75	$ 195.53
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 500-749	RN-ETP-C-000749-CAP5Y	$ 280.94	$ 244.42
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 500-749	RN-ETP-C-000749-PPL1Y	$ 62.43	$ 54.31
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 500-749	RN-ETP-C-000749-PPL2Y	$ 124.86	$ 108.63

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 500-749	RN-ETP-C-000749-PPL3Y	$ 168.56	$ 146.65
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 500-749	RN-ETP-C-000749-PPL4Y	$ 224.75	$ 195.53
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 500-749	RN-ETP-C-000749-PPL5Y	$ 280.94	$ 244.42
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 500-749	RN-ETP-C-000749-PTM1Y	$ 59.89	$ 52.10
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 500-749	RN-ETP-C-000749-PTM2Y	$ 119.78	$ 104.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 500-749	RN-ETP-C-000749-PTM3Y	$ 161.70	$ 140.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 500-749	RN-ETP-C-000749-PTM4Y	$ 215.60	$ 187.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 500-749	RN-ETP-C-000749-PTM5Y	$ 269.51	$ 234.47
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 500-749	RN-ETP-C-000749-USG1Y	$ 59.89	$ 52.10
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 500-749	RN-ETP-C-000749-USG2Y	$ 119.78	$ 104.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 500-749	RN-ETP-C-000749-USG3Y	$ 161.70	$ 140.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 500-749	RN-ETP-C-000749-USG4Y	$ 215.60	$ 187.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 500-749	RN-ETP-C-000749-USG5Y	$ 269.51	$ 234.47
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 500-749	RN-ETP-C-000749-USP1Y	$ 62.43	$ 54.31
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 500-749	RN-ETP-C-000749-USP2Y	$ 124.86	$ 108.63
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 500-749	RN-ETP-C-000749-USP3Y	$ 168.56	$ 146.65
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 500-749	RN-ETP-C-000749-USP4Y	$ 224.75	$ 195.53
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 500-749	RN-ETP-C-000749-USP5Y	$ 280.94	$ 244.42
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 750-999	RN-ETP-C-000999-CAG1Y	$ 50.30	$ 43.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 750-999	RN-ETP-C-000999-CAG2Y	$ 100.60	$ 87.52
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 750-999	RN-ETP-C-000999-CAG3Y	$ 135.81	$ 118.15
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 750-999	RN-ETP-C-000999-CAG4Y	$ 181.08	$ 157.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 750-999	RN-ETP-C-000999-CAG5Y	$ 226.35	$ 196.92
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 750-999	RN-ETP-C-000999-CAP1Y	$ 52.43	$ 45.61
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 750-999	RN-ETP-C-000999-CAP2Y	$ 104.86	$ 91.23
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 750-999	RN-ETP-C-000999-CAP3Y	$ 141.56	$ 123.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 750-999	RN-ETP-C-000999-CAP4Y	$ 188.75	$ 164.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 750-999	RN-ETP-C-000999-CAP5Y	$ 235.94	$ 205.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 750-999	RN-ETP-C-000999-PPL1Y	$ 52.43	$ 45.61
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 750-999	RN-ETP-C-000999-PPL2Y	$ 104.86	$ 91.23
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 750-999	RN-ETP-C-000999-PPL3Y	$ 141.56	$ 123.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 750-999	RN-ETP-C-000999-PPL4Y	$ 188.75	$ 164.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 750-999	RN-ETP-C-000999-PPL5Y	$ 235.94	$ 205.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 750-999	RN-ETP-C-000999-PTM1Y	$ 50.30	$ 43.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 750-999	RN-ETP-C-000999-PTM2Y	$ 100.60	$ 87.52
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 750-999	RN-ETP-C-000999-PTM3Y	$ 135.81	$ 118.15
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 750-999	RN-ETP-C-000999-PTM4Y	$ 181.08	$ 157.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 750-999	RN-ETP-C-000999-PTM5Y	$ 226.35	$ 196.92
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 750-999	RN-ETP-C-000999-USG1Y	$ 50.30	$ 43.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 750-999	RN-ETP-C-000999-USG2Y	$ 100.60	$ 87.52
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 750-999	RN-ETP-C-000999-USG3Y	$ 135.81	$ 118.15
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 750-999	RN-ETP-C-000999-USG4Y	$ 181.08	$ 157.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 750-999	RN-ETP-C-000999-USG5Y	$ 226.35	$ 196.92
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 750-999	RN-ETP-C-000999-USP1Y	$ 52.43	$ 45.61
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 750-999	RN-ETP-C-000999-USP2Y	$ 104.86	$ 91.23
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 750-999	RN-ETP-C-000999-USP3Y	$ 141.56	$ 123.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 750-999	RN-ETP-C-000999-USP4Y	$ 188.75	$ 164.21
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 750-999	RN-ETP-C-000999-USP5Y	$ 235.94	$ 205.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 1,000-1999	RN-ETP-C-001999-CAG1Y	$ 45.62	$ 39.69

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 1,000-1999	RN-ETP-C-001999-CAG2Y	$ 91.24	$ 79.38
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 1,000-1999	RN-ETP-C-001999-CAG3Y	$ 123.17	$ 107.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 1,000-1999	RN-ETP-C-001999-CAG4Y	$ 164.23	$ 142.88
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 1,000-1999	RN-ETP-C-001999-CAG5Y	$ 205.29	$ 178.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 1,000-1999	RN-ETP-C-001999-CAP1Y	$ 47.55	$ 41.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 1,000-1999	RN-ETP-C-001999-CAP2Y	$ 95.10	$ 82.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 1,000-1999	RN-ETP-C-001999-CAP3Y	$ 128.39	$ 111.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 1,000-1999	RN-ETP-C-001999-CAP4Y	$ 171.18	$ 148.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 1,000-1999	RN-ETP-C-001999-CAP5Y	$ 213.98	$ 186.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 1,000-1999	RN-ETP-C-001999-PPL1Y	$ 47.55	$ 41.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 1,000-1999	RN-ETP-C-001999-PPL2Y	$ 95.10	$ 82.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 1,000-1999	RN-ETP-C-001999-PPL3Y	$ 128.39	$ 111.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 1,000-1999	RN-ETP-C-001999-PPL4Y	$ 171.18	$ 148.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 1,000-1999	RN-ETP-C-001999-PPL5Y	$ 213.98	$ 186.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 1,000-1999	RN-ETP-C-001999-PTM1Y	$ 45.62	$ 39.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 1,000-1999	RN-ETP-C-001999-PTM2Y	$ 91.24	$ 79.38
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 1,000-1999	RN-ETP-C-001999-PTM3Y	$ 123.17	$ 107.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 1,000-1999	RN-ETP-C-001999-PTM4Y	$ 164.23	$ 142.88
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 1,000-1999	RN-ETP-C-001999-PTM5Y	$ 205.29	$ 178.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 1,000-1999	RN-ETP-C-001999-USG1Y	$ 45.62	$ 39.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 1,000-1999	RN-ETP-C-001999-USG2Y	$ 91.24	$ 79.38
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 1,000-1999	RN-ETP-C-001999-USG3Y	$ 123.17	$ 107.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 1,000-1999	RN-ETP-C-001999-USG4Y	$ 164.23	$ 142.88
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 1,000-1999	RN-ETP-C-001999-USG5Y	$ 205.29	$ 178.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 1,000-1999	RN-ETP-C-001999-USP1Y	$ 47.55	$ 41.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 1,000-1999	RN-ETP-C-001999-USP2Y	$ 95.10	$ 82.74
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 1,000-1999	RN-ETP-C-001999-USP3Y	$ 128.39	$ 111.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 1,000-1999	RN-ETP-C-001999-USP4Y	$ 171.18	$ 148.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 1,000-1999	RN-ETP-C-001999-USP5Y	$ 213.98	$ 186.16
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 2,000-4999	RN-ETP-C-004999-CAG1Y	$ 41.53	$ 36.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 2,000-4999	RN-ETP-C-004999-CAG2Y	$ 83.06	$ 72.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 2,000-4999	RN-ETP-C-004999-CAG3Y	$ 112.13	$ 97.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 2,000-4999	RN-ETP-C-004999-CAG4Y	$ 149.51	$ 130.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 2,000-4999	RN-ETP-C-004999-CAG5Y	$ 186.89	$ 162.59
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 2,000-4999	RN-ETP-C-004999-CAP1Y	$ 43.29	$ 37.66
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 2,000-4999	RN-ETP-C-004999-CAP2Y	$ 86.58	$ 75.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 2,000-4999	RN-ETP-C-004999-CAP3Y	$ 116.88	$ 101.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 2,000-4999	RN-ETP-C-004999-CAP4Y	$ 155.84	$ 135.58
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 2,000-4999	RN-ETP-C-004999-CAP5Y	$ 194.81	$ 169.48
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 2,000-4999	RN-ETP-C-004999-PPL1Y	$ 43.29	$ 37.66
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 2,000-4999	RN-ETP-C-004999-PPL2Y	$ 86.58	$ 75.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 2,000-4999	RN-ETP-C-004999-PPL3Y	$ 116.88	$ 101.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 2,000-4999	RN-ETP-C-004999-PPL4Y	$ 155.84	$ 135.58
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 2,000-4999	RN-ETP-C-004999-PPL5Y	$ 194.81	$ 169.48
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 2,000-4999	RN-ETP-C-004999-PTM1Y	$ 41.53	$ 36.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 2,000-4999	RN-ETP-C-004999-PTM2Y	$ 83.06	$ 72.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 2,000-4999	RN-ETP-C-004999-PTM3Y	$ 112.13	$ 97.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 2,000-4999	RN-ETP-C-004999-PTM4Y	$ 149.51	$ 130.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 2,000-4999	RN-ETP-C-004999-PTM5Y	$ 186.89	$ 162.59

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 2,000-4999	RN-ETP-C-004999-USG1Y	$ 41.53	$ 36.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 2,000-4999	RN-ETP-C-004999-USG2Y	$ 83.06	$ 72.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 2,000-4999	RN-ETP-C-004999-USG3Y	$ 112.13	$ 97.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 2,000-4999	RN-ETP-C-004999-USG4Y	$ 149.51	$ 130.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 2,000-4999	RN-ETP-C-004999-USG5Y	$ 186.89	$ 162.59
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 2,000-4999	RN-ETP-C-004999-USP1Y	$ 43.29	$ 37.66
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 2,000-4999	RN-ETP-C-004999-USP2Y	$ 86.58	$ 75.32
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 2,000-4999	RN-ETP-C-004999-USP3Y	$ 116.88	$ 101.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 2,000-4999	RN-ETP-C-004999-USP4Y	$ 155.84	$ 135.58
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 2,000-4999	RN-ETP-C-004999-USP5Y	$ 194.81	$ 169.48
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 5,000-9999	RN-ETP-C-009999-CAG1Y	$ 39.22	$ 34.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 5,000-9999	RN-ETP-C-009999-CAG2Y	$ 78.44	$ 68.24
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 5,000-9999	RN-ETP-C-009999-CAG3Y	$ 105.89	$ 92.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 5,000-9999	RN-ETP-C-009999-CAG4Y	$ 141.19	$ 122.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 5,000-9999	RN-ETP-C-009999-CAG5Y	$ 176.49	$ 153.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 5,000-9999	RN-ETP-C-009999-CAP1Y	$ 40.88	$ 35.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 5,000-9999	RN-ETP-C-009999-CAP2Y	$ 81.76	$ 71.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 5,000-9999	RN-ETP-C-009999-CAP3Y	$ 110.38	$ 96.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 5,000-9999	RN-ETP-C-009999-CAP4Y	$ 147.17	$ 128.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 5,000-9999	RN-ETP-C-009999-CAP5Y	$ 183.96	$ 160.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 5,000-9999	RN-ETP-C-009999-PPL1Y	$ 40.88	$ 35.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 5,000-9999	RN-ETP-C-009999-PPL2Y	$ 81.76	$ 71.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 5,000-9999	RN-ETP-C-009999-PPL3Y	$ 110.38	$ 96.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 5,000-9999	RN-ETP-C-009999-PPL4Y	$ 147.17	$ 128.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 5,000-9999	RN-ETP-C-009999-PPL5Y	$ 183.96	$ 160.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 5,000-9999	RN-ETP-C-009999-PTM1Y	$ 39.22	$ 34.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 5,000-9999	RN-ETP-C-009999-PTM2Y	$ 78.44	$ 68.24
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 5,000-9999	RN-ETP-C-009999-PTM3Y	$ 105.89	$ 92.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 5,000-9999	RN-ETP-C-009999-PTM4Y	$ 141.19	$ 122.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 5,000-9999	RN-ETP-C-009999-PTM5Y	$ 176.49	$ 153.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 5,000-9999	RN-ETP-C-009999-USG1Y	$ 39.22	$ 34.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 5,000-9999	RN-ETP-C-009999-USG2Y	$ 78.44	$ 68.24
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 5,000-9999	RN-ETP-C-009999-USG3Y	$ 105.89	$ 92.12
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 5,000-9999	RN-ETP-C-009999-USG4Y	$ 141.19	$ 122.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 5,000-9999	RN-ETP-C-009999-USG5Y	$ 176.49	$ 153.55
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 5,000-9999	RN-ETP-C-009999-USP1Y	$ 40.88	$ 35.57
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 5,000-9999	RN-ETP-C-009999-USP2Y	$ 81.76	$ 71.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 5,000-9999	RN-ETP-C-009999-USP3Y	$ 110.38	$ 96.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 5,000-9999	RN-ETP-C-009999-USP4Y	$ 147.17	$ 128.04
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 5,000-9999	RN-ETP-C-009999-USP5Y	$ 183.96	$ 160.05
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 10,000-19999	RN-ETP-C-019999-CAG1Y	$ 32.81	$ 28.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 10,000-19999	RN-ETP-C-019999-CAG2Y	$ 65.62	$ 57.09
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 10,000-19999	RN-ETP-C-019999-CAG3Y	$ 88.59	$ 77.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 10,000-19999	RN-ETP-C-019999-CAG4Y	$ 118.12	$ 102.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 10,000-19999	RN-ETP-C-019999-CAG5Y	$ 147.65	$ 128.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 10,000-19999	RN-ETP-C-019999-CAP1Y	$ 34.20	$ 29.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 10,000-19999	RN-ETP-C-019999-CAP2Y	$ 68.40	$ 59.51
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 10,000-19999	RN-ETP-C-019999-CAP3Y	$ 92.34	$ 80.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 10,000-19999	RN-ETP-C-019999-CAP4Y	$ 123.12	$ 107.11

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 10,000-19999	RN-ETP-C-019999-CAP5Y	$ 153.90	$ 133.89
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 10,000-19999	RN-ETP-C-019999-PPL1Y	$ 34.20	$ 29.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 10,000-19999	RN-ETP-C-019999-PPL2Y	$ 68.40	$ 59.51
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 10,000-19999	RN-ETP-C-019999-PPL3Y	$ 92.34	$ 80.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 10,000-19999	RN-ETP-C-019999-PPL4Y	$ 123.12	$ 107.11
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 10,000-19999	RN-ETP-C-019999-PPL5Y	$ 153.90	$ 133.89
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 10,000-19999	RN-ETP-C-019999-PTM1Y	$ 32.81	$ 28.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 10,000-19999	RN-ETP-C-019999-PTM2Y	$ 65.62	$ 57.09
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 10,000-19999	RN-ETP-C-019999-PTM3Y	$ 88.59	$ 77.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 10,000-19999	RN-ETP-C-019999-PTM4Y	$ 118.12	$ 102.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 10,000-19999	RN-ETP-C-019999-PTM5Y	$ 147.65	$ 128.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 10,000-19999	RN-ETP-C-019999-USG1Y	$ 32.81	$ 28.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 10,000-19999	RN-ETP-C-019999-USG2Y	$ 65.62	$ 57.09
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 10,000-19999	RN-ETP-C-019999-USG3Y	$ 88.59	$ 77.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 10,000-19999	RN-ETP-C-019999-USG4Y	$ 118.12	$ 102.76
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 10,000-19999	RN-ETP-C-019999-USG5Y	$ 147.65	$ 128.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 10,000-19999	RN-ETP-C-019999-USP1Y	$ 34.20	$ 29.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 10,000-19999	RN-ETP-C-019999-USP2Y	$ 68.40	$ 59.51
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 10,000-19999	RN-ETP-C-019999-USP3Y	$ 92.34	$ 80.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 10,000-19999	RN-ETP-C-019999-USP4Y	$ 123.12	$ 107.11
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 10,000-19999	RN-ETP-C-019999-USP5Y	$ 153.90	$ 133.89
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 20,000-49999	RN-ETP-C-049999-CAG1Y	$ 30.10	$ 26.19
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 20,000-49999	RN-ETP-C-049999-CAG2Y	$ 60.20	$ 52.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 20,000-49999	RN-ETP-C-049999-CAG3Y	$ 81.27	$ 70.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 20,000-49999	RN-ETP-C-049999-CAG4Y	$ 108.36	$ 94.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 20,000-49999	RN-ETP-C-049999-CAG5Y	$ 135.45	$ 117.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 20,000-49999	RN-ETP-C-049999-CAP1Y	$ 31.38	$ 27.30
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 20,000-49999	RN-ETP-C-049999-CAP2Y	$ 62.76	$ 54.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 20,000-49999	RN-ETP-C-049999-CAP3Y	$ 84.73	$ 73.72
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 20,000-49999	RN-ETP-C-049999-CAP4Y	$ 112.97	$ 98.28
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 20,000-49999	RN-ETP-C-049999-CAP5Y	$ 141.21	$ 122.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 20,000-49999	RN-ETP-C-049999-PPL1Y	$ 31.38	$ 27.30
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 20,000-49999	RN-ETP-C-049999-PPL2Y	$ 62.76	$ 54.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 20,000-49999	RN-ETP-C-049999-PPL3Y	$ 84.73	$ 73.72
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 20,000-49999	RN-ETP-C-049999-PPL4Y	$ 112.97	$ 98.28
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 20,000-49999	RN-ETP-C-049999-PPL5Y	$ 141.21	$ 122.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 20,000-49999	RN-ETP-C-049999-PTM1Y	$ 30.10	$ 26.19
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 20,000-49999	RN-ETP-C-049999-PTM2Y	$ 60.20	$ 52.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 20,000-49999	RN-ETP-C-049999-PTM3Y	$ 81.27	$ 70.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 20,000-49999	RN-ETP-C-049999-PTM4Y	$ 108.36	$ 94.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 20,000-49999	RN-ETP-C-049999-PTM5Y	$ 135.45	$ 117.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 20,000-49999	RN-ETP-C-049999-USG1Y	$ 30.10	$ 26.19
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 20,000-49999	RN-ETP-C-049999-USG2Y	$ 60.20	$ 52.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 20,000-49999	RN-ETP-C-049999-USG3Y	$ 81.27	$ 70.70
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 20,000-49999	RN-ETP-C-049999-USG4Y	$ 108.36	$ 94.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 20,000-49999	RN-ETP-C-049999-USG5Y	$ 135.45	$ 117.84
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 20,000-49999	RN-ETP-C-049999-USP1Y	$ 31.38	$ 27.30
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 20,000-49999	RN-ETP-C-049999-USP2Y	$ 62.76	$ 54.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 20,000-49999	RN-ETP-C-049999-USP3Y	$ 84.73	$ 73.72

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 20,000-49999	RN-ETP-C-049999-USP4Y	$ 112.97	$ 98.28
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 20,000-49999	RN-ETP-C-049999-USP5Y	$ 141.21	$ 122.85
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 50,000-74999	RN-ETP-C-074999-CAG1Y	$ 27.55	$ 23.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 50,000-74999	RN-ETP-C-074999-CAG2Y	$ 55.10	$ 47.94
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 50,000-74999	RN-ETP-C-074999-CAG3Y	$ 74.39	$ 64.72
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 50,000-74999	RN-ETP-C-074999-CAG4Y	$ 99.18	$ 86.29
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 50,000-74999	RN-ETP-C-074999-CAG5Y	$ 123.98	$ 107.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 50,000-74999	RN-ETP-C-074999-CAP1Y	$ 28.72	$ 24.99
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 50,000-74999	RN-ETP-C-074999-CAP2Y	$ 57.44	$ 49.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 50,000-74999	RN-ETP-C-074999-CAP3Y	$ 77.54	$ 67.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 50,000-74999	RN-ETP-C-074999-CAP4Y	$ 103.39	$ 89.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 50,000-74999	RN-ETP-C-074999-CAP5Y	$ 129.24	$ 112.44
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 50,000-74999	RN-ETP-C-074999-PPL1Y	$ 28.72	$ 24.99
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 50,000-74999	RN-ETP-C-074999-PPL2Y	$ 57.44	$ 49.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 50,000-74999	RN-ETP-C-074999-PPL3Y	$ 77.54	$ 67.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 50,000-74999	RN-ETP-C-074999-PPL4Y	$ 103.39	$ 89.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 50,000-74999	RN-ETP-C-074999-PPL5Y	$ 129.24	$ 112.44
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 50,000-74999	RN-ETP-C-074999-PTM1Y	$ 27.55	$ 23.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 50,000-74999	RN-ETP-C-074999-PTM2Y	$ 55.10	$ 47.94
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 50,000-74999	RN-ETP-C-074999-PTM3Y	$ 74.39	$ 64.72
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 50,000-74999	RN-ETP-C-074999-PTM4Y	$ 99.18	$ 86.29
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 50,000-74999	RN-ETP-C-074999-PTM5Y	$ 123.98	$ 107.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 50,000-74999	RN-ETP-C-074999-USG1Y	$ 27.55	$ 23.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 50,000-74999	RN-ETP-C-074999-USG2Y	$ 55.10	$ 47.94
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 50,000-74999	RN-ETP-C-074999-USG3Y	$ 74.39	$ 64.72
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 50,000-74999	RN-ETP-C-074999-USG4Y	$ 99.18	$ 86.29
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 50,000-74999	RN-ETP-C-074999-USG5Y	$ 123.98	$ 107.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 50,000-74999	RN-ETP-C-074999-USP1Y	$ 28.72	$ 24.99
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 50,000-74999	RN-ETP-C-074999-USP2Y	$ 57.44	$ 49.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 50,000-74999	RN-ETP-C-074999-USP3Y	$ 77.54	$ 67.46
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 50,000-74999	RN-ETP-C-074999-USP4Y	$ 103.39	$ 89.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 50,000-74999	RN-ETP-C-074999-USP5Y	$ 129.24	$ 112.44
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 75,000-99999	RN-ETP-C-099999-CAG1Y	$ 24.44	$ 21.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 75,000-99999	RN-ETP-C-099999-CAG2Y	$ 48.88	$ 42.53
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 75,000-99999	RN-ETP-C-099999-CAG3Y	$ 65.99	$ 57.41
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 75,000-99999	RN-ETP-C-099999-CAG4Y	$ 87.98	$ 76.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 75,000-99999	RN-ETP-C-099999-CAG5Y	$ 109.98	$ 95.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 75,000-99999	RN-ETP-C-099999-CAP1Y	$ 25.48	$ 22.17
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 75,000-99999	RN-ETP-C-099999-CAP2Y	$ 50.96	$ 44.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 75,000-99999	RN-ETP-C-099999-CAP3Y	$ 68.80	$ 59.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 75,000-99999	RN-ETP-C-099999-CAP4Y	$ 91.73	$ 79.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 75,000-99999	RN-ETP-C-099999-CAP5Y	$ 114.66	$ 99.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 75,000-99999	RN-ETP-C-099999-PPL1Y	$ 25.48	$ 22.17
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 75,000-99999	RN-ETP-C-099999-PPL2Y	$ 50.96	$ 44.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 75,000-99999	RN-ETP-C-099999-PPL3Y	$ 68.80	$ 59.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 75,000-99999	RN-ETP-C-099999-PPL4Y	$ 91.73	$ 79.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 75,000-99999	RN-ETP-C-099999-PPL5Y	$ 114.66	$ 99.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 75,000-99999	RN-ETP-C-099999-PTM1Y	$ 24.44	$ 21.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 75,000-99999	RN-ETP-C-099999-PTM2Y	$ 48.88	$ 42.53

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 75,000-99999	RN-ETP-C-099999-PTM3Y	$ 65.99	$ 57.41
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 75,000-99999	RN-ETP-C-099999-PTM4Y	$ 87.98	$ 76.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 75,000-99999	RN-ETP-C-099999-PTM5Y	$ 109.98	$ 95.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 75,000-99999	RN-ETP-C-099999-USG1Y	$ 24.44	$ 21.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 75,000-99999	RN-ETP-C-099999-USG2Y	$ 48.88	$ 42.53
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 75,000-99999	RN-ETP-C-099999-USG3Y	$ 65.99	$ 57.41
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 75,000-99999	RN-ETP-C-099999-USG4Y	$ 87.98	$ 76.54
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 75,000-99999	RN-ETP-C-099999-USG5Y	$ 109.98	$ 95.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 75,000-99999	RN-ETP-C-099999-USP1Y	$ 25.48	$ 22.17
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 75,000-99999	RN-ETP-C-099999-USP2Y	$ 50.96	$ 44.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 75,000-99999	RN-ETP-C-099999-USP3Y	$ 68.80	$ 59.86
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 75,000-99999	RN-ETP-C-099999-USP4Y	$ 91.73	$ 79.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 75,000-99999	RN-ETP-C-099999-USP5Y	$ 114.66	$ 99.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 100,000-199999	RN-ETP-C-199999-CAG1Y	$ 20.84	$ 18.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 100,000-199999	RN-ETP-C-199999-CAG2Y	$ 41.68	$ 36.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 100,000-199999	RN-ETP-C-199999-CAG3Y	$ 56.27	$ 48.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 100,000-199999	RN-ETP-C-199999-CAG4Y	$ 75.02	$ 65.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 100,000-199999	RN-ETP-C-199999-CAG5Y	$ 93.78	$ 81.59
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 100,000-199999	RN-ETP-C-199999-CAP1Y	$ 21.72	$ 18.90
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 100,000-199999	RN-ETP-C-199999-CAP2Y	$ 43.44	$ 37.79
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 100,000-199999	RN-ETP-C-199999-CAP3Y	$ 58.64	$ 51.02
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 100,000-199999	RN-ETP-C-199999-CAP4Y	$ 78.19	$ 68.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 100,000-199999	RN-ETP-C-199999-CAP5Y	$ 97.74	$ 85.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 100,000-199999	RN-ETP-C-199999-PPL1Y	$ 21.72	$ 18.90
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 100,000-199999	RN-ETP-C-199999-PPL2Y	$ 43.44	$ 37.79
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 100,000-199999	RN-ETP-C-199999-PPL3Y	$ 58.64	$ 51.02
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 100,000-199999	RN-ETP-C-199999-PPL4Y	$ 78.19	$ 68.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 100,000-199999	RN-ETP-C-199999-PPL5Y	$ 97.74	$ 85.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 100,000-199999	RN-ETP-C-199999-PTM1Y	$ 20.84	$ 18.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 100,000-199999	RN-ETP-C-199999-PTM2Y	$ 41.68	$ 36.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 100,000-199999	RN-ETP-C-199999-PTM3Y	$ 56.27	$ 48.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 100,000-199999	RN-ETP-C-199999-PTM4Y	$ 75.02	$ 65.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 100,000-199999	RN-ETP-C-199999-PTM5Y	$ 93.78	$ 81.59
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 100,000-199999	RN-ETP-C-199999-USG1Y	$ 20.84	$ 18.13
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 100,000-199999	RN-ETP-C-199999-USG2Y	$ 41.68	$ 36.26
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 100,000-199999	RN-ETP-C-199999-USG3Y	$ 56.27	$ 48.95
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 100,000-199999	RN-ETP-C-199999-USG4Y	$ 75.02	$ 65.27
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 100,000-199999	RN-ETP-C-199999-USG5Y	$ 93.78	$ 81.59
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 100,000-199999	RN-ETP-C-199999-USP1Y	$ 21.72	$ 18.90
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 100,000-199999	RN-ETP-C-199999-USP2Y	$ 43.44	$ 37.79
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 100,000-199999	RN-ETP-C-199999-USP3Y	$ 58.64	$ 51.02
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 100,000-199999	RN-ETP-C-199999-USP4Y	$ 78.19	$ 68.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 100,000-199999	RN-ETP-C-199999-USP5Y	$ 97.74	$ 85.03
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 1 Year 200,000+	RN-ETP-C-200000+CAG1Y	$ 19.50	$ 16.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 2 Year 200,000+	RN-ETP-C-200000+CAG2Y	$ 39.00	$ 33.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 3 Year 200,000+	RN-ETP-C-200000+CAG3Y	$ 52.65	$ 45.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 4 Year 200,000+	RN-ETP-C-200000+CAG4Y	$ 70.20	$ 61.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA 5 Year 200,000+	RN-ETP-C-200000+CAG5Y	$ 87.75	$ 76.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 1 Year 200,000+	RN-ETP-C-200000+CAP1Y	$ 20.33	$ 17.69

FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 2 Year 200,000+	RN-ETP-C-200000+CAP2Y	$ 40.66	$ 35.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 3 Year 200,000+	RN-ETP-C-200000+CAP3Y	$ 54.89	$ 47.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 4 Year 200,000+	RN-ETP-C-200000+CAP4Y	$ 73.19	$ 63.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov CA Plat Prio Plus 5 Year 200,000+	RN-ETP-C-200000+CAP5Y	$ 91.49	$ 79.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 1 Year 200,000+	RN-ETP-C-200000+PPL1Y	$ 20.33	$ 17.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 2 Year 200,000+	RN-ETP-C-200000+PPL2Y	$ 40.66	$ 35.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 3 Year 200,000+	RN-ETP-C-200000+PPL3Y	$ 54.89	$ 47.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 4 Year 200,000+	RN-ETP-C-200000+PPL4Y	$ 73.19	$ 63.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Plat Prio Plus Support 5 Year 200,000+	RN-ETP-C-200000+PPL5Y	$ 91.49	$ 79.60
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 1 Year 200,000+	RN-ETP-C-200000+PTM1Y	$ 19.50	$ 16.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 2 Year 200,000+	RN-ETP-C-200000+PTM2Y	$ 39.00	$ 33.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 3 Year 200,000+	RN-ETP-C-200000+PTM3Y	$ 52.65	$ 45.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 4 Year 200,000+	RN-ETP-C-200000+PTM4Y	$ 70.20	$ 61.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Platinum Support 5 Year 200,000+	RN-ETP-C-200000+PTM5Y	$ 87.75	$ 76.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 1 Year 200,000+	RN-ETP-C-200000+USG1Y	$ 19.50	$ 16.97
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 2 Year 200,000+	RN-ETP-C-200000+USG2Y	$ 39.00	$ 33.93
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 3 Year 200,000+	RN-ETP-C-200000+USG3Y	$ 52.65	$ 45.81
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 4 Year 200,000+	RN-ETP-C-200000+USG4Y	$ 70.20	$ 61.07
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US 5 Year 200,000+	RN-ETP-C-200000+USG5Y	$ 87.75	$ 76.34
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 1 Year 200,000+	RN-ETP-C-200000+USP1Y	$ 20.33	$ 17.69
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 2 Year 200,000+	RN-ETP-C-200000+USP2Y	$ 40.66	$ 35.37
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 3 Year 200,000+	RN-ETP-C-200000+USP3Y	$ 54.89	$ 47.75
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 4 Year 200,000+	RN-ETP-C-200000+USP4Y	$ 73.19	$ 63.68
FireEye	Renewal-Email Threat Prevention Cloud with AV/AS & Gov US Plat Prio Plus 5 Year 200,000+	RN-ETP-C-200000+USP5Y	$ 91.49	$ 79.60
FireEye	Online Web Training-30-day access to eLearning, self-paced, course on Email Threat Prevention Cloud Deployment	EDU-OWT-BSC-ETP	$ 295.00	$ 256.65
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 1-249	ETP-000249-PPL1Y	$ 74.52	$ 64.83
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 1-249	ETP-000249-PPL2Y	$ 149.04	$ 129.66
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 1-249	ETP-000249-PPL3Y	$ 201.20	$ 175.04
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 1-249	ETP-000249-PPL4Y	$ 268.27	$ 233.39
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 1-249	ETP-000249-PPL5Y	$ 335.34	$ 291.75
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 1-249	ETP-000249-USP1Y	$ 74.52	$ 64.83
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 1-249	ETP-000249-USP2Y	$ 149.04	$ 129.66
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 1-249	ETP-000249-USP3Y	$ 201.20	$ 175.04
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 1-249	ETP-000249-USP4Y	$ 268.27	$ 233.39
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 1-249	ETP-000249-USP5Y	$ 335.34	$ 291.75
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 250-499	ETP-000499-PPL1Y	$ 61.52	$ 53.52
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 250-499	ETP-000499-PPL2Y	$ 123.04	$ 107.04
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 250-499	ETP-000499-PPL3Y	$ 166.10	$ 144.51
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 250-499	ETP-000499-PPL4Y	$ 221.47	$ 192.68
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 250-499	ETP-000499-PPL5Y	$ 276.84	$ 240.85
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 250-499	ETP-000499-USP1Y	$ 61.52	$ 53.52
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 250-499	ETP-000499-USP2Y	$ 123.04	$ 107.04
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 250-499	ETP-000499-USP3Y	$ 166.10	$ 144.51
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 250-499	ETP-000499-USP4Y	$ 221.47	$ 192.68
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 250-499	ETP-000499-USP5Y	$ 276.84	$ 240.85
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 500-749	ETP-000749-PPL1Y	$ 52.77	$ 45.91
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 500-749	ETP-000749-PPL2Y	$ 105.54	$ 91.82
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 500-749	ETP-000749-PPL3Y	$ 142.48	$ 123.96
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 500-749	ETP-000749-PPL4Y	$ 189.97	$ 165.27

FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 500-749	ETP-000749-PPL5Y	$ 237.47	$ 206.60
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 500-749	ETP-000749-USP1Y	$ 52.77	$ 45.91
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 500-749	ETP-000749-USP2Y	$ 105.54	$ 91.82
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 500-749	ETP-000749-USP3Y	$ 142.48	$ 123.96
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 500-749	ETP-000749-USP4Y	$ 189.97	$ 165.27
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 500-749	ETP-000749-USP5Y	$ 237.47	$ 206.60
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 750-999	ETP-000999-PPL1Y	$ 44.32	$ 38.56
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 750-999	ETP-000999-PPL2Y	$ 88.64	$ 77.12
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 750-999	ETP-000999-PPL3Y	$ 119.66	$ 104.10
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 750-999	ETP-000999-PPL4Y	$ 159.55	$ 138.81
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 750-999	ETP-000999-PPL5Y	$ 199.44	$ 173.51
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 750-999	ETP-000999-USP1Y	$ 44.32	$ 38.56
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 750-999	ETP-000999-USP2Y	$ 88.64	$ 77.12
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 750-999	ETP-000999-USP3Y	$ 119.66	$ 104.10
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 750-999	ETP-000999-USP4Y	$ 159.55	$ 138.81
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 750-999	ETP-000999-USP5Y	$ 199.44	$ 173.51
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 1,000-1999	ETP-001999-PPL1Y	$ 40.20	$ 34.97
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 1,000-1999	ETP-001999-PPL2Y	$ 80.40	$ 69.95
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 1,000-1999	ETP-001999-PPL3Y	$ 108.54	$ 94.43
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 1,000-1999	ETP-001999-PPL4Y	$ 144.72	$ 125.91
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 1,000-1999	ETP-001999-PPL5Y	$ 180.90	$ 157.38
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 1,000-1999	ETP-001999-USP1Y	$ 40.20	$ 34.97
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 1,000-1999	ETP-001999-USP2Y	$ 80.40	$ 69.95
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 1,000-1999	ETP-001999-USP3Y	$ 108.54	$ 94.43
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 1,000-1999	ETP-001999-USP4Y	$ 144.72	$ 125.91
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 1,000-1999	ETP-001999-USP5Y	$ 180.90	$ 157.38
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 2,000-4999	ETP-004999-PPL1Y	$ 36.59	$ 31.83
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 2,000-4999	ETP-004999-PPL2Y	$ 73.18	$ 63.67
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 2,000-4999	ETP-004999-PPL3Y	$ 98.79	$ 85.95
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 2,000-4999	ETP-004999-PPL4Y	$ 131.72	$ 114.60
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 2,000-4999	ETP-004999-PPL5Y	$ 164.66	$ 143.25
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 2,000-4999	ETP-004999-USP1Y	$ 36.59	$ 31.83
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 2,000-4999	ETP-004999-USP2Y	$ 73.18	$ 63.67
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 2,000-4999	ETP-004999-USP3Y	$ 98.79	$ 85.95
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 2,000-4999	ETP-004999-USP4Y	$ 131.72	$ 114.60
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 2,000-4999	ETP-004999-USP5Y	$ 164.66	$ 143.25
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 5,000-9999	ETP-009999-PPL1Y	$ 32.59	$ 28.35
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 5,000-9999	ETP-009999-PPL2Y	$ 65.18	$ 56.71
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 5,000-9999	ETP-009999-PPL3Y	$ 87.99	$ 76.55
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 5,000-9999	ETP-009999-PPL4Y	$ 117.32	$ 102.07
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 5,000-9999	ETP-009999-PPL5Y	$ 146.66	$ 127.59
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 5,000-9999	ETP-009999-USP1Y	$ 32.59	$ 28.35
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 5,000-9999	ETP-009999-USP2Y	$ 65.18	$ 56.71
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 5,000-9999	ETP-009999-USP3Y	$ 87.99	$ 76.55
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 5,000-9999	ETP-009999-USP4Y	$ 117.32	$ 102.07
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 5,000-9999	ETP-009999-USP5Y	$ 146.66	$ 127.59
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 10,000-19999	ETP-019999-PPL1Y	$ 28.13	$ 24.47
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 10,000-19999	ETP-019999-PPL2Y	$ 56.26	$ 48.95
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 10,000-19999	ETP-019999-PPL3Y	$ 75.95	$ 66.08

FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 10,000-19999	ETP-019999-PPL4Y	$ 101.27	$ 88.10
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 10,000-19999	ETP-019999-PPL5Y	$ 126.59	$ 110.13
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 10,000-19999	ETP-019999-USP1Y	$ 28.13	$ 24.47
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 10,000-19999	ETP-019999-USP2Y	$ 56.26	$ 48.95
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 10,000-19999	ETP-019999-USP3Y	$ 75.95	$ 66.08
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 10,000-19999	ETP-019999-USP4Y	$ 101.27	$ 88.10
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 10,000-19999	ETP-019999-USP5Y	$ 126.59	$ 110.13
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 20,000-49999	ETP-049999-PPL1Y	$ 26.53	$ 23.08
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 20,000-49999	ETP-049999-PPL2Y	$ 53.06	$ 46.16
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 20,000-49999	ETP-049999-PPL3Y	$ 71.63	$ 62.32
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 20,000-49999	ETP-049999-PPL4Y	$ 95.51	$ 83.09
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 20,000-49999	ETP-049999-PPL5Y	$ 119.39	$ 103.87
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 20,000-49999	ETP-049999-USP1Y	$ 26.53	$ 23.08
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 20,000-49999	ETP-049999-USP2Y	$ 53.06	$ 46.16
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 20,000-49999	ETP-049999-USP3Y	$ 71.63	$ 62.32
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 20,000-49999	ETP-049999-USP4Y	$ 95.51	$ 83.09
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 20,000-49999	ETP-049999-USP5Y	$ 119.39	$ 103.87
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 50,000-74999	ETP-074999-PPL1Y	$ 23.96	$ 20.85
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 50,000-74999	ETP-074999-PPL2Y	$ 47.92	$ 41.69
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 50,000-74999	ETP-074999-PPL3Y	$ 64.69	$ 56.28
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 50,000-74999	ETP-074999-PPL4Y	$ 86.26	$ 75.05
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 50,000-74999	ETP-074999-PPL5Y	$ 107.82	$ 93.80
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 50,000-74999	ETP-074999-USP1Y	$ 23.96	$ 20.85
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 50,000-74999	ETP-074999-USP2Y	$ 47.92	$ 41.69
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 50,000-74999	ETP-074999-USP3Y	$ 64.69	$ 56.28
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 50,000-74999	ETP-074999-USP4Y	$ 86.26	$ 75.05
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 50,000-74999	ETP-074999-USP5Y	$ 107.82	$ 93.80
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 75,000-99999	ETP-099999-PPL1Y	$ 20.72	$ 18.03
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 75,000-99999	ETP-099999-PPL2Y	$ 41.44	$ 36.05
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 75,000-99999	ETP-099999-PPL3Y	$ 55.94	$ 48.67
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 75,000-99999	ETP-099999-PPL4Y	$ 74.59	$ 64.89
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 75,000-99999	ETP-099999-PPL5Y	$ 93.24	$ 81.12
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 75,000-99999	ETP-099999-USP1Y	$ 20.72	$ 18.03
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 75,000-99999	ETP-099999-USP2Y	$ 41.44	$ 36.05
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 75,000-99999	ETP-099999-USP3Y	$ 55.94	$ 48.67
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 75,000-99999	ETP-099999-USP4Y	$ 74.59	$ 64.89
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 75,000-99999	ETP-099999-USP5Y	$ 93.24	$ 81.12
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 100,000-199999	ETP-199999-PPL1Y	$ 18.22	$ 15.85
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 100,000-199999	ETP-199999-PPL2Y	$ 36.44	$ 31.70
FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 100,000-199999	ETP-199999-PPL3Y	$ 49.19	$ 42.80
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 100,000-199999	ETP-199999-PPL4Y	$ 65.59	$ 57.06
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 100,000-199999	ETP-199999-PPL5Y	$ 81.99	$ 71.33
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 100,000-199999	ETP-199999-USP1Y	$ 18.22	$ 15.85
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 100,000-199999	ETP-199999-USP2Y	$ 36.44	$ 31.70
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 100,000-199999	ETP-199999-USP3Y	$ 49.19	$ 42.80
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 100,000-199999	ETP-199999-USP4Y	$ 65.59	$ 57.06
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 100,000-199999	ETP-199999-USP5Y	$ 81.99	$ 71.33
FireEye	Email Threat Prevention, Plat Prio Plus Support 1 Year 200,000+	ETP-200000+PPL1Y	$ 17.20	$ 14.96
FireEye	Email Threat Prevention, Plat Prio Plus Support 2 Year 200,000+	ETP-200000+PPL2Y	$ 34.40	$ 29.93

FireEye	Email Threat Prevention, Plat Prio Plus Support 3 Year 200,000+	ETP-200000+PPL3Y	$ 46.44	$ 40.40
FireEye	Email Threat Prevention, Plat Prio Plus Support 4 Year 200,000+	ETP-200000+PPL4Y	$ 61.92	$ 53.87
FireEye	Email Threat Prevention, Plat Prio Plus Support 5 Year 200,000+	ETP-200000+PPL5Y	$ 77.40	$ 67.34
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 1 Year 200,000+	ETP-200000+USP1Y	$ 17.20	$ 14.96
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 2 Year 200,000+	ETP-200000+USP2Y	$ 34.40	$ 29.93
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 3 Year 200,000+	ETP-200000+USP3Y	$ 46.44	$ 40.40
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 4 Year 200,000+	ETP-200000+USP4Y	$ 61.92	$ 53.87
FireEye	Email Threat Prevention, Gov US Plat Prio Plus 5 Year 200,000+	ETP-200000+USP5Y	$ 77.40	$ 67.34
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 1-249	RN-ETP-000249-PPL1Y	$ 74.52	$ 64.83
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 1-249	RN-ETP-000249-PPL2Y	$ 149.04	$ 129.66
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 1-249	RN-ETP-000249-PPL3Y	$ 201.20	$ 175.04
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 1-249	RN-ETP-000249-PPL4Y	$ 268.27	$ 233.39
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 1-249	RN-ETP-000249-USP1Y	$ 74.52	$ 64.83
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 1-249	RN-ETP-000249-USP2Y	$ 149.04	$ 129.66
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 1-249	RN-ETP-000249-USP3Y	$ 201.20	$ 175.04
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 1-249	RN-ETP-000249-USP4Y	$ 268.27	$ 233.39
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 250-499	RN-ETP-000499-PPL1Y	$ 61.52	$ 53.52
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 250-499	RN-ETP-000499-PPL2Y	$ 123.04	$ 107.04
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 250-499	RN-ETP-000499-PPL3Y	$ 166.10	$ 144.51
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 250-499	RN-ETP-000499-PPL4Y	$ 221.47	$ 192.68
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 250-499	RN-ETP-000499-USP1Y	$ 61.52	$ 53.52
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 250-499	RN-ETP-000499-USP2Y	$ 123.04	$ 107.04
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 250-499	RN-ETP-000499-USP3Y	$ 166.10	$ 144.51
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 250-499	RN-ETP-000499-USP4Y	$ 221.47	$ 192.68
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 500-749	RN-ETP-000749-PPL1Y	$ 52.77	$ 45.91
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 500-749	RN-ETP-000749-PPL2Y	$ 105.54	$ 91.82
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 500-749	RN-ETP-000749-PPL3Y	$ 142.48	$ 123.96
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 500-749	RN-ETP-000749-PPL4Y	$ 189.97	$ 165.27
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 500-749	RN-ETP-000749-USP1Y	$ 52.77	$ 45.91
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 500-749	RN-ETP-000749-USP2Y	$ 105.54	$ 91.82
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 500-749	RN-ETP-000749-USP3Y	$ 142.48	$ 123.96
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 500-749	RN-ETP-000749-USP4Y	$ 189.97	$ 165.27
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 750-999	RN-ETP-000999-PPL1Y	$ 44.32	$ 38.56
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 750-999	RN-ETP-000999-PPL2Y	$ 88.64	$ 77.12
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 750-999	RN-ETP-000999-PPL3Y	$ 119.66	$ 104.10
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 750-999	RN-ETP-000999-PPL4Y	$ 159.55	$ 138.81
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 750-999	RN-ETP-000999-USP1Y	$ 44.32	$ 38.56
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 750-999	RN-ETP-000999-USP2Y	$ 88.64	$ 77.12
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 750-999	RN-ETP-000999-USP3Y	$ 119.66	$ 104.10
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 750-999	RN-ETP-000999-USP4Y	$ 159.55	$ 138.81
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 1,000-1999	RN-ETP-001999-PPL1Y	$ 40.20	$ 34.97
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 1,000-1999	RN-ETP-001999-PPL2Y	$ 80.40	$ 69.95
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 1,000-1999	RN-ETP-001999-PPL3Y	$ 108.54	$ 94.43
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 1,000-1999	RN-ETP-001999-PPL4Y	$ 144.72	$ 125.91
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 1,000-1999	RN-ETP-001999-USP1Y	$ 40.20	$ 34.97
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 1,000-1999	RN-ETP-001999-USP2Y	$ 80.40	$ 69.95
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 1,000-1999	RN-ETP-001999-USP3Y	$ 108.54	$ 94.43
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 1,000-1999	RN-ETP-001999-USP4Y	$ 144.72	$ 125.91
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 2,000-4999	RN-ETP-004999-PPL1Y	$ 36.59	$ 31.83

FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 2,000-4999	RN-ETP-004999-PPL2Y	$ 73.18	$ 63.67
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 2,000-4999	RN-ETP-004999-PPL3Y	$ 98.79	$ 85.95
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 2,000-4999	RN-ETP-004999-PPL4Y	$ 131.72	$ 114.60
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 2,000-4999	RN-ETP-004999-USP1Y	$ 36.59	$ 31.83
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 2,000-4999	RN-ETP-004999-USP2Y	$ 73.18	$ 63.67
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 2,000-4999	RN-ETP-004999-USP3Y	$ 98.79	$ 85.95
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 2,000-4999	RN-ETP-004999-USP4Y	$ 131.72	$ 114.60
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 5,000-9999	RN-ETP-009999-PPL1Y	$ 32.59	$ 28.35
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 5,000-9999	RN-ETP-009999-PPL2Y	$ 65.18	$ 56.71
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 5,000-9999	RN-ETP-009999-PPL3Y	$ 87.99	$ 76.55
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 5,000-9999	RN-ETP-009999-PPL4Y	$ 117.32	$ 102.07
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 5,000-9999	RN-ETP-009999-USP1Y	$ 32.59	$ 28.35
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 5,000-9999	RN-ETP-009999-USP2Y	$ 65.18	$ 56.71
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 5,000-9999	RN-ETP-009999-USP3Y	$ 87.99	$ 76.55
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 5,000-9999	RN-ETP-009999-USP4Y	$ 117.32	$ 102.07
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 10,000-19999	RN-ETP-019999-PPL1Y	$ 28.13	$ 24.47
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 10,000-19999	RN-ETP-019999-PPL2Y	$ 56.26	$ 48.95
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 10,000-19999	RN-ETP-019999-PPL3Y	$ 75.95	$ 66.08
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 10,000-19999	RN-ETP-019999-PPL4Y	$ 101.27	$ 88.10
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 10,000-19999	RN-ETP-019999-USP1Y	$ 28.13	$ 24.47
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 10,000-19999	RN-ETP-019999-USP2Y	$ 56.26	$ 48.95
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 10,000-19999	RN-ETP-019999-USP3Y	$ 75.95	$ 66.08
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 10,000-19999	RN-ETP-019999-USP4Y	$ 101.27	$ 88.10
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 20,000-49999	RN-ETP-049999-PPL1Y	$ 26.53	$ 23.08
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 20,000-49999	RN-ETP-049999-PPL2Y	$ 53.06	$ 46.16
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 20,000-49999	RN-ETP-049999-PPL3Y	$ 71.63	$ 62.32
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 20,000-49999	RN-ETP-049999-PPL4Y	$ 95.51	$ 83.09
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 20,000-49999	RN-ETP-049999-USP1Y	$ 26.53	$ 23.08
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 20,000-49999	RN-ETP-049999-USP2Y	$ 53.06	$ 46.16
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 20,000-49999	RN-ETP-049999-USP3Y	$ 71.63	$ 62.32
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 20,000-49999	RN-ETP-049999-USP4Y	$ 95.51	$ 83.09
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 50,000-74999	RN-ETP-074999-PPL1Y	$ 23.96	$ 20.85
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 50,000-74999	RN-ETP-074999-PPL2Y	$ 47.92	$ 41.69
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 50,000-74999	RN-ETP-074999-PPL3Y	$ 64.69	$ 56.28
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 50,000-74999	RN-ETP-074999-PPL4Y	$ 86.26	$ 75.05
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 50,000-74999	RN-ETP-074999-USP1Y	$ 23.96	$ 20.85
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 50,000-74999	RN-ETP-074999-USP2Y	$ 47.92	$ 41.69
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 50,000-74999	RN-ETP-074999-USP3Y	$ 64.69	$ 56.28
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 50,000-74999	RN-ETP-074999-USP4Y	$ 86.26	$ 75.05
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 75,000-99999	RN-ETP-099999-PPL1Y	$ 20.72	$ 18.03
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 75,000-99999	RN-ETP-099999-PPL2Y	$ 41.44	$ 36.05
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 75,000-99999	RN-ETP-099999-PPL3Y	$ 55.94	$ 48.67
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 75,000-99999	RN-ETP-099999-PPL4Y	$ 74.59	$ 64.89
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 75,000-99999	RN-ETP-099999-USP1Y	$ 20.72	$ 18.03
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 75,000-99999	RN-ETP-099999-USP2Y	$ 41.44	$ 36.05
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 75,000-99999	RN-ETP-099999-USP3Y	$ 55.94	$ 48.67
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 75,000-99999	RN-ETP-099999-USP4Y	$ 74.59	$ 64.89
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 100,000-199999	RN-ETP-199999-PPL1Y	$ 18.22	$ 15.85
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 100,000-199999	RN-ETP-199999-PPL2Y	$ 36.44	$ 31.70

FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 100,000-199999	RN-ETP-199999-PPL3Y	$ 49.19	$ 42.80
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 100,000-199999	RN-ETP-199999-PPL4Y	$ 65.59	$ 57.06
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 100,000-199999	RN-ETP-199999-USP1Y	$ 18.22	$ 15.85
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 100,000-199999	RN-ETP-199999-USP2Y	$ 36.44	$ 31.70
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 100,000-199999	RN-ETP-199999-USP3Y	$ 49.19	$ 42.80
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 100,000-199999	RN-ETP-199999-USP4Y	$ 65.59	$ 57.06
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 1 Year 200,000+	RN-ETP-200000+PPL1Y	$ 17.20	$ 14.96
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 2 Year 200,000+	RN-ETP-200000+PPL2Y	$ 34.40	$ 29.93
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 3 Year 200,000+	RN-ETP-200000+PPL3Y	$ 46.44	$ 40.40
FireEye	Renewal-Email Threat Prevention, Plat Prio Plus Support 4 Year 200,000+	RN-ETP-200000+PPL4Y	$ 61.92	$ 53.87
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 1 Year 200,000+	RN-ETP-200000+USP1Y	$ 17.20	$ 14.96
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 2 Year 200,000+	RN-ETP-200000+USP2Y	$ 34.40	$ 29.93
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 3 Year 200,000+	RN-ETP-200000+USP3Y	$ 46.44	$ 40.40
FireEye	Renewal-Email Threat Prevention, Gov US Plat Prio Plus 4 Year 200,000+	RN-ETP-200000+USP4Y	$ 61.92	$ 53.87
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 1-249	RN-ETP-000249-PTM2Y	$ 116.64	$ 101.48
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 1-249	RN-ETP-000249-USG2Y	$ 116.64	$ 101.48
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 250-499	RN-ETP-000499-PTM2Y	$ 96.30	$ 83.78
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 250-499	RN-ETP-000499-USG2Y	$ 96.30	$ 83.78
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 500-749	RN-ETP-000749-PTM2Y	$ 82.60	$ 71.86
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 500-749	RN-ETP-000749-USG2Y	$ 82.60	$ 71.86
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 750-999	RN-ETP-000999-PTM2Y	$ 69.38	$ 60.36
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 750-999	RN-ETP-000999-USG2Y	$ 69.38	$ 60.36
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 1,000-1999	RN-ETP-001999-PTM2Y	$ 62.92	$ 54.74
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 1,000-1999	RN-ETP-001999-USG2Y	$ 62.92	$ 54.74
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 2,000-4999	RN-ETP-004999-PTM2Y	$ 57.28	$ 49.83
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 2,000-4999	RN-ETP-004999-USG2Y	$ 57.28	$ 49.83
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 5,000-9999	RN-ETP-009999-PTM2Y	$ 51.02	$ 44.39
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 5,000-9999	RN-ETP-009999-USG2Y	$ 51.02	$ 44.39
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 10,000-19999	RN-ETP-019999-PTM2Y	$ 44.04	$ 38.31
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 10,000-19999	RN-ETP-019999-USG2Y	$ 44.04	$ 38.31
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 20,000-49999	RN-ETP-049999-PTM2Y	$ 41.52	$ 36.12
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 20,000-49999	RN-ETP-049999-USG2Y	$ 41.52	$ 36.12
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 50,000-74999	RN-ETP-074999-PTM2Y	$ 37.50	$ 32.63
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 50,000-74999	RN-ETP-074999-USG2Y	$ 37.50	$ 32.63
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 75,000-99999	RN-ETP-099999-PTM2Y	$ 32.44	$ 28.22
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 75,000-99999	RN-ETP-099999-USG2Y	$ 32.44	$ 28.22
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 100,000-199999	RN-ETP-199999-PTM2Y	$ 28.52	$ 24.81
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 100,000-199999	RN-ETP-199999-USG2Y	$ 28.52	$ 24.81
FireEye	Renewal-Email Threat Prevention, Platinum Support 2 Year 200,000+	RN-ETP-200000+PTM2Y	$ 26.92	$ 23.42
FireEye	Renewal-Email Threat Prevention, Government US 2 Year 200,000+	RN-ETP-200000+USG2Y	$ 26.92	$ 23.42
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Platinum Support 1 Year	ETP-C-PROMO-PTM1Y	$ 25.00	$ 21.75
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Plat Prio Plus Support 1 Year	ETP-C-PROMO-PPL1Y	$ 26.06	$ 22.67
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Gov CA 1 Year	ETP-C-PROMO-CAG1Y	$ 25.00	$ 21.75
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Gov CA Plat Prio Plus 1 Year	ETP-C-PROMO-CAP1Y	$ 26.06	$ 22.67
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Gov US 1 Year	ETP-C-PROMO-USG1Y	$ 25.00	$ 21.75
FireEye	Email Threat Prevention Cloud with AV/AS 1 User & Gov US Plat Prio Plus 1 Year	ETP-C-PROMO-USP1Y	$ 26.06	$ 22.67
FireEye	Professional services custom SKU	PS-OS-CUST	Call for quote	#VALUE!
FireEye	Onsite professional services - includes FTE for 5 days a week for 6 months of services - No travel included - if travel is required please include travel SKU.	PS-OS-LTSER	$ 192,000.00	$ 174,720.00
FireEye	Onsite professional services - includes 40 hrs of services, 4 hrs of proj mgmt AND travel expenses within country. Any travel out of country will require th	PS-OS-T	$ 15,040.00	$ 13,686.40

FireEye	Professional services travel SKU	PS-OS-TRAVEL	$ 500.00	$ 455.00
FireEye	Online Web Training-FireEye Product Overview	EDU-OWT-BSC-OV	$ -	$ -
FireEye	Managed Defense Continuous Vigilance 1 Year 1-249	MDCV-002491Y	$ 1,296.00	$ 1,127.52
FireEye	Managed Defense Continuous Vigilance 2 Year 1-249	MDCV-002492Y	$ 2,592.00	$ 2,255.04
FireEye	Managed Defense Continuous Vigilance 3 Year 1-249	MDCV-002493Y	$ 3,888.00	$ 3,382.56
FireEye	Managed Defense Continuous Vigilance 4 Year 1-249	MDCV-002494Y	$ 5,184.00	$ 4,510.08
FireEye	Managed Defense Continuous Vigilance 5 Year 1-249	MDCV-002495Y	$ 6,480.00	$ 5,637.60
FireEye	Managed Defense Continuous Vigilance 1 Year 250-499	MDCV-004991Y	$ 656.54	$ 571.19
FireEye	Managed Defense Continuous Vigilance 2 Year 250-499	MDCV-004992Y	$ 1,313.08	$ 1,142.38
FireEye	Threat Analytics Platform-Basic Jumpstart-5 Days	PS-TAP-JS-B	$ 35,000.00	$ 30,450.00
FireEye	EVL Threat Analytics Platform Adv Intel Platinum	EVL-TAP	$ -	$ -
FireEye	Managed Defense Continuous Vigilance 3 Year 250-499	MDCV-004993Y	$ 1,969.62	$ 1,713.57
FireEye	Managed Defense Continuous Vigilance 4 Year 250-499	MDCV-004994Y	$ 2,626.16	$ 2,284.76
FireEye	Managed Defense Continuous Vigilance 5 Year 250-499	MDCV-004995Y	$ 3,282.70	$ 2,855.95
FireEye	Managed Defense Continuous Vigilance 1 Year 500-999	MDCV-009991Y	$ 334.80	$ 291.28
FireEye	Managed Defense Continuous Vigilance 2 Year 500-999	MDCV-009992Y	$ 669.60	$ 582.55
FireEye	Managed Defense Continuous Vigilance 3 Year 500-999	MDCV-009993Y	$ 1,004.40	$ 873.83
FireEye	Managed Defense Continuous Vigilance 4 Year 500-999	MDCV-009994Y	$ 1,339.20	$ 1,165.10
FireEye	Managed Defense Continuous Vigilance 5 Year 500-999	MDCV-009995Y	$ 1,674.00	$ 1,456.38
FireEye	Managed Defense Continuous Vigilance 1 Year 1000-1999	MDCV-019991Y	$ 179.28	$ 155.97
FireEye	Managed Defense Continuous Vigilance 2 Year 1000-1999	MDCV-019992Y	$ 358.56	$ 311.95
FireEye	Managed Defense Continuous Vigilance 3 Year 1000-1999	MDCV-019993Y	$ 537.84	$ 467.92
FireEye	Managed Defense Continuous Vigilance 4 Year 1000-1999	MDCV-019994Y	$ 717.12	$ 623.89
FireEye	Managed Defense Continuous Vigilance 5 Year 1000-1999	MDCV-019995Y	$ 896.40	$ 779.87
FireEye	Managed Defense Continuous Vigilance 1 Year 2000-4999	MDCV-049991Y	$ 79.49	$ 69.16
FireEye	Managed Defense Continuous Vigilance 2 Year 2000-4999	MDCV-049992Y	$ 158.98	$ 138.31
FireEye	Managed Defense Continuous Vigilance 3 Year 2000-4999	MDCV-049993Y	$ 238.47	$ 207.47
FireEye	Managed Defense Continuous Vigilance 4 Year 2000-4999	MDCV-049994Y	$ 317.96	$ 276.63
FireEye	Managed Defense Continuous Vigilance 5 Year 2000-4999	MDCV-049995Y	$ 397.45	$ 345.78
FireEye	Managed Defense Continuous Vigilance 1 Year 5000-9999	MDCV-099991Y	$ 62.64	$ 54.50
FireEye	Managed Defense Continuous Vigilance 2 Year 5000-9999	MDCV-099992Y	$ 125.28	$ 108.99
FireEye	Managed Defense Continuous Vigilance 3 Year 5000-9999	MDCV-099993Y	$ 187.92	$ 163.49
FireEye	Managed Defense Continuous Vigilance 4 Year 5000-9999	MDCV-099994Y	$ 250.56	$ 217.99
FireEye	Managed Defense Continuous Vigilance 5 Year 5000-9999	MDCV-099995Y	$ 313.20	$ 272.48
FireEye	Managed Defense Continuous Vigilance 1 Year 100K-149999	MDCV-1499991Y	$ 23.04	$ 20.04
FireEye	Managed Defense Continuous Vigilance 2 Year 100K-149999	MDCV-1499992Y	$ 46.08	$ 40.09
FireEye	Managed Defense Continuous Vigilance 3 Year 100K-149999	MDCV-1499993Y	$ 69.12	$ 60.13
FireEye	Managed Defense Continuous Vigilance 4 Year 100K-149999	MDCV-1499994Y	$ 92.16	$ 80.18
FireEye	Managed Defense Continuous Vigilance 5 Year 100K-149999	MDCV-1499995Y	$ 115.20	$ 100.22
FireEye	Managed Defense Continuous Vigilance 1 Year 10000-19999	MDCV-199991Y	$ 47.41	$ 41.25
FireEye	Managed Defense Continuous Vigilance 2 Year 10000-19999	MDCV-199992Y	$ 94.82	$ 82.49
FireEye	Managed Defense Continuous Vigilance 3 Year 10000-19999	MDCV-199993Y	$ 142.23	$ 123.74
FireEye	Managed Defense Continuous Vigilance 4 Year 10000-19999	MDCV-199994Y	$ 189.64	$ 164.99
FireEye	Managed Defense Continuous Vigilance 5 Year 10000-19999	MDCV-199995Y	$ 237.05	$ 206.23
FireEye	Managed Defense Continuous Vigilance 1 Year 150,000-199,999	MDCV-1999991Y	$ 18.60	$ 16.18
FireEye	Managed Defense Continuous Vigilance 2 Year 150,000-199,999	MDCV-1999992Y	$ 37.20	$ 32.36
FireEye	Managed Defense Continuous Vigilance 3 Year 150,000-199,999	MDCV-1999993Y	$ 55.80	$ 48.55
FireEye	Managed Defense Continuous Vigilance 4 Year 150,000-199,999	MDCV-1999994Y	$ 74.40	$ 64.73
FireEye	Managed Defense Continuous Vigilance 5 Year 150,000-199,999	MDCV-1999995Y	$ 93.00	$ 80.91

FireEye	Managed Defense Continuous Vigilance 1 Year 200,000+	MDCV-200000+1Y	$ 15.40	$ 13.40
FireEye	Managed Defense Continuous Vigilance 2 Year 200,000+	MDCV-200000+2Y	$ 30.80	$ 26.80
FireEye	Managed Defense Continuous Vigilance 3 Year 200,000+	MDCV-200000+3Y	$ 46.20	$ 40.19
FireEye	Managed Defense Continuous Vigilance 4 Year 200,000+	MDCV-200000+4Y	$ 61.60	$ 53.59
FireEye	Managed Defense Continuous Vigilance 5 Year 200,000+	MDCV-200000+5Y	$ 77.00	$ 66.99
FireEye	Managed Defense Continuous Vigilance 1 Year 20000-39999	MDCV-399991Y	$ 41.00	$ 35.67
FireEye	Managed Defense Continuous Vigilance 2 Year 20000-39999	MDCV-399992Y	$ 82.00	$ 71.34
FireEye	Managed Defense Continuous Vigilance 3 Year 20000-39999	MDCV-399993Y	$ 123.00	$ 107.01
FireEye	Managed Defense Continuous Vigilance 4 Year 20000-39999	MDCV-399994Y	$ 164.00	$ 142.68
FireEye	Managed Defense Continuous Vigilance 5 Year 20000-39999	MDCV-399995Y	$ 205.00	$ 178.35
FireEye	Managed Defense Continuous Vigilance 1 Year 40000-59999	MDCV-599991Y	$ 36.00	$ 31.32
FireEye	Managed Defense Continuous Vigilance 2 Year 40000-59999	MDCV-599992Y	$ 72.00	$ 62.64
FireEye	Managed Defense Continuous Vigilance 3 Year 40000-59999	MDCV-599993Y	$ 108.00	$ 93.96
FireEye	Managed Defense Continuous Vigilance 4 Year 40000-59999	MDCV-599994Y	$ 144.00	$ 125.28
FireEye	Managed Defense Continuous Vigilance 5 Year 40000-59999	MDCV-599995Y	$ 180.00	$ 156.60
FireEye	Managed Defense Continuous Vigilance 1 Year 60000-79999	MDCV-799991Y	$ 30.00	$ 26.10
FireEye	Managed Defense Continuous Vigilance 2 Year 60000-79999	MDCV-799992Y	$ 60.00	$ 52.20
FireEye	Managed Defense Continuous Vigilance 3 Year 60000-79999	MDCV-799993Y	$ 90.00	$ 78.30
FireEye	Managed Defense Continuous Vigilance 4 Year 60000-79999	MDCV-799994Y	$ 120.00	$ 104.40
FireEye	Managed Defense Continuous Vigilance 5 Year 60000-79999	MDCV-799995Y	$ 150.00	$ 130.50
FireEye	Managed Defense Continuous Vigilance 1 Year 80000-99999	MDCV-999991Y	$ 26.72	$ 23.25
FireEye	Managed Defense Continuous Vigilance 2 Year 80000-99999	MDCV-999992Y	$ 53.44	$ 46.49
FireEye	Managed Defense Continuous Vigilance 3 Year 80000-99999	MDCV-999993Y	$ 80.16	$ 69.74
FireEye	Managed Defense Continuous Vigilance 4 Year 80000-99999	MDCV-999994Y	$ 106.88	$ 92.99
FireEye	Managed Defense Continuous Vigilance 5 Year 80000-99999	MDCV-999995Y	$ 133.60	$ 116.23
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 1-249	RN-MDCV-002491Y	$ 1,296.00	$ 1,127.52
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 1-249	RN-MDCV-002492Y	$ 2,592.00	$ 2,255.04
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 1-249	RN-MDCV-002493Y	$ 3,888.00	$ 3,382.56
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 1-249	RN-MDCV-002494Y	$ 5,184.00	$ 4,510.08
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 250-499	RN-MDCV-004991Y	$ 656.64	$ 571.28
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 250-499	RN-MDCV-004992Y	$ 1,313.28	$ 1,142.55
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 250-499	RN-MDCV-004993Y	$ 1,969.92	$ 1,713.83
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 250-499	RN-MDCV-004994Y	$ 2,626.56	$ 2,285.11
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 500-999	RN-MDCV-009991Y	$ 334.80	$ 291.28
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 500-999	RN-MDCV-009992Y	$ 669.60	$ 582.55
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 500-999	RN-MDCV-009993Y	$ 1,004.40	$ 873.83
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 500-999	RN-MDCV-009994Y	$ 1,339.20	$ 1,165.10
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 1000-1999	RN-MDCV-019991Y	$ 179.28	$ 155.97
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 1000-1999	RN-MDCV-019992Y	$ 358.56	$ 311.95
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 1000-1999	RN-MDCV-019993Y	$ 537.84	$ 467.92
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 1000-1999	RN-MDCV-019994Y	$ 717.12	$ 623.89
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 2000-4999	RN-MDCV-049991Y	$ 79.49	$ 69.16
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 2000-4999	RN-MDCV-049992Y	$ 158.98	$ 138.31
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 2000-4999	RN-MDCV-049993Y	$ 238.47	$ 207.47
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 2000-4999	RN-MDCV-049994Y	$ 317.96	$ 276.63
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 5000-9999	RN-MDCV-099991Y	$ 62.64	$ 54.50
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 5000-9999	RN-MDCV-099992Y	$ 125.28	$ 108.99
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 5000-9999	RN-MDCV-099993Y	$ 187.92	$ 163.49
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 5000-9999	RN-MDCV-099994Y	$ 250.56	$ 217.99

FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 100K-149999	RN-MDCV-1499991Y	$ 23.04	$ 20.04
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 100K-149999	RN-MDCV-1499992Y	$ 46.08	$ 40.09
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 100K-149999	RN-MDCV-1499993Y	$ 69.12	$ 60.13
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 100K-149999	RN-MDCV-1499994Y	$ 92.16	$ 80.18
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 10000-19999	RN-MDCV-199991Y	$ 47.41	$ 41.25
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 10000-19999	RN-MDCV-199992Y	$ 94.82	$ 82.49
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 10000-19999	RN-MDCV-199993Y	$ 142.23	$ 123.74
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 10000-19999	RN-MDCV-199994Y	$ 189.64	$ 164.99
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 150,000-199,999	RN-MDCV-1999991Y	$ 18.60	$ 16.18
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 150,000-199,999	RN-MDCV-1999992Y	$ 37.20	$ 32.36
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 150,000-199,999	RN-MDCV-1999993Y	$ 55.80	$ 48.55
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 150,000-199,999	RN-MDCV-1999994Y	$ 74.40	$ 64.73
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 200,000+	RN-MDCV-200000+1Y	$ 15.40	$ 13.40
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 200,000+	RN-MDCV-200000+2Y	$ 30.80	$ 26.80
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 200,000+	RN-MDCV-200000+3Y	$ 46.20	$ 40.19
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 200,000+	RN-MDCV-200000+4Y	$ 61.60	$ 53.59
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 20000-39999	RN-MDCV-399991Y	$ 41.00	$ 35.67
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 20000-39999	RN-MDCV-399992Y	$ 82.00	$ 71.34
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 20000-39999	RN-MDCV-399993Y	$ 123.00	$ 107.01
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 20000-39999	RN-MDCV-399994Y	$ 164.00	$ 142.68
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 40000-59999	RN-MDCV-599991Y	$ 36.00	$ 31.32
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 40000-59999	RN-MDCV-599992Y	$ 72.00	$ 62.64
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 40000-59999	RN-MDCV-599993Y	$ 108.00	$ 93.96
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 40000-59999	RN-MDCV-599994Y	$ 144.00	$ 125.28
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 60000-79999	RN-MDCV-799991Y	$ 30.00	$ 26.10
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 60000-79999	RN-MDCV-799992Y	$ 60.00	$ 52.20
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 60000-79999	RN-MDCV-799994Y	$ 120.00	$ 104.40
FireEye	Renewal-Managed Defense Continuous Vigilance 1 Year 80000-99999	RN-MDCV-999991Y	$ 26.72	$ 23.25
FireEye	Renewal-Managed Defense Continuous Vigilance 2 Year 80000-99999	RN-MDCV-999992Y	$ 53.44	$ 46.49
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 80000-99999	RN-MDCV-999993Y	$ 80.16	$ 69.74
FireEye	Renewal-Managed Defense Continuous Vigilance 4 Year 80000-99999	RN-MDCV-999994Y	$ 106.88	$ 92.99
FireEye	Renewal-Managed Defense Continuous Vigilance 3 Year 60000-79999	RN-MDCV-799993Y	$ 90.00	$ 78.30
FireEye	PX 004S Managed Defense Appliance Tech Enabler Bundle	MD-004SPX-TE-BDL	$ 7,000.00	$ 6,090.00
FireEye	PX 2040ESS48 Managed Defense Appliance Tech Enabler	MD-2040ESS48PX-TE-BDL	$ 40,000.00	$ 34,800.00
FireEye	Up to 3 days of services including installation of up to 4 total components (e.g. HX, DMZ, NX, PX) and transition to the FaaS team. Fixed price engageme	CS-FaaS-JS-B	$ 9,000.00	$ 7,830.00
FireEye	Up to 5 days of services including installation of up to 6 total components (e.g. HX, DMZ, NX, PX) and transition to the FaaS team. Fixed price engageme	CS-FaaS-JS-ADV	$ 15,000.00	$ 13,050.00
FireEye	Eval - Mobile Threat Prevention - Application Analysis - 1 Year	EVL-MC-AA	$ -	$ -
FireEye	Eval - Mobile Threat Prevention - API (100 devices) - 1 Year	EVL-MC-MS	$ -	$ -
FireEye	Mobile Threat Prevention - Application Analysis Admin Addon (5 admins) - 1 Year	MC-AA-ADM-1Y	$ 5,000.00	$ 4,350.00
FireEye	Mobile Threat Prevention - Application Analysis Admin Addon (5 admins) - 2 Year	MC-AA-ADM-2Y	$ 10,000.00	$ 8,700.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA 1 Year	MC-AA1Y-CAG	$ 20,000.00	$ 17,400.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 1 Year	MC-AA1Y-CAP	$ 21,000.00	$ 18,270.00
FireEye	Mobile Threat Prevention - Application Analysis Platinum 1 Year	MC-AA1Y-PLT	$ 20,000.00	$ 17,400.00
FireEye	Mobile Threat Prevention - Application Analysis Plat Prio Plus 1 Year	MC-AA1Y-PPL	$ 21,000.00	$ 18,270.00
FireEye	Mobile Threat Prevention - Application Analysis Government US 1 Year	MC-AA1Y-USG	$ 20,000.00	$ 17,400.00
FireEye	Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 1 Year	MC-AA1Y-USP	$ 21,000.00	$ 18,270.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA 2 Year	MC-AA2Y-CAG	$ 40,000.00	$ 34,800.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 2 Year	MC-AA2Y-CAP	$ 42,000.00	$ 36,540.00
FireEye	Mobile Threat Prevention - Application Analysis Platinum 2 Year	MC-AA2Y-PLT	$ 40,000.00	$ 34,800.00

FireEye	Mobile Threat Prevention - Application Analysis Plat Prio Plus 2 Year	MC-AA2Y-PPL	$ 42,000.00	$ 36,540.00
FireEye	Mobile Threat Prevention - Application Analysis Government US 2 Year	MC-AA2Y-USG	$ 40,000.00	$ 34,800.00
FireEye	Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 2 Year	MC-AA2Y-USP	$ 42,000.00	$ 36,540.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA 3 Year	MC-AA3Y-CAG	$ 48,000.00	$ 41,760.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 3 Year	MC-AA3Y-CAP	$ 50,400.00	$ 43,848.00
FireEye	Mobile Threat Prevention - Application Analysis Platinum 3 Year	MC-AA3Y-PLT	$ 48,000.00	$ 41,760.00
FireEye	Mobile Threat Prevention - Application Analysis Plat Prio Plus 3 Year	MC-AA3Y-PPL	$ 50,400.00	$ 43,848.00
FireEye	Mobile Threat Prevention - Application Analysis Government US 3 Year	MC-AA3Y-USG	$ 48,000.00	$ 41,760.00
FireEye	Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 3 Year	MC-AA3Y-USP	$ 50,400.00	$ 43,848.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA 4 Year	MC-AA4Y-CAG	$ 64,000.00	$ 55,680.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 4 Year	MC-AA4Y-CAP	$ 67,200.00	$ 58,464.00
FireEye	Mobile Threat Prevention - Application Analysis Platinum 4 Year	MC-AA4Y-PLT	$ 64,000.00	$ 55,680.00
FireEye	Mobile Threat Prevention - Application Analysis Plat Prio Plus 4 Year	MC-AA4Y-PPL	$ 67,200.00	$ 58,464.00
FireEye	Mobile Threat Prevention - Application Analysis Government US 4 Year	MC-AA4Y-USG	$ 64,000.00	$ 55,680.00
FireEye	Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 4 Year	MC-AA4Y-USP	$ 67,200.00	$ 58,464.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA 5 Year	MC-AA5Y-CAG	$ 80,000.00	$ 69,600.00
FireEye	Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 5 Year	MC-AA5Y-CAP	$ 84,000.00	$ 73,080.00
FireEye	Mobile Threat Prevention - Application Analysis Platinum 5 Year	MC-AA5Y-PLT	$ 80,000.00	$ 69,600.00
FireEye	Mobile Threat Prevention - Application Analysis Plat Prio Plus 5 Year	MC-AA5Y-PPL	$ 84,000.00	$ 73,080.00
FireEye	Mobile Threat Prevention - Application Analysis Government US 5 Year	MC-AA5Y-USG	$ 80,000.00	$ 69,600.00
FireEye	Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 5 Year	MC-AA5Y-USP	$ 84,000.00	$ 73,080.00
FireEye	Mobile Threat Prevention - API 1 Year 100-499	MC-MS-000499-1Y	$ 99.00	$ 86.13
FireEye	Mobile Threat Prevention - API 2 Year 100-499	MC-MS-000499-2Y	$ 198.00	$ 172.26
FireEye	Mobile Threat Prevention - API 3 Year 100-499	MC-MS-000499-3Y	$ 260.00	$ 226.20
FireEye	Mobile Threat Prevention - API 4 Year 100-499	MC-MS-000499-4Y	$ 340.00	$ 295.80
FireEye	Mobile Threat Prevention - API 5 Year 100-499	MC-MS-000499-5Y	$ 430.00	$ 374.10
FireEye	Mobile Threat Prevention - API 1 Year 500-999	MC-MS-000999-1Y	$ 88.00	$ 76.56
FireEye	Mobile Threat Prevention - API 2 Year 500-999	MC-MS-000999-2Y	$ 176.00	$ 153.12
FireEye	Mobile Threat Prevention - API 3 Year 500-999	MC-MS-000999-3Y	$ 230.00	$ 200.10
FireEye	Mobile Threat Prevention - API 4 Year 500-999	MC-MS-000999-4Y	$ 300.00	$ 261.00
FireEye	Mobile Threat Prevention - API 5 Year 500-999	MC-MS-000999-5Y	$ 380.00	$ 330.60
FireEye	Mobile Threat Prevention - API 1 Year 1K-1999	MC-MS-001999-1Y	$ 79.00	$ 68.73
FireEye	Mobile Threat Prevention - API 2 Year 1K-1999	MC-MS-001999-2Y	$ 158.00	$ 137.46
FireEye	Mobile Threat Prevention - API 3 Year 1K-1999	MC-MS-001999-3Y	$ 210.00	$ 182.70
FireEye	Mobile Threat Prevention - API 4 Year 1K-1999	MC-MS-001999-4Y	$ 270.00	$ 234.90
FireEye	Mobile Threat Prevention - API 5 Year 1K-1999	MC-MS-001999-5Y	$ 340.00	$ 295.80
FireEye	Mobile Threat Prevention - API 1 Year 2K-4999	MC-MS-004999-1Y	$ 71.00	$ 61.77
FireEye	Mobile Threat Prevention - API 2 Year 2K-4999	MC-MS-004999-2Y	$ 142.00	$ 123.54
FireEye	Mobile Threat Prevention - API 3 Year 2K-4999	MC-MS-004999-3Y	$ 190.00	$ 165.30
FireEye	Mobile Threat Prevention - API 4 Year 2K-4999	MC-MS-004999-4Y	$ 250.00	$ 217.50
FireEye	Mobile Threat Prevention - API 5 Year 2K-4999	MC-MS-004999-5Y	$ 310.00	$ 269.70
FireEye	Mobile Threat Prevention - API 1 Year 5K-9999	MC-MS-009999-1Y	$ 63.00	$ 54.81
FireEye	Mobile Threat Prevention - API 2 Year 5K-9999	MC-MS-009999-2Y	$ 126.00	$ 109.62
FireEye	Mobile Threat Prevention - API 3 Year 5K-9999	MC-MS-009999-3Y	$ 170.00	$ 147.90
FireEye	Mobile Threat Prevention - API 4 Year 5K-9999	MC-MS-009999-4Y	$ 220.00	$ 191.40
FireEye	Mobile Threat Prevention - API 5 Year 5K-9999	MC-MS-009999-5Y	$ 270.00	$ 234.90
FireEye	Mobile Threat Prevention - API 1 Year 10K-19999	MC-MS-019999-1Y	$ 56.00	$ 48.72
FireEye	Mobile Threat Prevention - API 2 Year 10K-19999	MC-MS-019999-2Y	$ 112.00	$ 97.44
FireEye	Mobile Threat Prevention - API 3 Year 10K-19999	MC-MS-019999-3Y	$ 150.00	$ 130.50

FireEye	Mobile Threat Prevention - API 4 Year 10K-19999	MC-MS-019999-4Y	$ 200.00	$ 174.00
FireEye	Mobile Threat Prevention - API 5 Year 10K-19999	MC-MS-019999-5Y	$ 240.00	$ 208.80
FireEye	Mobile Threat Prevention - API 1 Year 20K-49999	MC-MS-049999-1Y	$ 50.00	$ 43.50
FireEye	Mobile Threat Prevention - API 2 Year 20K-49999	MC-MS-049999-2Y	$ 100.00	$ 87.00
FireEye	Mobile Threat Prevention - API 3 Year 20K-49999	MC-MS-049999-3Y	$ 130.00	$ 113.10
FireEye	Mobile Threat Prevention - API 4 Year 20K-49999	MC-MS-049999-4Y	$ 170.00	$ 147.90
FireEye	Mobile Threat Prevention - API 5 Year 20K-49999	MC-MS-049999-5Y	$ 220.00	$ 191.40
FireEye	Mobile Threat Prevention - API 1 Year 50K-74999	MC-MS-074999-1Y	$ 45.00	$ 39.15
FireEye	Mobile Threat Prevention - API 2 Year 50K-74999	MC-MS-074999-2Y	$ 90.00	$ 78.30
FireEye	Mobile Threat Prevention - API 3 Year 50K-74999	MC-MS-074999-3Y	$ 120.00	$ 104.40
FireEye	Mobile Threat Prevention - API 4 Year 50K-74999	MC-MS-074999-4Y	$ 160.00	$ 139.20
FireEye	Mobile Threat Prevention - API 5 Year 50K-74999	MC-MS-074999-5Y	$ 200.00	$ 174.00
FireEye	Mobile Threat Prevention - API 1 Year 75K-99999	MC-MS-099999-1Y	$ 40.00	$ 34.80
FireEye	Mobile Threat Prevention - API 2 Year 75K-99999	MC-MS-099999-2Y	$ 80.00	$ 69.60
FireEye	Mobile Threat Prevention - API 3 Year 75K-99999	MC-MS-099999-3Y	$ 110.00	$ 95.70
FireEye	Mobile Threat Prevention - API 4 Year 75K-99999	MC-MS-099999-4Y	$ 140.00	$ 121.80
FireEye	Mobile Threat Prevention - API 5 Year 75K-99999	MC-MS-099999-5Y	$ 170.00	$ 147.90
FireEye	Mobile Threat Prevention - API 1 Year 100000+	MC-MS-100000+-1Y	$ 36.00	$ 31.32
FireEye	Mobile Threat Prevention - API 2 Year 100000+	MC-MS-100000+-2Y	$ 72.00	$ 62.64
FireEye	Mobile Threat Prevention - API 3 Year 100000+	MC-MS-100000+-3Y	$ 100.00	$ 87.00
FireEye	Mobile Threat Prevention - API 4 Year 100000+	MC-MS-100000+-4Y	$ 130.00	$ 113.10
FireEye	Mobile Threat Prevention - API 5 Year 100000+	MC-MS-100000+-5Y	$ 160.00	$ 139.20
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA 1 Year	RN-MC-AA1Y-CAG	$ 20,000.00	$ 17,400.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 1 Year	RN-MC-AA1Y-CAP	$ 21,000.00	$ 18,270.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Platinum 1 Year	RN-MC-AA1Y-PLT	$ 20,000.00	$ 17,400.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Plat Prio Plus 1 Year	RN-MC-AA1Y-PPL	$ 21,000.00	$ 18,270.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US 1 Year	RN-MC-AA1Y-USG	$ 20,000.00	$ 17,400.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 1 Year	RN-MC-AA1Y-USP	$ 21,000.00	$ 18,270.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA 2 Year	RN-MC-AA2Y-CAG	$ 40,000.00	$ 34,800.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 2 Year	RN-MC-AA2Y-CAP	$ 42,000.00	$ 36,540.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Platinum 2 Year	RN-MC-AA2Y-PLT	$ 40,000.00	$ 34,800.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Plat Prio Plus 2 Year	RN-MC-AA2Y-PPL	$ 42,000.00	$ 36,540.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US 2 Year	RN-MC-AA2Y-USG	$ 40,000.00	$ 34,800.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 2 Year	RN-MC-AA2Y-USP	$ 42,000.00	$ 36,540.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA 3 Year	RN-MC-AA3Y-CAG	$ 48,000.00	$ 41,760.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 3 Year	RN-MC-AA3Y-CAP	$ 50,400.00	$ 43,848.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Platinum 3 Year	RN-MC-AA3Y-PLT	$ 48,000.00	$ 41,760.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Plat Prio Plus 3 Year	RN-MC-AA3Y-PPL	$ 50,400.00	$ 43,848.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US 3 Year	RN-MC-AA3Y-USG	$ 48,000.00	$ 41,760.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 3 Year	RN-MC-AA3Y-USP	$ 50,400.00	$ 43,848.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA 4 Year	RN-MC-AA4Y-CAG	$ 64,000.00	$ 55,680.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government CA Plat Prio Plus 4 Year	RN-MC-AA4Y-CAP	$ 67,200.00	$ 58,464.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Platinum 4 Year	RN-MC-AA4Y-PLT	$ 64,000.00	$ 55,680.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Plat Prio Plus 4 Year	RN-MC-AA4Y-PPL	$ 67,200.00	$ 58,464.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US 4 Year	RN-MC-AA4Y-USG	$ 64,000.00	$ 55,680.00
FireEye	Renewal-Mobile Threat Prevention - Application Analysis Government US Plat Prio Plus 4 Year	RN-MC-AA4Y-USP	$ 67,200.00	$ 58,464.00
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 100-499	RN-MC-MS-000499-1Y	$ 99.00	$ 86.13
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 100-499	RN-MC-MS-000499-2Y	$ 260.00	$ 226.20
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 100-499	RN-MC-MS-000499-3Y	$ 340.00	$ 295.80

FireEye	Renewal-Mobile Threat Prevention - API 4 Year 100-499	RN-MC-MS-000499-4Y	$ 430.00	$ 374.10
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 500-999	RN-MC-MS-000999-1Y	$ 88.00	$ 76.56
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 500-999	RN-MC-MS-000999-2Y	$ 230.00	$ 200.10
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 500-999	RN-MC-MS-000999-3Y	$ 300.00	$ 261.00
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 500-999	RN-MC-MS-000999-4Y	$ 380.00	$ 330.60
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 1K-1999	RN-MC-MS-001999-1Y	$ 79.00	$ 68.73
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 1K-1999	RN-MC-MS-001999-2Y	$ 210.00	$ 182.70
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 1K-1999	RN-MC-MS-001999-3Y	$ 270.00	$ 234.90
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 1K-1999	RN-MC-MS-001999-4Y	$ 340.00	$ 295.80
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 2K-4999	RN-MC-MS-004999-1Y	$ 71.00	$ 61.77
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 2K-4999	RN-MC-MS-004999-2Y	$ 190.00	$ 165.30
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 2K-4999	RN-MC-MS-004999-3Y	$ 250.00	$ 217.50
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 2K-4999	RN-MC-MS-004999-4Y	$ 310.00	$ 269.70
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 5K-9999	RN-MC-MS-009999-1Y	$ 63.00	$ 54.81
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 5K-9999	RN-MC-MS-009999-2Y	$ 170.00	$ 147.90
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 5K-9999	RN-MC-MS-009999-3Y	$ 220.00	$ 191.40
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 5K-9999	RN-MC-MS-009999-4Y	$ 270.00	$ 234.90
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 10K-19999	RN-MC-MS-019999-1Y	$ 56.00	$ 48.72
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 10K-19999	RN-MC-MS-019999-2Y	$ 150.00	$ 130.50
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 10K-19999	RN-MC-MS-019999-3Y	$ 200.00	$ 174.00
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 10K-19999	RN-MC-MS-019999-4Y	$ 240.00	$ 208.80
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 20K-49999	RN-MC-MS-049999-1Y	$ 50.00	$ 43.50
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 20K-49999	RN-MC-MS-049999-2Y	$ 130.00	$ 113.10
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 20K-49999	RN-MC-MS-049999-3Y	$ 170.00	$ 147.90
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 20K-49999	RN-MC-MS-049999-4Y	$ 220.00	$ 191.40
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 50K-74999	RN-MC-MS-074999-1Y	$ 45.00	$ 39.15
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 50K-74999	RN-MC-MS-074999-2Y	$ 120.00	$ 104.40
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 50K-74999	RN-MC-MS-074999-3Y	$ 160.00	$ 139.20
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 50K-74999	RN-MC-MS-074999-4Y	$ 200.00	$ 174.00
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 75K-99999	RN-MC-MS-099999-1Y	$ 40.00	$ 34.80
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 75K-99999	RN-MC-MS-099999-2Y	$ 110.00	$ 95.70
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 75K-99999	RN-MC-MS-099999-3Y	$ 140.00	$ 121.80
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 75K-99999	RN-MC-MS-099999-4Y	$ 170.00	$ 147.90
FireEye	Renewal-Mobile Threat Prevention - API 1 Year 100000+	RN-MC-MS-100000+-1Y	$ 36.00	$ 31.32
FireEye	Renewal-Mobile Threat Prevention - API 2 Year 100000+	RN-MC-MS-100000+-2Y	$ 100.00	$ 87.00
FireEye	Renewal-Mobile Threat Prevention - API 3 Year 100000+	RN-MC-MS-100000+-3Y	$ 130.00	$ 113.10
FireEye	Renewal-Mobile Threat Prevention - API 4 Year 100000+	RN-MC-MS-100000+-4Y	$ 160.00	$ 139.20
FireEye	MX 900 Appliance - Mobile Threat Prevention - Mobile Security Management	900MX-HW	$ 7,995.00	$ 6,955.65
FireEye	MX 900 Appliance Standby- Mobile Threat Prevention - Mobile Security Management	900MX-HWSB	$ 7,995.00	$ 6,955.65
FireEye	EVAL-MX 900 appliance - Mobile Threat Prevention - Mobile Security Management	EVL-900MX-HW	$ 1,450.00	$ 1,261.50
FireEye	POC-MX 900 appliance - Mobile Threat Prevention - Mobile Security Management	POC-900MX-HW	$ 1,450.00	$ 1,261.50
FireEye	Eval - Mobile Threat Prevention - Mobile Security Management 1 Year 100 devices	EVL-MC-MSM	$ -	$ -
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 100-499	MC-MSM-000499-1Y	$ 62.00	$ 53.94
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 100-499	MC-MSM-000499-2Y	$ 124.00	$ 107.88
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 100-499	MC-MSM-000499-3Y	$ 159.00	$ 138.33
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 100-499	MC-MSM-000499-4Y	$ 211.00	$ 183.57
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 100-499	MC-MSM-000499-5Y	$ 264.00	$ 229.68
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 500-999	MC-MSM-000999-1Y	$ 52.00	$ 45.24
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 500-999	MC-MSM-000999-2Y	$ 104.00	$ 90.48

FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 500-999	RN-MC-MSM-000999-2Y	$ 104.00	$ 90.48
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 500-999	MC-MSM-000999-3Y	$ 133.00	$ 115.71
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 500-999	MC-MSM-000999-4Y	$ 177.00	$ 153.99
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 500-999	MC-MSM-000999-5Y	$ 221.00	$ 192.27
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 1000-1999	MC-MSM-001999-1Y	$ 43.00	$ 37.41
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 1000-1999	MC-MSM-001999-2Y	$ 86.00	$ 74.82
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 1000-1999	MC-MSM-001999-3Y	$ 110.00	$ 95.70
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 1000-1999	MC-MSM-001999-4Y	$ 147.00	$ 127.89
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 1000-1999	MC-MSM-001999-5Y	$ 183.00	$ 159.21
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 2000-4999	MC-MSM-004999-1Y	$ 36.00	$ 31.32
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 2000-4999	MC-MSM-004999-2Y	$ 72.00	$ 62.64
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 2000-4999	MC-MSM-004999-3Y	$ 92.00	$ 80.04
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 2000-4999	MC-MSM-004999-4Y	$ 123.00	$ 107.01
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 2000-4999	MC-MSM-004999-5Y	$ 153.00	$ 133.11
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 5000-9999	MC-MSM-009999-1Y	$ 30.00	$ 26.10
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 5000-9999	MC-MSM-009999-2Y	$ 60.00	$ 52.20
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 5000-9999	MC-MSM-009999-3Y	$ 77.00	$ 66.99
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 5000-9999	MC-MSM-009999-4Y	$ 102.00	$ 88.74
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 5000-9999	MC-MSM-009999-5Y	$ 130.00	$ 113.10
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 10000-19999	MC-MSM-019999-1Y	$ 25.00	$ 21.75
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 10000-19999	MC-MSM-019999-2Y	$ 50.00	$ 43.50
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 10000-19999	MC-MSM-019999-3Y	$ 64.00	$ 55.68
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 10000-19999	MC-MSM-019999-4Y	$ 85.00	$ 73.95
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 10000-19999	MC-MSM-019999-5Y	$ 107.00	$ 93.09
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 20000-49999	MC-MSM-049999-1Y	$ 21.00	$ 18.27
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 20000-49999	MC-MSM-049999-2Y	$ 42.00	$ 36.54
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 20000-49999	MC-MSM-049999-3Y	$ 54.00	$ 46.98
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 20000-49999	MC-MSM-049999-4Y	$ 72.00	$ 62.64
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 20000-49999	MC-MSM-049999-5Y	$ 90.00	$ 78.30
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 50000-74999	MC-MSM-074999-1Y	$ 17.00	$ 14.79
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 50000-74999	MC-MSM-074999-2Y	$ 34.00	$ 29.58
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 50000-74999	MC-MSM-074999-3Y	$ 44.00	$ 38.28
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 50000-74999	MC-MSM-074999-4Y	$ 58.00	$ 50.46
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 50000-74999	MC-MSM-074999-5Y	$ 73.00	$ 63.51
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 75000-99999	MC-MSM-099999-1Y	$ 14.00	$ 12.18
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 75000-99999	MC-MSM-099999-2Y	$ 28.00	$ 24.36
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 75000-99999	MC-MSM-099999-3Y	$ 36.00	$ 31.32
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 75000-99999	MC-MSM-099999-4Y	$ 48.00	$ 41.76
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 75000-99999	MC-MSM-099999-5Y	$ 60.00	$ 52.20
FireEye	Mobile Threat Prevention - Mobile Security Management 1 Year 100000+	MC-MSM-100000+1Y	$ 12.00	$ 10.44
FireEye	Mobile Threat Prevention - Mobile Security Management 2 Year 100000+	MC-MSM-100000+2Y	$ 24.00	$ 20.88
FireEye	Mobile Threat Prevention - Mobile Security Management 3 Year 100000+	MC-MSM-100000+3Y	$ 31.00	$ 26.97
FireEye	Mobile Threat Prevention - Mobile Security Management 4 Year 100000+	MC-MSM-100000+4Y	$ 41.00	$ 35.67
FireEye	Mobile Threat Prevention - Mobile Security Management 5 Year 100000+	MC-MSM-100000+5Y	$ 51.00	$ 44.37
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 100-499	RN-MC-MSM-000499-1Y	$ 62.00	$ 53.94
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 100-499	RN-MC-MSM-000499-2Y	$ 124.00	$ 107.88
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 100-499	RN-MC-MSM-000499-3Y	$ 159.00	$ 138.33
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 100-499	RN-MC-MSM-000499-4Y	$ 211.00	$ 183.57
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 100-499	RN-MC-MSM-000499-5Y	$ 264.00	$ 229.68

FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 500-999	RN-MC-MSM-000999-1Y	$ 52.00	$ 45.24
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 500-999	RN-MC-MSM-000999-3Y	$ 133.00	$ 115.71
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 500-999	RN-MC-MSM-000999-4Y	$ 177.00	$ 153.99
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 500-999	RN-MC-MSM-000999-5Y	$ 221.00	$ 192.27
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 1000-1999	RN-MC-MSM-001999-1Y	$ 43.00	$ 37.41
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 1000-1999	RN-MC-MSM-001999-2Y	$ 86.00	$ 74.82
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 1000-1999	RN-MC-MSM-001999-3Y	$ 110.00	$ 95.70
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 1000-1999	RN-MC-MSM-001999-4Y	$ 147.00	$ 127.89
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 1000-1999	RN-MC-MSM-001999-5Y	$ 183.00	$ 159.21
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 2000-4999	RN-MC-MSM-004999-1Y	$ 36.00	$ 31.32
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 2000-4999	RN-MC-MSM-004999-2Y	$ 72.00	$ 62.64
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 2000-4999	RN-MC-MSM-004999-3Y	$ 92.00	$ 80.04
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 2000-4999	RN-MC-MSM-004999-4Y	$ 123.00	$ 107.01
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 2000-4999	RN-MC-MSM-004999-5Y	$ 153.00	$ 133.11
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 5000-9999	RN-MC-MSM-009999-1Y	$ 30.00	$ 26.10
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 5000-9999	RN-MC-MSM-009999-2Y	$ 60.00	$ 52.20
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 5000-9999	RN-MC-MSM-009999-3Y	$ 77.00	$ 66.99
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 5000-9999	RN-MC-MSM-009999-4Y	$ 102.00	$ 88.74
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 5000-9999	RN-MC-MSM-009999-5Y	$ 130.00	$ 113.10
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 10000-19999	RN-MC-MSM-019999-1Y	$ 25.00	$ 21.75
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 10000-19999	RN-MC-MSM-019999-2Y	$ 50.00	$ 43.50
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 10000-19999	RN-MC-MSM-019999-3Y	$ 64.00	$ 55.68
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 10000-19999	RN-MC-MSM-019999-4Y	$ 85.00	$ 73.95
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 10000-19999	RN-MC-MSM-019999-5Y	$ 107.00	$ 93.09
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 20000-49999	RN-MC-MSM-049999-1Y	$ 21.00	$ 18.27
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 20000-49999	RN-MC-MSM-049999-2Y	$ 42.00	$ 36.54
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 20000-49999	RN-MC-MSM-049999-3Y	$ 54.00	$ 46.98
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 20000-49999	RN-MC-MSM-049999-4Y	$ 72.00	$ 62.64
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 20000-49999	RN-MC-MSM-049999-5Y	$ 90.00	$ 78.30
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 50000-74999	RN-MC-MSM-074999-1Y	$ 17.00	$ 14.79
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 50000-74999	RN-MC-MSM-074999-2Y	$ 34.00	$ 29.58
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 50000-74999	RN-MC-MSM-074999-3Y	$ 44.00	$ 38.28
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 50000-74999	RN-MC-MSM-074999-4Y	$ 58.00	$ 50.46
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 50000-74999	RN-MC-MSM-074999-5Y	$ 73.00	$ 63.51
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 75000-99999	RN-MC-MSM-099999-1Y	$ 14.00	$ 12.18
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 75000-99999	RN-MC-MSM-099999-2Y	$ 28.00	$ 24.36
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 75000-99999	RN-MC-MSM-099999-3Y	$ 36.00	$ 31.32
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 75000-99999	RN-MC-MSM-099999-4Y	$ 48.00	$ 41.76
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 75000-99999	RN-MC-MSM-099999-5Y	$ 60.00	$ 52.20
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 1 Year 100000+	RN-MC-MSM-100000+1Y	$ 12.00	$ 10.44
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 2 Year 100000+	RN-MC-MSM-100000+2Y	$ 24.00	$ 20.88
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 3 Year 100000+	RN-MC-MSM-100000+3Y	$ 31.00	$ 26.97
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 4 Year 100000+	RN-MC-MSM-100000+4Y	$ 41.00	$ 35.67
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management 5 Year 100000+	RN-MC-MSM-100000+5Y	$ 51.00	$ 44.37
FireEye	MX 900 Support Government CA 1 Year	900MX-CAG1Y	$ 1,600.00	$ 1,392.00
FireEye	MX 900 Support Government CA 2 Year	900MX-CAG2Y	$ 3,200.00	$ 2,784.00
FireEye	MX 900 Support Government CA 3 Year	900MX-CAG3Y	$ 3,840.00	$ 3,340.80
FireEye	MX 900 Support Government CA 4 Year	900MX-CAG4Y	$ 5,120.00	$ 4,454.40
FireEye	MX 900 Support Government CA 5 Year	900MX-CAG5Y	$ 6,400.00	$ 5,568.00

FireEye	MX 900 Support Government CA Priorioty Plus 1 Year	900MX-CAP1Y	$ 2,000.00	$ 1,740.00
FireEye	MX 900 Support Government CA Priorioty Plus 2 Year	900MX-CAP2Y	$ 4,000.00	$ 3,480.00
FireEye	MX 900 Support Government CA Priorioty Plus 3 Year	900MX-CAP3Y	$ 4,800.00	$ 4,176.00
FireEye	MX 900 Support Government CA Priorioty Plus 4 Year	900MX-CAP4Y	$ 6,400.00	$ 5,568.00
FireEye	MX 900 Support Government CA Priorioty Plus 5 Year	900MX-CAP5Y	$ 8,000.00	$ 6,960.00
FireEye	MX 900 Support Platinum Priority Plus 1 Year	900MX-PPL1Y	$ 2,000.00	$ 1,740.00
FireEye	MX 900 Support Platinum Priority Plus 2 Year	900MX-PPL2Y	$ 4,000.00	$ 3,480.00
FireEye	MX 900 Support Platinum Priority Plus 3 Year	900MX-PPL3Y	$ 4,800.00	$ 4,176.00
FireEye	MX 900 Support Platinum Priority Plus 4 Year	900MX-PPL4Y	$ 6,400.00	$ 5,568.00
FireEye	MX 900 Support Platinum Priority Plus 5 Year	900MX-PPL5Y	$ 8,000.00	$ 6,960.00
FireEye	MX 900 Support Platinum 1 Year	900MX-PTM1Y	$ 1,600.00	$ 1,392.00
FireEye	MX 900 Support Platinum 2 Year	900MX-PTM2Y	$ 3,200.00	$ 2,784.00
FireEye	MX 900 Support Platinum 3 Year	900MX-PTM3Y	$ 3,840.00	$ 3,340.80
FireEye	MX 900 Support Platinum 4 Year	900MX-PTM4Y	$ 5,120.00	$ 4,454.40
FireEye	MX 900 Support Platinum 5 Year	900MX-PTM5Y	$ 6,400.00	$ 5,568.00
FireEye	MX 900 Support Government US 1 Year	900MX-USG1Y	$ 1,600.00	$ 1,392.00
FireEye	MX 900 Support Government US 2 Year	900MX-USG2Y	$ 3,200.00	$ 2,784.00
FireEye	MX 900 Support Government US 3 Year	900MX-USG3Y	$ 3,840.00	$ 3,340.80
FireEye	MX 900 Support Government US 4 Year	900MX-USG4Y	$ 5,120.00	$ 4,454.40
FireEye	MX 900 Support Government US 5 Year	900MX-USG5Y	$ 6,400.00	$ 5,568.00
FireEye	MX 900 Support Government US Priorioty Plus 1 Year	900MX-USP1Y	$ 2,000.00	$ 1,740.00
FireEye	MX 900 Support Government US Priorioty Plus 2 Year	900MX-USP2Y	$ 4,000.00	$ 3,480.00
FireEye	MX 900 Support Government US Priorioty Plus 3 Year	900MX-USP3Y	$ 4,800.00	$ 4,176.00
FireEye	MX 900 Support Government US Priorioty Plus 4 Year	900MX-USP4Y	$ 6,400.00	$ 5,568.00
FireEye	MX 900 Support Government US Priorioty Plus 5 Year	900MX-USP5Y	$ 8,000.00	$ 6,960.00
FireEye	Renewal MX 900 Support Government CA 1 Year	RN-900MX-CAG1Y	$ 1,600.00	$ 1,392.00
FireEye	Renewal MX 900 Support Government CA 2 Year	RN-900MX-CAG2Y	$ 3,200.00	$ 2,784.00
FireEye	Renewal MX 900 Support Government CA 3 Year	RN-900MX-CAG3Y	$ 3,840.00	$ 3,340.80
FireEye	Renewal MX 900 Support Government CA 4 Year	RN-900MX-CAG4Y	$ 5,120.00	$ 4,454.40
FireEye	Renewal MX 900 Support Government CA 5 Year	RN-900MX-CAG5Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Government CA Priorioty Plus 1 Year	RN-900MX-CAP1Y	$ 2,000.00	$ 1,740.00
FireEye	Renewal-MX 900 Support Government CA Priorioty Plus 2 Year	RN-900MX-CAP2Y	$ 4,000.00	$ 3,480.00
FireEye	Renewal MX 900 Support Government CA Priorioty Plus 3 Year	RN-900MX-CAP3Y	$ 4,800.00	$ 4,176.00
FireEye	Renewal MX 900 Support Government CA Priorioty Plus 4 Year	RN-900MX-CAP4Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Government CA Priorioty Plus 5 Year	RN-900MX-CAP5Y	$ 8,000.00	$ 6,960.00
FireEye	Renewal MX 900 Support Platinum Priority Plus 1 Year	RN-900MX-PPL1Y	$ 2,000.00	$ 1,740.00
FireEye	Renewal MX 900 Support Platinum Priority Plus 2 Year	RN-900MX-PPL2Y	$ 4,000.00	$ 3,480.00
FireEye	Renewal MX 900 Support Platinum Priority Plus 3 Year	RN-900MX-PPL3Y	$ 4,800.00	$ 4,176.00
FireEye	Renewal MX 900 Support Platinum Priority Plus 4 Year	RN-900MX-PPL4Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Platinum Priority Plus 5 Year	RN-900MX-PPL5Y	$ 8,000.00	$ 6,960.00
FireEye	Renewal MX 900 Support Platinum 1 Year	RN-900MX-PTM1Y	$ 1,600.00	$ 1,392.00
FireEye	Renewal MX 900 Support Platinum 2 Year	RN-900MX-PTM2Y	$ 3,200.00	$ 2,784.00
FireEye	Renewal MX 900 Support Platinum 3 Year	RN-900MX-PTM3Y	$ 3,840.00	$ 3,340.80
FireEye	Renewal MX 900 Support Platinum 4 Year	RN-900MX-PTM4Y	$ 5,120.00	$ 4,454.40
FireEye	Renewal MX 900 Support Platinum 5 Year	RN-900MX-PTM5Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Government US 1 Year	RN-900MX-USG1Y	$ 1,600.00	$ 1,392.00
FireEye	Renewal MX 900 Support Government US 2 Year	RN-900MX-USG2Y	$ 3,200.00	$ 2,784.00
FireEye	Renewal MX 900 Support Government US 3 Year	RN-900MX-USG3Y	$ 3,840.00	$ 3,340.80
FireEye	Renewal MX 900 Support Government US 4 Year	RN-900MX-USG4Y	$ 5,120.00	$ 4,454.40

FireEye	Renewal MX 900 Support Government US 5 Year	RN-900MX-USG5Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Government US Priorioty Plus 1 Year	RN-900MX-USP1Y	$ 2,000.00	$ 1,740.00
FireEye	Renewal-MX 900 Support Government US Priorioty Plus 2 Year	RN-900MX-USP2Y	$ 4,000.00	$ 3,480.00
FireEye	Renewal MX 900 Support Government US Priorioty Plus 3 Year	RN-900MX-USP3Y	$ 4,800.00	$ 4,176.00
FireEye	Renewal MX 900 Support Government US Priorioty Plus 4 Year	RN-900MX-USP4Y	$ 6,400.00	$ 5,568.00
FireEye	Renewal MX 900 Support Government US Priorioty Plus 5 Year	RN-900MX-USP5Y	$ 8,000.00	$ 6,960.00
FireEye	Upgrade-MX 900 Support GovCA to GovCA Priority Plus 1 Year	UP-900MX-GAG2PP1Y	$ 400.00	$ 348.00
FireEye	Upgrade-MX 900 Support GovCA to GovCA Priority Plus 2 Year	UP-900MX-GAG2PP2Y	$ 800.00	$ 696.00
FireEye	Upgrade-MX 900 Support GovCA to GovCA Priority Plus 3 Year	UP-900MX-GAG2PP3Y	$ 960.00	$ 835.20
FireEye	Upgrade-MX 900 Support GovCA to GovCA Priority Plus 4 Year	UP-900MX-GAG2PP4Y	$ 1,280.00	$ 1,113.60
FireEye	Upgrade-MX 900 Support GovCA to GovCA Priority Plus 5 Year	UP-900MX-GAG2PP5Y	$ 1,600.00	$ 1,392.00
FireEye	Upgrade-MX 900 Support Platinum to Plat Priority Plus 1 Year	UP-900MX-PTM2PPP1Y	$ 400.00	$ 348.00
FireEye	Upgrade-MX 900 Support Platinum to Plat Priority Plus 2 Year	UP-900MX-PTM2PPP2Y	$ 800.00	$ 696.00
FireEye	Upgrade-MX 900 Support Platinum to Plat Priority Plus 3 Year	UP-900MX-PTM2PPP3Y	$ 960.00	$ 835.20
FireEye	Upgrade-MX 900 Support Platinum to Plat Priority Plus 4 Year	UP-900MX-PTM2PPP4Y	$ 1,280.00	$ 1,113.60
FireEye	Upgrade-MX 900 Support Platinum to Plat Priority Plus 5 Year	UP-900MX-PTM2PPP5Y	$ 1,600.00	$ 1,392.00
FireEye	Upgrade-MX 900 Support GovUS to GovUS Priority Plus1 Year	UP-900MX-USG2PP1Y	$ 400.00	$ 348.00
FireEye	Upgrade-MX 900 Support GovUS to GovUS Priority Plus2 Year	UP-900MX-USG2PP2Y	$ 800.00	$ 696.00
FireEye	Upgrade-MX 900 Support GovUS to GovUS Priority Plus3 Year	UP-900MX-USG2PP3Y	$ 960.00	$ 835.20
FireEye	Upgrade-MX 900 Support GovUS to GovUS Priority Plus4 Year	UP-900MX-USG2PP4Y	$ 1,280.00	$ 1,113.60
FireEye	Upgrade-MX 900 Support GovUS to GovUS Priority Plus5 Year	UP-900MX-USG2PP5Y	$ 1,600.00	$ 1,392.00
FireEye	MX 8400 Appliance/Server - Mobile Threat Prevention - Mobile Security Management - Compliance Model AX 8400	8400MX-HW	$ 64,995.00	$ 56,545.65
FireEye	MX 8400 Appliance/Server Standby- Mobile Threat Prevention - Mobile Security Management - Compliance Model AX 8400	8400MX-HWSB	$ 64,995.00	$ 56,545.65
FireEye	EVAL-MX 8400 appliance/Server - Mobile Threat Prevention - Mobile Security Management - Compliance Model AX 8400	EVL-8400MX-HW	$ 13,000.00	$ 11,310.00
FireEye	POC-MX 8400 appliance/Server - Mobile Threat Prevention - Mobile Security Management - Compliance Model AX 8400	POC-8400MX-HW	$ 13,000.00	$ 11,310.00
FireEye	MX 8400 Support Government CA 1 Year	8400MX-CAG1Y	$ 23,400.00	$ 20,358.00
FireEye	MX 8400 Support Government CA 2 Year	8400MX-CAG2Y	$ 32,760.00	$ 28,501.20
FireEye	MX 8400 Support Government CA 3 Year	8400MX-CAG3Y	$ 39,312.00	$ 34,201.44
FireEye	MX 8400 Support Government CA 4 Year	8400MX-CAG4Y	$ 52,416.00	$ 45,601.92
FireEye	MX 8400 Support Government CA 5 Year	8400MX-CAG5Y	$ 46,800.00	$ 40,716.00
FireEye	MX 8400 Support Government CA Priorioty Plus 1 Year	8400MX-CAP1Y	$ 19,434.00	$ 16,907.58
FireEye	MX 8400 Support Government CA Priorioty Plus 2 Year	8400MX-CAP2Y	$ 41,858.00	$ 36,416.46
FireEye	MX 8400 Support Government CA Priorioty Plus 3 Year	8400MX-CAP3Y	$ 46,642.00	$ 40,578.54
FireEye	MX 8400 Support Government CA Priorioty Plus 4 Year	8400MX-CAP4Y	$ 95,674.00	$ 83,236.38
FireEye	MX 8400 Support Government CA Priorioty Plus 5 Year	8400MX-CAP5Y	$ 119,592.00	$ 104,045.04
FireEye	MX 8400 Support Platinum Priority Plus 1 Year	8400MX-PPL1Y	$ 14,949.00	$ 13,005.63
FireEye	MX 8400 Support Platinum Priority Plus 2 Year	8400MX-PPL2Y	$ 29,898.00	$ 26,011.26
FireEye	MX 8400 Support Platinum Priority Plus 3 Year	8400MX-PPL3Y	$ 35,878.00	$ 31,213.86
FireEye	MX 8400 Support Platinum Priority Plus 4 Year	8400MX-PPL4Y	$ 47,837.00	$ 41,618.19
FireEye	MX 8400 Support Platinum Priority Plus 5 Year	8400MX-PPL5Y	$ 59,796.00	$ 52,022.52
FireEye	MX 8400 Support Platinum 1 Year	8400MX-PTM1Y	$ 11,700.00	$ 10,179.00
FireEye	MX 8400 Support Platinum 2 Year	8400MX-PTM2Y	$ 23,400.00	$ 20,358.00
FireEye	MX 8400 Support Platinum 3 Year	8400MX-PTM3Y	$ 28,080.00	$ 24,429.60
FireEye	MX 8400 Support Platinum 4 Year	8400MX-PTM4Y	$ 37,440.00	$ 32,572.80
FireEye	MX 8400 Support Platinum 5 Year	8400MX-PTM5Y	$ 46,800.00	$ 40,716.00
FireEye	MX 8400 Support Government US 1 Year	8400MX-USG1Y	$ 15,210.00	$ 13,232.70
FireEye	MX 8400 Support Government US 2 Year	8400MX-USG2Y	$ 23,400.00	$ 20,358.00
FireEye	MX 8400 Support Government US 3 Year	8400MX-USG3Y	$ 36,504.00	$ 31,758.48
FireEye	MX 8400 Support Government US 4 Year	8400MX-USG4Y	$ 48,672.00	$ 42,344.64

FireEye	MX 8400 Support Government US 5 Year	8400MX-USG5Y	$ 60,840.00	$ 52,930.80
FireEye	MX 8400 Support Government US Priorioty Plus 1 Year	8400MX-USP1Y	$ 20,929.00	$ 18,208.23
FireEye	MX 8400 Support Government US Priorioty Plus 2 Year	8400MX-USP2Y	$ 38,868.00	$ 33,815.16
FireEye	MX 8400 Support Government US Priorioty Plus 3 Year	8400MX-USP3Y	$ 46,642.00	$ 40,578.54
FireEye	MX 8400 Support Government US Priorioty Plus 4 Year	8400MX-USP4Y	$ 47,837.00	$ 41,618.19
FireEye	MX 8400 Support Government US Priorioty Plus 5 Year	8400MX-USP5Y	$ 83,715.00	$ 72,832.05
FireEye	Renewal MX 8400 Support Government CA 1 Year	RN-8400MX-CAG1Y	$ 15,210.00	$ 13,232.70
FireEye	Renewal MX 8400 Support Government CA 2 Year	RN-8400MX-CAG2Y	$ 23,400.00	$ 20,358.00
FireEye	Renewal MX 8400 Support Government CA 3 Year	RN-8400MX-CAG3Y	$ 28,080.00	$ 24,429.60
FireEye	Renewal MX 8400 Support Government CA 4 Year	RN-8400MX-CAG4Y	$ 74,880.00	$ 65,145.60
FireEye	Renewal MX 8400 Support Government CA 5 Year	RN-8400MX-CAG5Y	$ 93,600.00	$ 81,432.00
FireEye	Renewal MX 8400 Support Government CA Priorioty Plus 1 Year	RN-8400MX-CAP1Y	$ 19,434.00	$ 16,907.58
FireEye	Renewal-MX 8400 Support Government CA Priorioty Plus 2 Year	RN-8400MX-CAP2Y	$ 29,898.00	$ 26,011.26
FireEye	Renewal MX 8400 Support Government CA Priorioty Plus 3 Year	RN-8400MX-CAP3Y	$ 35,878.00	$ 31,213.86
FireEye	Renewal MX 8400 Support Government CA Priorioty Plus 4 Year	RN-8400MX-CAP4Y	$ 62,189.00	$ 54,104.43
FireEye	Renewal MX 8400 Support Government CA Priorioty Plus 5 Year	RN-8400MX-CAP5Y	$ 77,735.00	$ 67,629.45
FireEye	Renewal MX 8400 Support Platinum Priority Plus 1 Year	RN-8400MX-PPL1Y	$ 14,949.00	$ 13,005.63
FireEye	Renewal MX 8400 Support Platinum Priority Plus 2 Year	RN-8400MX-PPL2Y	$ 29,898.00	$ 26,011.26
FireEye	Renewal MX 8400 Support Platinum Priority Plus 3 Year	RN-8400MX-PPL3Y	$ 35,878.00	$ 31,213.86
FireEye	Renewal MX 8400 Support Platinum Priority Plus 4 Year	RN-8400MX-PPL4Y	$ 47,837.00	$ 41,618.19
FireEye	Renewal MX 8400 Support Platinum Priority Plus 5 Year	RN-8400MX-PPL5Y	$ 59,796.00	$ 52,022.52
FireEye	Renewal MX 8400 Support Platinum 1 Year	RN-8400MX-PTM1Y	$ 11,700.00	$ 10,179.00
FireEye	Renewal MX 8400 Support Platinum 2 Year	RN-8400MX-PTM2Y	$ 23,400.00	$ 20,358.00
FireEye	Renewal MX 8400 Support Platinum 3 Year	RN-8400MX-PTM3Y	$ 28,080.00	$ 24,429.60
FireEye	Renewal MX 8400 Support Platinum 4 Year	RN-8400MX-PTM4Y	$ 37,440.00	$ 32,572.80
FireEye	Renewal MX 8400 Support Platinum 5 Year	RN-8400MX-PTM5Y	$ 46,800.00	$ 40,716.00
FireEye	Renewal MX 8400 Support Government US 1 Year	RN-8400MX-USG1Y	$ 11,700.00	$ 10,179.00
FireEye	Renewal MX 8400 Support Government US 2 Year	RN-8400MX-USG2Y	$ 30,420.00	$ 26,465.40
FireEye	Renewal MX 8400 Support Government US 3 Year	RN-8400MX-USG3Y	$ 36,504.00	$ 31,758.48
FireEye	Renewal MX 8400 Support Government US 4 Year	RN-8400MX-USG4Y	$ 74,880.00	$ 65,145.60
FireEye	Renewal MX 8400 Support Government US 5 Year	RN-8400MX-USG5Y	$ 93,600.00	$ 81,432.00
FireEye	Renewal MX 8400 Support Government US Priorioty Plus 1 Year	RN-8400MX-USP1Y	$ 19,434.00	$ 16,907.58
FireEye	Renewal-MX 8400 Support Government US Priorioty Plus 2 Year	RN-8400MX-USP2Y	$ 38,868.00	$ 33,815.16
FireEye	Renewal MX 8400 Support Government US Priorioty Plus 3 Year	RN-8400MX-USP3Y	$ 35,878.00	$ 31,213.86
FireEye	Renewal MX 8400 Support Government US Priorioty Plus 4 Year	RN-8400MX-USP4Y	$ 62,189.00	$ 54,104.43
FireEye	Renewal MX 8400 Support Government US Priorioty Plus 5 Year	RN-8400MX-USP5Y	$ 83,715.00	$ 72,832.05
FireEye	Upgrade-MX 8400 Support GovCA to GovCA Priority Plus 1 Year	UP-8400MX-GAG2PP1Y	$ 4,549.00	$ 3,957.63
FireEye	Upgrade-MX 8400 Support GovCA to GovCA Priority Plus 2 Year	UP-8400MX-GAG2PP2Y	$ 8,448.00	$ 7,349.76
FireEye	Upgrade-MX 8400 Support GovCA to GovCA Priority Plus 3 Year	UP-8400MX-GAG2PP3Y	$ 15,596.00	$ 13,568.52
FireEye	Upgrade-MX 8400 Support GovCA to GovCA Priority Plus 4 Year	UP-8400MX-GAG2PP4Y	$ 20,794.00	$ 18,090.78
FireEye	Upgrade-MX 8400 Support GovCA to GovCA Priority Plus 5 Year	UP-8400MX-GAG2PP5Y	$ 25,992.00	$ 22,613.04
FireEye	Upgrade-MX 8400 Support Platinum to Plat Priority Plus 1 Year	UP-8400MX-PTM2PPP1Y	$ 3,249.00	$ 2,826.63
FireEye	Upgrade-MX 8400 Support Platinum to Plat Priority Plus 2 Year	UP-8400MX-PTM2PPP2Y	$ 6,498.00	$ 5,653.26
FireEye	Upgrade-MX 8400 Support Platinum to Plat Priority Plus 3 Year	UP-8400MX-PTM2PPP3Y	$ 7,798.00	$ 6,784.26
FireEye	Upgrade-MX 8400 Support Platinum to Plat Priority Plus 4 Year	UP-8400MX-PTM2PPP4Y	$ 10,397.00	$ 9,045.39
FireEye	Upgrade-MX 8400 Support Platinum to Plat Priority Plus 5 Year	UP-8400MX-PTM2PPP5Y	$ 12,996.00	$ 11,306.52
FireEye	Upgrade-MX 8400 Support GovUS to GovUS Priority Plus1 Year	UP-8400MX-USG2PP1Y	$ 3,249.00	$ 2,826.63
FireEye	Upgrade-MX 8400 Support GovUS to GovUS Priority Plus2 Year	UP-8400MX-USG2PP2Y	$ 8,448.00	$ 7,349.76
FireEye	Upgrade-MX 8400 Support GovUS to GovUS Priority Plus3 Year	UP-8400MX-USG2PP3Y	$ 7,798.00	$ 6,784.26

FireEye	Upgrade-MX 8400 Support GovUS to GovUS Priority Plus4 Year	UP-8400MX-USG2PP4Y	$ 20,794.00	$ 18,090.78
FireEye	Upgrade-MX 8400 Support GovUS to GovUS Priority Plus5 Year	UP-8400MX-USG2PP5Y	$ 16,895.00	$ 14,698.65
FireEye	Online Web Training-30-day access to eLearning, self-paced, course on Mobile Threat Prevention Cloud Deployment	EDU-OWT-BSC-MTP	$ 295.00	$ 256.65
FireEye	Eval - Mobile Threat Prevention - Mobile Security Management Cloud	EVL-MC-MSMC	$ -	$ -
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 100-499	MC-MSMC-000499-1Y	$ 62.00	$ 53.94
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 100-499	MC-MSMC-000499-2Y	$ 124.00	$ 107.88
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 100-499	MC-MSMC-000499-3Y	$ 167.40	$ 145.64
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 100-499	MC-MSMC-000499-4Y	$ 223.20	$ 194.18
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 100-499	MC-MSMC-000499-5Y	$ 279.00	$ 242.73
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 500-999	MC-MSMC-000999-1Y	$ 52.00	$ 45.24
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 500-999	MC-MSMC-000999-2Y	$ 104.00	$ 90.48
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 500-999	MC-MSMC-000999-3Y	$ 140.40	$ 122.15
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 500-999	MC-MSMC-000999-4Y	$ 187.20	$ 162.86
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 500-999	MC-MSMC-000999-5Y	$ 234.00	$ 203.58
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 1000-1999	MC-MSMC-001999-1Y	$ 43.00	$ 37.41
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 1000-1999	MC-MSMC-001999-2Y	$ 86.00	$ 74.82
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 1000-1999	MC-MSMC-001999-3Y	$ 116.10	$ 101.01
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 1000-1999	MC-MSMC-001999-4Y	$ 154.80	$ 134.68
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 1000-1999	MC-MSMC-001999-5Y	$ 193.50	$ 168.35
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 2000-4999	MC-MSMC-004999-1Y	$ 36.00	$ 31.32
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 2000-4999	MC-MSMC-004999-2Y	$ 72.00	$ 62.64
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 2000-4999	MC-MSMC-004999-3Y	$ 97.20	$ 84.56
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 2000-4999	MC-MSMC-004999-4Y	$ 129.60	$ 112.75
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 2000-4999	MC-MSMC-004999-5Y	$ 162.00	$ 140.94
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 5000-9999	MC-MSMC-009999-1Y	$ 30.00	$ 26.10
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 5000-9999	MC-MSMC-009999-2Y	$ 60.00	$ 52.20
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 5000-9999	MC-MSMC-009999-3Y	$ 81.00	$ 70.47
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 5000-9999	MC-MSMC-009999-4Y	$ 108.00	$ 93.96
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 5000-9999	MC-MSMC-009999-5Y	$ 135.00	$ 117.45
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 10000-19999	MC-MSMC-019999-1Y	$ 25.00	$ 21.75
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 10000-19999	MC-MSMC-019999-2Y	$ 50.00	$ 43.50
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 10000-19999	MC-MSMC-019999-3Y	$ 67.50	$ 58.73
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 10000-19999	MC-MSMC-019999-4Y	$ 90.00	$ 78.30
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 10000-19999	MC-MSMC-019999-5Y	$ 112.50	$ 97.88
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 20000-49999	MC-MSMC-049999-1Y	$ 21.00	$ 18.27
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 20000-49999	MC-MSMC-049999-2Y	$ 42.00	$ 36.54
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 20000-49999	MC-MSMC-049999-3Y	$ 56.70	$ 49.33
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 20000-49999	MC-MSMC-049999-4Y	$ 75.60	$ 65.77
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 20000-49999	MC-MSMC-049999-5Y	$ 94.50	$ 82.22
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 50000-74999	MC-MSMC-074999-1Y	$ 17.00	$ 14.79
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 50000-74999	MC-MSMC-074999-2Y	$ 34.00	$ 29.58
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 50000-74999	MC-MSMC-074999-3Y	$ 45.90	$ 39.93
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 50000-74999	MC-MSMC-074999-4Y	$ 61.20	$ 53.24
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 50000-74999	MC-MSMC-074999-5Y	$ 76.50	$ 66.56
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 75000-99999	MC-MSMC-099999-1Y	$ 14.00	$ 12.18
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 75000-99999	MC-MSMC-099999-2Y	$ 28.00	$ 24.36
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 75000-99999	MC-MSMC-099999-3Y	$ 37.80	$ 32.89
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 75000-99999	MC-MSMC-099999-4Y	$ 50.40	$ 43.85
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 75000-99999	MC-MSMC-099999-5Y	$ 63.00	$ 54.81

FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 100000+	MC-MSMC-100000+1Y	$ 12.00	$ 10.44
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 100000+	MC-MSMC-100000+2Y	$ 24.00	$ 20.88
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 100000+	MC-MSMC-100000+3Y	$ 32.40	$ 28.19
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 100000+	MC-MSMC-100000+4Y	$ 43.20	$ 37.58
FireEye	Mobile Threat Prevention - Mobile Security Management Cloud 5 Year 100000+	MC-MSMC-100000+5Y	$ 54.00	$ 46.98
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 100-499	RN-MC-MSMC-000499-1Y	$ 62.00	$ 53.94
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 100-499	RN-MC-MSMC-000499-2Y	$ 124.00	$ 107.88
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 100-499	RN-MC-MSMC-000499-3Y	$ 167.40	$ 145.64
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 100-499	RN-MC-MSMC-000499-4Y	$ 223.20	$ 194.18
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - Platinum	TAP-1KEPS-BD-1Y-P	$ 110,450.00	$ 96,091.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-BD-1Y-P	$ 118,988.00	$ 103,519.56
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - Platinum	TAP-5KEPS-BD-1Y-P	$ 121,208.00	$ 105,450.96
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - Platinum	TAP-10KEPS-BD-1Y-P	$ 148,132.00	$ 128,874.84
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - Platinum	TAP-15KEPS-BD-1Y-P	$ 222,198.00	$ 193,312.26
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - Platinum	TAP-20KEPS-BD-1Y-P	$ 265,078.00	$ 230,617.86
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - Platinum	TAP-25KEPS-BD-1Y-P	$ 314,780.00	$ 273,858.60
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - Platinum	TAP-30KEPS-BD-1Y-P	$ 377,736.00	$ 328,630.32
FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - Platinum	TAP-35KEPS-BD-1Y-P	$ 440,692.00	$ 383,402.04
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - Platinum	TAP-40KEPS-BD-1Y-P	$ 503,648.00	$ 438,173.76
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - Platinum	TAP-45KEPS-BD-1Y-P	$ 566,604.00	$ 492,945.48
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - Platinum	TAP-50KEPS-BD-1Y-P	$ 629,560.00	$ 547,717.20
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - Platinum	TAP-55KEPS-BD-1Y-P	$ 692,516.00	$ 602,488.92
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - Platinum	TAP-60KEPS-BD-1Y-P	$ 755,472.00	$ 657,260.64
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - Platinum	TAP-65KEPS-BD-1Y-P	$ 818,428.00	$ 712,032.36
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - Platinum	TAP-70KEPS-BD-1Y-P	$ 881,384.00	$ 766,804.08
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - Platinum	TAP-75KEPS-BD-1Y-P	$ 944,340.00	$ 821,575.80
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - Platinum	TAP-80KEPS-BD-1Y-P	$ 1,007,296.00	$ 876,347.52
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - Platinum	TAP-1KEPS-BD-2Y-P	$ 220,900.00	$ 192,183.00
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-BD-2Y-P	$ 237,976.00	$ 207,039.12
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - Platinum	TAP-5KEPS-BD-2Y-P	$ 242,416.00	$ 210,901.92
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - Platinum	TAP-10KEPS-BD-2Y-P	$ 296,264.00	$ 257,749.68
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - Platinum	TAP-15KEPS-BD-2Y-P	$ 444,396.00	$ 386,624.52
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - Platinum	TAP-20KEPS-BD-2Y-P	$ 530,156.00	$ 461,235.72
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - Platinum	TAP-25KEPS-BD-2Y-P	$ 629,560.00	$ 547,717.20
FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - Platinum	TAP-30KEPS-BD-2Y-P	$ 755,472.00	$ 657,260.64
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - Platinum	TAP-35KEPS-BD-2Y-P	$ 881,384.00	$ 766,804.08
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - Platinum	TAP-40KEPS-BD-2Y-P	$ 1,007,296.00	$ 876,347.52
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - Platinum	TAP-45KEPS-BD-2Y-P	$ 1,133,208.00	$ 985,890.96
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - Platinum	TAP-50KEPS-BD-2Y-P	$ 1,259,120.00	$ 1,095,434.40
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - Platinum	TAP-55KEPS-BD-2Y-P	$ 1,385,032.00	$ 1,204,977.84
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - Platinum	TAP-60KEPS-BD-2Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - Platinum	TAP-65KEPS-BD-2Y-P	$ 1,636,856.00	$ 1,424,064.72
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - Platinum	TAP-70KEPS-BD-2Y-P	$ 1,762,768.00	$ 1,533,608.16
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - Platinum	TAP-75KEPS-BD-2Y-P	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - Platinum	TAP-80KEPS-BD-2Y-P	$ 2,014,592.00	$ 1,752,695.04
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - Platinum	TAP-1KEPS-BD-3Y-P	$ 331,350.00	$ 288,274.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-BD-3Y-P	$ 356,964.00	$ 310,558.68
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - Platinum	TAP-5KEPS-BD-3Y-P	$ 363,624.00	$ 316,352.88
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - Platinum	TAP-10KEPS-BD-3Y-P	$ 444,396.00	$ 386,624.52

FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - Platinum	TAP-15KEPS-BD-3Y-P	$ 666,594.00	$ 579,936.78
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - Platinum	TAP-20KEPS-BD-3Y-P	$ 795,234.00	$ 691,853.58
FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - Platinum	TAP-25KEPS-BD-3Y-P	$ 944,340.00	$ 821,575.80
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - Platinum	TAP-30KEPS-BD-3Y-P	$ 1,133,208.00	$ 985,890.96
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - Platinum	TAP-35KEPS-BD-3Y-P	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - Platinum	TAP-40KEPS-BD-3Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - Platinum	TAP-45KEPS-BD-3Y-P	$ 1,699,812.00	$ 1,478,836.44
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - Platinum	TAP-50KEPS-BD-3Y-P	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - Platinum	TAP-55KEPS-BD-3Y-P	$ 2,077,548.00	$ 1,807,466.76
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - Platinum	TAP-60KEPS-BD-3Y-P	$ 2,266,416.00	$ 1,971,781.92
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - Platinum	TAP-65KEPS-BD-3Y-P	$ 2,455,284.00	$ 2,136,097.08
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - Platinum	TAP-70KEPS-BD-3Y-P	$ 2,644,152.00	$ 2,300,412.24
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - Platinum	TAP-75KEPS-BD-3Y-P	$ 2,833,020.00	$ 2,464,727.40
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - Platinum	TAP-80KEPS-BD-3Y-P	$ 3,021,888.00	$ 2,629,042.56
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - Platinum	TAP-1KEPS-BD-4Y-P	$ 441,800.00	$ 384,366.00
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-BD-4Y-P	$ 475,952.00	$ 414,078.24
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - Platinum	TAP-5KEPS-BD-4Y-P	$ 484,832.00	$ 421,803.84
FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - Platinum	TAP-10KEPS-BD-4Y-P	$ 592,528.00	$ 515,499.36
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - Platinum	TAP-15KEPS-BD-4Y-P	$ 888,792.00	$ 773,249.04
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - Platinum	TAP-20KEPS-BD-4Y-P	$ 1,060,312.00	$ 922,471.44
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - Platinum	TAP-25KEPS-BD-4Y-P	$ 1,259,120.00	$ 1,095,434.40
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - Platinum	TAP-30KEPS-BD-4Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - Platinum	TAP-35KEPS-BD-4Y-P	$ 1,762,768.00	$ 1,533,608.16
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - Platinum	TAP-40KEPS-BD-4Y-P	$ 2,014,592.00	$ 1,752,695.04
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - Platinum	TAP-45KEPS-BD-4Y-P	$ 2,266,416.00	$ 1,971,781.92
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - Platinum	TAP-50KEPS-BD-4Y-P	$ 2,518,240.00	$ 2,190,868.80
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - Platinum	TAP-55KEPS-BD-4Y-P	$ 2,770,064.00	$ 2,409,955.68
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - Platinum	TAP-60KEPS-BD-4Y-P	$ 3,021,888.00	$ 2,629,042.56
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - Platinum	TAP-65KEPS-BD-4Y-P	$ 3,273,712.00	$ 2,848,129.44
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - Platinum	TAP-70KEPS-BD-4Y-P	$ 3,525,536.00	$ 3,067,216.32
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - Platinum	TAP-75KEPS-BD-4Y-P	$ 3,777,360.00	$ 3,286,303.20
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - Platinum	TAP-80KEPS-BD-4Y-P	$ 4,029,184.00	$ 3,505,390.08
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - Platinum	TAP-1KEPS-BD-5Y-P	$ 552,250.00	$ 480,457.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-BD-5Y-P	$ 594,940.00	$ 517,597.80
FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - Platinum	TAP-5KEPS-BD-5Y-P	$ 606,040.00	$ 527,254.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - Platinum	TAP-10KEPS-BD-5Y-P	$ 740,660.00	$ 644,374.20
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - Platinum	TAP-15KEPS-BD-5Y-P	$ 1,110,990.00	$ 966,561.30
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - Platinum	TAP-20KEPS-BD-5Y-P	$ 1,325,390.00	$ 1,153,089.30
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - Platinum	TAP-25KEPS-BD-5Y-P	$ 1,573,900.00	$ 1,369,293.00
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - Platinum	TAP-30KEPS-BD-5Y-P	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - Platinum	TAP-35KEPS-BD-5Y-P	$ 2,203,460.00	$ 1,917,010.20
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - Platinum	TAP-40KEPS-BD-5Y-P	$ 2,518,240.00	$ 2,190,868.80
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - Platinum	TAP-45KEPS-BD-5Y-P	$ 2,833,020.00	$ 2,464,727.40
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - Platinum	TAP-50KEPS-BD-5Y-P	$ 3,147,800.00	$ 2,738,586.00
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - Platinum	TAP-55KEPS-BD-5Y-P	$ 3,462,580.00	$ 3,012,444.60
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - Platinum	TAP-60KEPS-BD-5Y-P	$ 3,777,360.00	$ 3,286,303.20
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - Platinum	TAP-65KEPS-BD-5Y-P	$ 4,092,140.00	$ 3,560,161.80
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - Platinum	TAP-70KEPS-BD-5Y-P	$ 4,406,920.00	$ 3,834,020.40
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - Platinum	TAP-75KEPS-BD-5Y-P	$ 4,721,700.00	$ 4,107,879.00

FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - Platinum	TAP-80KEPS-BD-5Y-P	$ 5,036,480.00	$ 4,381,737.60
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 1YR - Platinum	RN-TAP-1KEPS-BD-1Y-P	$ 110,450.00	$ 96,091.50
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 1YR - Platinum	RN-TAP-2.5KEPS-BD-1Y-P	$ 118,988.00	$ 103,519.56
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 1YR - Platinum	RN-TAP-5KEPS-BD-1Y-P	$ 121,208.00	$ 105,450.96
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 1YR - Platinum	RN-TAP-10KEPS-BD-1Y-P	$ 148,132.00	$ 128,874.84
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 1YR - Platinum	RN-TAP-15KEPS-BD-1Y-P	$ 222,198.00	$ 193,312.26
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 1YR - Platinum	RN-TAP-20KEPS-BD-1Y-P	$ 265,078.00	$ 230,617.86
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 1YR - Platinum	RN-TAP-25KEPS-BD-1Y-P	$ 314,780.00	$ 273,858.60
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 1YR - Platinum	RN-TAP-30KEPS-BD-1Y-P	$ 377,736.00	$ 328,630.32
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 1YR - Platinum	RN-TAP-35KEPS-BD-1Y-P	$ 440,692.00	$ 383,402.04
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 1YR - Platinum	RN-TAP-40KEPS-BD-1Y-P	$ 503,648.00	$ 438,173.76
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 1YR - Platinum	RN-TAP-45KEPS-BD-1Y-P	$ 566,604.00	$ 492,945.48
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 1YR - Platinum	RN-TAP-50KEPS-BD-1Y-P	$ 629,560.00	$ 547,717.20
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 1YR - Platinum	RN-TAP-55KEPS-BD-1Y-P	$ 692,516.00	$ 602,488.92
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 1YR - Platinum	RN-TAP-60KEPS-BD-1Y-P	$ 755,472.00	$ 657,260.64
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 1YR - Platinum	RN-TAP-65KEPS-BD-1Y-P	$ 818,428.00	$ 712,032.36
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 1YR - Platinum	RN-TAP-70KEPS-BD-1Y-P	$ 881,384.00	$ 766,804.08
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 1YR - Platinum	RN-TAP-75KEPS-BD-1Y-P	$ 944,340.00	$ 821,575.80
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 1YR - Platinum	RN-TAP-80KEPS-BD-1Y-P	$ 1,007,296.00	$ 876,347.52
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 2YR - Platinum	RN-TAP-1KEPS-BD-2Y-P	$ 220,900.00	$ 192,183.00
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 2YR - Platinum	RN-TAP-2.5KEPS-BD-2Y-P	$ 237,976.00	$ 207,039.12
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 2YR - Platinum	RN-TAP-5KEPS-BD-2Y-P	$ 242,416.00	$ 210,901.92
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 2YR - Platinum	RN-TAP-10KEPS-BD-2Y-P	$ 296,264.00	$ 257,749.68
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 2YR - Platinum	RN-TAP-15KEPS-BD-2Y-P	$ 444,396.00	$ 386,624.52
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 2YR - Platinum	RN-TAP-20KEPS-BD-2Y-P	$ 530,156.00	$ 461,235.72
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 2YR - Platinum	RN-TAP-25KEPS-BD-2Y-P	$ 629,560.00	$ 547,717.20
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 2YR - Platinum	RN-TAP-30KEPS-BD-2Y-P	$ 755,472.00	$ 657,260.64
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 2YR - Platinum	RN-TAP-35KEPS-BD-2Y-P	$ 881,384.00	$ 766,804.08
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 2YR - Platinum	RN-TAP-40KEPS-BD-2Y-P	$ 1,007,296.00	$ 876,347.52
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 2YR - Platinum	RN-TAP-45KEPS-BD-2Y-P	$ 1,133,208.00	$ 985,890.96
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 2YR - Platinum	RN-TAP-50KEPS-BD-2Y-P	$ 1,259,120.00	$ 1,095,434.40
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 2YR - Platinum	RN-TAP-55KEPS-BD-2Y-P	$ 1,385,032.00	$ 1,204,977.84
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 2YR - Platinum	RN-TAP-60KEPS-BD-2Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 2YR - Platinum	RN-TAP-65KEPS-BD-2Y-P	$ 1,636,856.00	$ 1,424,064.72
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 2YR - Platinum	RN-TAP-70KEPS-BD-2Y-P	$ 1,762,768.00	$ 1,533,608.16
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 2YR - Platinum	RN-TAP-75KEPS-BD-2Y-P	$ 1,888,680.00	$ 1,643,151.60
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 2YR - Platinum	RN-TAP-80KEPS-BD-2Y-P	$ 2,014,592.00	$ 1,752,695.04
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 3YR - Platinum	RN-TAP-1KEPS-BD-3Y-P	$ 331,350.00	$ 288,274.50
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 3YR - Platinum	RN-TAP-2.5KEPS-BD-3Y-P	$ 356,964.00	$ 310,558.68
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 3YR - Platinum	RN-TAP-5KEPS-BD-3Y-P	$ 363,624.00	$ 316,352.88
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 3YR - Platinum	RN-TAP-10KEPS-BD-3Y-P	$ 444,396.00	$ 386,624.52
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 3YR - Platinum	RN-TAP-15KEPS-BD-3Y-P	$ 666,594.00	$ 579,936.78
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 3YR - Platinum	RN-TAP-20KEPS-BD-3Y-P	$ 795,234.00	$ 691,853.58
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 3YR - Platinum	RN-TAP-25KEPS-BD-3Y-P	$ 944,340.00	$ 821,575.80
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 3YR - Platinum	RN-TAP-30KEPS-BD-3Y-P	$ 1,133,208.00	$ 985,890.96
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 3YR - Platinum	RN-TAP-35KEPS-BD-3Y-P	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 3YR - Platinum	RN-TAP-40KEPS-BD-3Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 3YR - Platinum	RN-TAP-45KEPS-BD-3Y-P	$ 1,699,812.00	$ 1,478,836.44
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 3YR - Platinum	RN-TAP-50KEPS-BD-3Y-P	$ 1,888,680.00	$ 1,643,151.60

FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 3YR - Platinum	RN-TAP-55KEPS-BD-3Y-P	$ 2,077,548.00	$ 1,807,466.76
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 3YR - Platinum	RN-TAP-60KEPS-BD-3Y-P	$ 2,266,416.00	$ 1,971,781.92
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 3YR - Platinum	RN-TAP-65KEPS-BD-3Y-P	$ 2,455,284.00	$ 2,136,097.08
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 3YR - Platinum	RN-TAP-70KEPS-BD-3Y-P	$ 2,644,152.00	$ 2,300,412.24
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 3YR - Platinum	RN-TAP-75KEPS-BD-3Y-P	$ 2,833,020.00	$ 2,464,727.40
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 3YR - Platinum	RN-TAP-80KEPS-BD-3Y-P	$ 3,021,888.00	$ 2,629,042.56
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 4YR - Platinum	RN-TAP-1KEPS-BD-4Y-P	$ 441,800.00	$ 384,366.00
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 4YR - Platinum	RN-TAP-2.5KEPS-BD-4Y-P	$ 475,952.00	$ 414,078.24
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 4YR - Platinum	RN-TAP-5KEPS-BD-4Y-P	$ 484,832.00	$ 421,803.84
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 4YR - Platinum	RN-TAP-10KEPS-BD-4Y-P	$ 592,528.00	$ 515,499.36
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 4YR - Platinum	RN-TAP-15KEPS-BD-4Y-P	$ 888,792.00	$ 773,249.04
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 4YR - Platinum	RN-TAP-20KEPS-BD-4Y-P	$ 1,060,312.00	$ 922,471.44
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 4YR - Platinum	RN-TAP-25KEPS-BD-4Y-P	$ 1,259,120.00	$ 1,095,434.40
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 4YR - Platinum	RN-TAP-30KEPS-BD-4Y-P	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 4YR - Platinum	RN-TAP-35KEPS-BD-4Y-P	$ 1,762,768.00	$ 1,533,608.16
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 4YR - Platinum	RN-TAP-40KEPS-BD-4Y-P	$ 2,014,592.00	$ 1,752,695.04
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 4YR - Platinum	RN-TAP-45KEPS-BD-4Y-P	$ 2,266,416.00	$ 1,971,781.92
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 4YR - Platinum	RN-TAP-50KEPS-BD-4Y-P	$ 2,518,240.00	$ 2,190,868.80
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 4YR - Platinum	RN-TAP-55KEPS-BD-4Y-P	$ 2,770,064.00	$ 2,409,955.68
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 4YR - Platinum	RN-TAP-60KEPS-BD-4Y-P	$ 3,021,888.00	$ 2,629,042.56
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 4YR - Platinum	RN-TAP-65KEPS-BD-4Y-P	$ 3,273,712.00	$ 2,848,129.44
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 4YR - Platinum	RN-TAP-70KEPS-BD-4Y-P	$ 3,525,536.00	$ 3,067,216.32
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 4YR - Platinum	RN-TAP-75KEPS-BD-4Y-P	$ 3,777,360.00	$ 3,286,303.20
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 4YR - Platinum	RN-TAP-80KEPS-BD-4Y-P	$ 4,029,184.00	$ 3,505,390.08
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-BD-1Y-PPP	$ 115,973.00	$ 100,896.51
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-BD-1Y-PPP	$ 124,937.00	$ 108,695.19
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-BD-1Y-PPP	$ 127,268.00	$ 110,723.16
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-BD-1Y-PPP	$ 155,539.00	$ 135,318.93
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-BD-1Y-PPP	$ 233,308.00	$ 202,977.96
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-BD-1Y-PPP	$ 278,332.00	$ 242,148.84
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-BD-1Y-PPP	$ 330,519.00	$ 287,551.53
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-BD-1Y-PPP	$ 396,623.00	$ 345,062.01
FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-BD-1Y-PPP	$ 462,727.00	$ 402,572.49
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-BD-1Y-PPP	$ 528,830.00	$ 460,082.10
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - Plat Prio Plus	TAP-45KEPS-BD-1Y-PPP	$ 594,934.00	$ 517,592.58
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - Plat Prio Plus	TAP-50KEPS-BD-1Y-PPP	$ 661,038.00	$ 575,103.06
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - Plat Prio Plus	TAP-55KEPS-BD-1Y-PPP	$ 727,142.00	$ 632,613.54
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - Plat Prio Plus	TAP-60KEPS-BD-1Y-PPP	$ 793,246.00	$ 690,124.02
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - Plat Prio Plus	TAP-65KEPS-BD-1Y-PPP	$ 859,349.00	$ 747,633.63
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - Plat Prio Plus	TAP-70KEPS-BD-1Y-PPP	$ 925,453.00	$ 805,144.11
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - Plat Prio Plus	TAP-75KEPS-BD-1Y-PPP	$ 991,557.00	$ 862,654.59
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - Plat Prio Plus	TAP-80KEPS-BD-1Y-PPP	$ 1,057,661.00	$ 920,165.07
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-BD-2Y-PPP	$ 231,946.00	$ 201,793.02
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-BD-2Y-PPP	$ 249,874.00	$ 217,390.38
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-BD-2Y-PPP	$ 254,536.00	$ 221,446.32
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-BD-2Y-PPP	$ 311,078.00	$ 270,637.86
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-BD-2Y-PPP	$ 466,616.00	$ 405,955.92
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-BD-2Y-PPP	$ 556,664.00	$ 484,297.68
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-BD-2Y-PPP	$ 661,038.00	$ 575,103.06

FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-BD-2Y-PPP	$ 793,246.00	$ 690,124.02
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-BD-2Y-PPP	$ 925,454.00	$ 805,144.98
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-BD-2Y-PPP	$ 1,057,660.00	$ 920,164.20
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - Plat Prio Plus	TAP-45KEPS-BD-2Y-PPP	$ 1,189,868.00	$ 1,035,185.16
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - Plat Prio Plus	TAP-50KEPS-BD-2Y-PPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - Plat Prio Plus	TAP-55KEPS-BD-2Y-PPP	$ 1,454,284.00	$ 1,265,227.08
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - Plat Prio Plus	TAP-60KEPS-BD-2Y-PPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - Plat Prio Plus	TAP-65KEPS-BD-2Y-PPP	$ 1,718,698.00	$ 1,495,267.26
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - Plat Prio Plus	TAP-70KEPS-BD-2Y-PPP	$ 1,850,906.00	$ 1,610,288.22
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - Plat Prio Plus	TAP-75KEPS-BD-2Y-PPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - Plat Prio Plus	TAP-80KEPS-BD-2Y-PPP	$ 2,115,322.00	$ 1,840,330.14
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-BD-3Y-PPP	$ 347,919.00	$ 302,689.53
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-BD-3Y-PPP	$ 374,811.00	$ 326,085.57
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-BD-3Y-PPP	$ 381,804.00	$ 332,169.48
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-BD-3Y-PPP	$ 466,617.00	$ 405,956.79
FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-BD-3Y-PPP	$ 699,924.00	$ 608,933.88
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-BD-3Y-PPP	$ 834,996.00	$ 726,446.52
FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-BD-3Y-PPP	$ 991,557.00	$ 862,654.59
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-BD-3Y-PPP	$ 1,189,869.00	$ 1,035,186.03
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-BD-3Y-PPP	$ 1,388,181.00	$ 1,207,717.47
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-BD-3Y-PPP	$ 1,586,490.00	$ 1,380,246.30
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - Plat Prio Plus	TAP-45KEPS-BD-3Y-PPP	$ 1,784,802.00	$ 1,552,777.74
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - Plat Prio Plus	TAP-50KEPS-BD-3Y-PPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - Plat Prio Plus	TAP-55KEPS-BD-3Y-PPP	$ 2,181,426.00	$ 1,897,840.62
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - Plat Prio Plus	TAP-60KEPS-BD-3Y-PPP	$ 2,379,738.00	$ 2,070,372.06
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - Plat Prio Plus	TAP-65KEPS-BD-3Y-PPP	$ 2,578,047.00	$ 2,242,900.89
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - Plat Prio Plus	TAP-70KEPS-BD-3Y-PPP	$ 2,776,359.00	$ 2,415,432.33
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - Plat Prio Plus	TAP-75KEPS-BD-3Y-PPP	$ 2,974,671.00	$ 2,587,963.77
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - Plat Prio Plus	TAP-80KEPS-BD-3Y-PPP	$ 3,172,983.00	$ 2,760,495.21
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-BD-4Y-PPP	$ 463,892.00	$ 403,586.04
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-BD-4Y-PPP	$ 499,748.00	$ 434,780.76
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-BD-4Y-PPP	$ 509,072.00	$ 442,892.64
FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-BD-4Y-PPP	$ 622,156.00	$ 541,275.72
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-BD-4Y-PPP	$ 933,232.00	$ 811,911.84
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-BD-4Y-PPP	$ 1,113,328.00	$ 968,595.36
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-BD-4Y-PPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-BD-4Y-PPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-BD-4Y-PPP	$ 1,850,908.00	$ 1,610,289.96
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-BD-4Y-PPP	$ 2,115,320.00	$ 1,840,328.40
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - Plat Prio Plus	TAP-45KEPS-BD-4Y-PPP	$ 2,379,736.00	$ 2,070,370.32
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - Plat Prio Plus	TAP-50KEPS-BD-4Y-PPP	$ 2,644,152.00	$ 2,300,412.24
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - Plat Prio Plus	TAP-55KEPS-BD-4Y-PPP	$ 2,908,568.00	$ 2,530,454.16
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - Plat Prio Plus	TAP-60KEPS-BD-4Y-PPP	$ 3,172,984.00	$ 2,760,496.08
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - Plat Prio Plus	TAP-65KEPS-BD-4Y-PPP	$ 3,437,396.00	$ 2,990,534.52
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - Plat Prio Plus	TAP-70KEPS-BD-4Y-PPP	$ 3,701,812.00	$ 3,220,576.44
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - Plat Prio Plus	TAP-75KEPS-BD-4Y-PPP	$ 3,966,228.00	$ 3,450,618.36
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - Plat Prio Plus	TAP-80KEPS-BD-4Y-PPP	$ 4,230,644.00	$ 3,680,660.28
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-BD-5Y-PPP	$ 579,865.00	$ 504,482.55
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-BD-5Y-PPP	$ 624,685.00	$ 543,475.95

FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-BD-5Y-PPP	$ 636,340.00	$ 553,615.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-BD-5Y-PPP	$ 777,695.00	$ 676,594.65
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-BD-5Y-PPP	$ 1,166,540.00	$ 1,014,889.80
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-BD-5Y-PPP	$ 1,391,660.00	$ 1,210,744.20
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-BD-5Y-PPP	$ 1,652,595.00	$ 1,437,757.65
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-BD-5Y-PPP	$ 1,983,115.00	$ 1,725,310.05
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-BD-5Y-PPP	$ 2,313,635.00	$ 2,012,862.45
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-BD-5Y-PPP	$ 2,644,150.00	$ 2,300,410.50
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - Plat Prio Plus	TAP-45KEPS-BD-5Y-PPP	$ 2,974,670.00	$ 2,587,962.90
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - Plat Prio Plus	TAP-50KEPS-BD-5Y-PPP	$ 3,305,190.00	$ 2,875,515.30
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - Plat Prio Plus	TAP-55KEPS-BD-5Y-PPP	$ 3,635,710.00	$ 3,163,067.70
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - Plat Prio Plus	TAP-60KEPS-BD-5Y-PPP	$ 3,966,230.00	$ 3,450,620.10
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - Plat Prio Plus	TAP-65KEPS-BD-5Y-PPP	$ 4,296,745.00	$ 3,738,168.15
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - Plat Prio Plus	TAP-70KEPS-BD-5Y-PPP	$ 4,627,265.00	$ 4,025,720.55
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - Plat Prio Plus	TAP-75KEPS-BD-5Y-PPP	$ 4,957,785.00	$ 4,313,272.95
FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - Plat Prio Plus	TAP-80KEPS-BD-5Y-PPP	$ 5,288,305.00	$ 4,600,825.35
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 1YR - Plat Prio Plus	RN-TAP-1KEPS-BD-1Y-PPP	$ 115,973.00	$ 100,896.51
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 1YR - Plat Prio Plus	RN-TAP-2.5KEPS-BD-1Y-PPP	$ 124,937.00	$ 108,695.19
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 1YR - Plat Prio Plus	RN-TAP-5KEPS-BD-1Y-PPP	$ 127,268.00	$ 110,723.16
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 1YR - Plat Prio Plus	RN-TAP-10KEPS-BD-1Y-PPP	$ 155,539.00	$ 135,318.93
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 1YR - Plat Prio Plus	RN-TAP-15KEPS-BD-1Y-PPP	$ 233,308.00	$ 202,977.96
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 1YR - Plat Prio Plus	RN-TAP-20KEPS-BD-1Y-PPP	$ 278,332.00	$ 242,148.84
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 1YR - Plat Prio Plus	RN-TAP-25KEPS-BD-1Y-PPP	$ 330,519.00	$ 287,551.53
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 1YR - Plat Prio Plus	RN-TAP-30KEPS-BD-1Y-PPP	$ 396,623.00	$ 345,062.01
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 1YR - Plat Prio Plus	RN-TAP-35KEPS-BD-1Y-PPP	$ 462,727.00	$ 402,572.49
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 1YR - Plat Prio Plus	RN-TAP-40KEPS-BD-1Y-PPP	$ 528,830.00	$ 460,082.10
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 1YR - Plat Prio Plus	RN-TAP-45KEPS-BD-1Y-PPP	$ 594,934.00	$ 517,592.58
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 1YR - Plat Prio Plus	RN-TAP-50KEPS-BD-1Y-PPP	$ 661,038.00	$ 575,103.06
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 1YR - Plat Prio Plus	RN-TAP-55KEPS-BD-1Y-PPP	$ 727,142.00	$ 632,613.54
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 1YR - Plat Prio Plus	RN-TAP-60KEPS-BD-1Y-PPP	$ 793,246.00	$ 690,124.02
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 1YR - Plat Prio Plus	RN-TAP-65KEPS-BD-1Y-PPP	$ 859,349.00	$ 747,633.63
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 1YR - Plat Prio Plus	RN-TAP-70KEPS-BD-1Y-PPP	$ 925,453.00	$ 805,144.11
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 1YR - Plat Prio Plus	RN-TAP-75KEPS-BD-1Y-PPP	$ 991,557.00	$ 862,654.59
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 1YR - Plat Prio Plus	RN-TAP-80KEPS-BD-1Y-PPP	$ 1,057,661.00	$ 920,165.07
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 2YR - Plat Prio Plus	RN-TAP-1KEPS-BD-2Y-PPP	$ 231,946.00	$ 201,793.02
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 2YR - Plat Prio Plus	RN-TAP-2.5KEPS-BD-2Y-PPP	$ 249,874.00	$ 217,390.38
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 2YR - Plat Prio Plus	RN-TAP-5KEPS-BD-2Y-PPP	$ 254,536.00	$ 221,446.32
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 2YR - Plat Prio Plus	RN-TAP-10KEPS-BD-2Y-PPP	$ 311,078.00	$ 270,637.86
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 2YR - Plat Prio Plus	RN-TAP-15KEPS-BD-2Y-PPP	$ 466,616.00	$ 405,955.92
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 2YR - Plat Prio Plus	RN-TAP-20KEPS-BD-2Y-PPP	$ 556,664.00	$ 484,297.68
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 2YR - Plat Prio Plus	RN-TAP-25KEPS-BD-2Y-PPP	$ 661,038.00	$ 575,103.06
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 2YR - Plat Prio Plus	RN-TAP-30KEPS-BD-2Y-PPP	$ 793,246.00	$ 690,124.02
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 2YR - Plat Prio Plus	RN-TAP-35KEPS-BD-2Y-PPP	$ 925,454.00	$ 805,144.98
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 2YR - Plat Prio Plus	RN-TAP-40KEPS-BD-2Y-PPP	$ 1,057,660.00	$ 920,164.20
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 2YR - Plat Prio Plus	RN-TAP-45KEPS-BD-2Y-PPP	$ 1,189,868.00	$ 1,035,185.16
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 2YR - Plat Prio Plus	RN-TAP-50KEPS-BD-2Y-PPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 2YR - Plat Prio Plus	RN-TAP-55KEPS-BD-2Y-PPP	$ 1,454,284.00	$ 1,265,227.08
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 2YR - Plat Prio Plus	RN-TAP-60KEPS-BD-2Y-PPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 2YR - Plat Prio Plus	RN-TAP-65KEPS-BD-2Y-PPP	$ 1,718,698.00	$ 1,495,267.26

FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 2YR - Plat Prio Plus	RN-TAP-70KEPS-BD-2Y-PPP	$ 1,850,906.00	$ 1,610,288.22
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 2YR - Plat Prio Plus	RN-TAP-75KEPS-BD-2Y-PPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 2YR - Plat Prio Plus	RN-TAP-80KEPS-BD-2Y-PPP	$ 2,115,322.00	$ 1,840,330.14
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 3YR - Plat Prio Plus	RN-TAP-1KEPS-BD-3Y-PPP	$ 347,919.00	$ 302,689.53
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 3YR - Plat Prio Plus	RN-TAP-2.5KEPS-BD-3Y-PPP	$ 374,811.00	$ 326,085.57
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 3YR - Plat Prio Plus	RN-TAP-5KEPS-BD-3Y-PPP	$ 381,804.00	$ 332,169.48
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 3YR - Plat Prio Plus	RN-TAP-10KEPS-BD-3Y-PPP	$ 466,617.00	$ 405,956.79
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 3YR - Plat Prio Plus	RN-TAP-15KEPS-BD-3Y-PPP	$ 699,924.00	$ 608,933.88
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 3YR - Plat Prio Plus	RN-TAP-20KEPS-BD-3Y-PPP	$ 834,996.00	$ 726,446.52
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 3YR - Plat Prio Plus	RN-TAP-25KEPS-BD-3Y-PPP	$ 991,557.00	$ 862,654.59
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 3YR - Plat Prio Plus	RN-TAP-30KEPS-BD-3Y-PPP	$ 1,189,869.00	$ 1,035,186.03
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 3YR - Plat Prio Plus	RN-TAP-35KEPS-BD-3Y-PPP	$ 1,388,181.00	$ 1,207,717.47
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 3YR - Plat Prio Plus	RN-TAP-40KEPS-BD-3Y-PPP	$ 1,586,490.00	$ 1,380,246.30
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 3YR - Plat Prio Plus	RN-TAP-45KEPS-BD-3Y-PPP	$ 1,784,802.00	$ 1,552,777.74
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 3YR - Plat Prio Plus	RN-TAP-50KEPS-BD-3Y-PPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 3YR - Plat Prio Plus	RN-TAP-55KEPS-BD-3Y-PPP	$ 2,181,426.00	$ 1,897,840.62
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 3YR - Plat Prio Plus	RN-TAP-60KEPS-BD-3Y-PPP	$ 2,379,738.00	$ 2,070,372.06
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 3YR - Plat Prio Plus	RN-TAP-65KEPS-BD-3Y-PPP	$ 2,578,047.00	$ 2,242,900.89
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 3YR - Plat Prio Plus	RN-TAP-70KEPS-BD-3Y-PPP	$ 2,776,359.00	$ 2,415,432.33
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 3YR - Plat Prio Plus	RN-TAP-75KEPS-BD-3Y-PPP	$ 2,974,671.00	$ 2,587,963.77
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 3YR - Plat Prio Plus	RN-TAP-80KEPS-BD-3Y-PPP	$ 3,172,983.00	$ 2,760,495.21
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 4YR - Plat Prio Plus	RN-TAP-1KEPS-BD-4Y-PPP	$ 463,892.00	$ 403,586.04
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 4YR - Plat Prio Plus	RN-TAP-2.5KEPS-BD-4Y-PPP	$ 499,748.00	$ 434,780.76
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 4YR - Plat Prio Plus	RN-TAP-5KEPS-BD-4Y-PPP	$ 509,072.00	$ 442,892.64
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 4YR - Plat Prio Plus	RN-TAP-10KEPS-BD-4Y-PPP	$ 622,156.00	$ 541,275.72
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 4YR - Plat Prio Plus	RN-TAP-15KEPS-BD-4Y-PPP	$ 933,232.00	$ 811,911.84
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 4YR - Plat Prio Plus	RN-TAP-20KEPS-BD-4Y-PPP	$ 1,113,328.00	$ 968,595.36
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 4YR - Plat Prio Plus	RN-TAP-25KEPS-BD-4Y-PPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 4YR - Plat Prio Plus	RN-TAP-30KEPS-BD-4Y-PPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 4YR - Plat Prio Plus	RN-TAP-35KEPS-BD-4Y-PPP	$ 1,850,908.00	$ 1,610,289.96
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 4YR - Plat Prio Plus	RN-TAP-40KEPS-BD-4Y-PPP	$ 2,115,320.00	$ 1,840,328.40
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 4YR - Plat Prio Plus	RN-TAP-45KEPS-BD-4Y-PPP	$ 2,379,736.00	$ 2,070,370.32
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 4YR - Plat Prio Plus	RN-TAP-50KEPS-BD-4Y-PPP	$ 2,644,152.00	$ 2,300,412.24
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 4YR - Plat Prio Plus	RN-TAP-55KEPS-BD-4Y-PPP	$ 2,908,568.00	$ 2,530,454.16
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 4YR - Plat Prio Plus	RN-TAP-60KEPS-BD-4Y-PPP	$ 3,172,984.00	$ 2,760,496.08
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 4YR - Plat Prio Plus	RN-TAP-65KEPS-BD-4Y-PPP	$ 3,437,396.00	$ 2,990,534.52
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 4YR - Plat Prio Plus	RN-TAP-70KEPS-BD-4Y-PPP	$ 3,701,812.00	$ 3,220,576.44
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 4YR - Plat Prio Plus	RN-TAP-75KEPS-BD-4Y-PPP	$ 3,966,228.00	$ 3,450,618.36
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 4YR - Plat Prio Plus	RN-TAP-80KEPS-BD-4Y-PPP	$ 4,230,644.00	$ 3,680,660.28
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - Platinum	TAP-1KEPS-SS-1Y-P	$ 232,635.00	$ 202,392.45
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-SS-1Y-P	$ 276,258.00	$ 240,344.46
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - Platinum	TAP-5KEPS-SS-1Y-P	$ 314,613.00	$ 273,713.31
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - Platinum	TAP-10KEPS-SS-1Y-P	$ 475,966.00	$ 414,090.42
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - Platinum	TAP-15KEPS-SS-1Y-P	$ 713,949.00	$ 621,135.63
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - Platinum	TAP-20KEPS-SS-1Y-P	$ 951,932.00	$ 828,180.84
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - Platinum	TAP-25KEPS-SS-1Y-P	$ 1,189,915.00	$ 1,035,226.05
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - Platinum	TAP-30KEPS-SS-1Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - Platinum	TAP-35KEPS-SS-1Y-P	$ 1,665,881.00	$ 1,449,316.47
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - Platinum	TAP-40KEPS-SS-1Y-P	$ 1,903,864.00	$ 1,656,361.68

FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - Platinum	TAP-45KEPS-SS-1Y-P	$ 2,141,847.00	$ 1,863,406.89
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - Platinum	TAP-50KEPS-SS-1Y-P	$ 2,379,830.00	$ 2,070,452.10
FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - Platinum	TAP-55KEPS-SS-1Y-P	$ 2,617,813.00	$ 2,277,497.31
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - Platinum	TAP-60KEPS-SS-1Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - Platinum	TAP-65KEPS-SS-1Y-P	$ 3,093,779.00	$ 2,691,587.73
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - Platinum	TAP-70KEPS-SS-1Y-P	$ 3,331,762.00	$ 2,898,632.94
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - Platinum	TAP-75KEPS-SS-1Y-P	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - Platinum	TAP-80KEPS-SS-1Y-P	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - Platinum	TAP-1KEPS-SS-2Y-P	$ 465,270.00	$ 404,784.90
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-SS-2Y-P	$ 552,516.00	$ 480,688.92
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - Platinum	TAP-5KEPS-SS-2Y-P	$ 629,226.00	$ 547,426.62
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - Platinum	TAP-10KEPS-SS-2Y-P	$ 951,932.00	$ 828,180.84
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - Platinum	TAP-15KEPS-SS-2Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - Platinum	TAP-20KEPS-SS-2Y-P	$ 1,903,864.00	$ 1,656,361.68
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - Platinum	TAP-25KEPS-SS-2Y-P	$ 2,379,830.00	$ 2,070,452.10
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - Platinum	TAP-30KEPS-SS-2Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - Platinum	TAP-35KEPS-SS-2Y-P	$ 3,331,762.00	$ 2,898,632.94
FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - Platinum	TAP-40KEPS-SS-2Y-P	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - Platinum	TAP-45KEPS-SS-2Y-P	$ 4,283,694.00	$ 3,726,813.78
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - Platinum	TAP-50KEPS-SS-2Y-P	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - Platinum	TAP-55KEPS-SS-2Y-P	$ 5,235,626.00	$ 4,554,994.62
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - Platinum	TAP-60KEPS-SS-2Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - Platinum	TAP-65KEPS-SS-2Y-P	$ 6,187,558.00	$ 5,383,175.46
FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - Platinum	TAP-70KEPS-SS-2Y-P	$ 6,663,524.00	$ 5,797,265.88
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - Platinum	TAP-75KEPS-SS-2Y-P	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - Platinum	TAP-80KEPS-SS-2Y-P	$ 7,615,456.00	$ 6,625,446.72
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - Platinum	TAP-1KEPS-SS-3Y-P	$ 697,905.00	$ 607,177.35
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-SS-3Y-P	$ 828,774.00	$ 721,033.38
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - Platinum	TAP-5KEPS-SS-3Y-P	$ 943,839.00	$ 821,139.93
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - Platinum	TAP-10KEPS-SS-3Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - Platinum	TAP-15KEPS-SS-3Y-P	$ 2,141,847.00	$ 1,863,406.89
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - Platinum	TAP-20KEPS-SS-3Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - Platinum	TAP-25KEPS-SS-3Y-P	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - Platinum	TAP-30KEPS-SS-3Y-P	$ 4,283,694.00	$ 3,726,813.78
FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - Platinum	TAP-35KEPS-SS-3Y-P	$ 4,997,643.00	$ 4,347,949.41
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - Platinum	TAP-40KEPS-SS-3Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - Platinum	TAP-45KEPS-SS-3Y-P	$ 6,425,541.00	$ 5,590,220.67
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - Platinum	TAP-50KEPS-SS-3Y-P	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - Platinum	TAP-55KEPS-SS-3Y-P	$ 7,853,439.00	$ 6,832,491.93
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - Platinum	TAP-60KEPS-SS-3Y-P	$ 8,567,388.00	$ 7,453,627.56
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - Platinum	TAP-65KEPS-SS-3Y-P	$ 9,281,337.00	$ 8,074,763.19
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - Platinum	TAP-70KEPS-SS-3Y-P	$ 9,995,286.00	$ 8,695,898.82
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - Platinum	TAP-75KEPS-SS-3Y-P	##############	$ 9,317,034.45
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - Platinum	TAP-80KEPS-SS-3Y-P	##############	$ 9,938,170.08
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - Platinum	TAP-1KEPS-SS-4Y-P	$ 930,540.00	$ 809,569.80
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-SS-4Y-P	$ 1,105,032.00	$ 961,377.84
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - Platinum	TAP-5KEPS-SS-4Y-P	$ 1,258,452.00	$ 1,094,853.24
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - Platinum	TAP-10KEPS-SS-4Y-P	$ 1,903,864.00	$ 1,656,361.68
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - Platinum	TAP-15KEPS-SS-4Y-P	$ 2,855,796.00	$ 2,484,542.52

FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - Platinum	TAP-20KEPS-SS-4Y-P	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - Platinum	TAP-25KEPS-SS-4Y-P	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - Platinum	TAP-30KEPS-SS-4Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - Platinum	TAP-35KEPS-SS-4Y-P	$ 6,663,524.00	$ 5,797,265.88
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - Platinum	TAP-40KEPS-SS-4Y-P	$ 7,615,456.00	$ 6,625,446.72
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - Platinum	TAP-45KEPS-SS-4Y-P	$ 8,567,388.00	$ 7,453,627.56
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - Platinum	TAP-50KEPS-SS-4Y-P	$ 9,519,320.00	$ 8,281,808.40
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - Platinum	TAP-55KEPS-SS-4Y-P	##############	$ 9,109,989.24
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - Platinum	TAP-60KEPS-SS-4Y-P	##############	$ 9,938,170.08
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - Platinum	TAP-65KEPS-SS-4Y-P	##############	##############
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - Platinum	TAP-70KEPS-SS-4Y-P	##############	##############
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - Platinum	TAP-75KEPS-SS-4Y-P	##############	##############
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - Platinum	TAP-80KEPS-SS-4Y-P	##############	##############
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - Platinum	TAP-1KEPS-SS-5Y-P	$ 1,163,175.00	$ 1,011,962.25
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-SS-5Y-P	$ 1,381,290.00	$ 1,201,722.30
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - Platinum	TAP-5KEPS-SS-5Y-P	$ 1,573,065.00	$ 1,368,566.55
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - Platinum	TAP-10KEPS-SS-5Y-P	$ 2,379,830.00	$ 2,070,452.10
FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - Platinum	TAP-15KEPS-SS-5Y-P	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - Platinum	TAP-20KEPS-SS-5Y-P	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - Platinum	TAP-25KEPS-SS-5Y-P	$ 5,949,575.00	$ 5,176,130.25
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - Platinum	TAP-30KEPS-SS-5Y-P	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - Platinum	TAP-35KEPS-SS-5Y-P	$ 8,329,405.00	$ 7,246,582.35
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - Platinum	TAP-40KEPS-SS-5Y-P	$ 9,519,320.00	$ 8,281,808.40
FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - Platinum	TAP-45KEPS-SS-5Y-P	##############	$ 9,317,034.45
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - Platinum	TAP-50KEPS-SS-5Y-P	##############	##############
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - Platinum	TAP-55KEPS-SS-5Y-P	##############	##############
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - Platinum	TAP-60KEPS-SS-5Y-P	##############	##############
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - Platinum	TAP-65KEPS-SS-5Y-P	##############	##############
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - Platinum	TAP-70KEPS-SS-5Y-P	##############	##############
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - Platinum	TAP-75KEPS-SS-5Y-P	##############	##############
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - Platinum	TAP-80KEPS-SS-5Y-P	##############	##############
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 1YR - Platinum	RN-TAP-1KEPS-SS-1Y-P	$ 232,635.00	$ 202,392.45
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 1YR - Platinum	RN-TAP-2.5KEPS-SS-1Y-P	$ 276,258.00	$ 240,344.46
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 1YR - Platinum	RN-TAP-5KEPS-SS-1Y-P	$ 314,613.00	$ 273,713.31
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 1YR - Platinum	RN-TAP-10KEPS-SS-1Y-P	$ 475,966.00	$ 414,090.42
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 1YR - Platinum	RN-TAP-15KEPS-SS-1Y-P	$ 713,949.00	$ 621,135.63
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 1YR - Platinum	RN-TAP-20KEPS-SS-1Y-P	$ 951,932.00	$ 828,180.84
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 1YR - Platinum	RN-TAP-25KEPS-SS-1Y-P	$ 1,189,915.00	$ 1,035,226.05
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 1YR - Platinum	RN-TAP-30KEPS-SS-1Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 1YR - Platinum	RN-TAP-35KEPS-SS-1Y-P	$ 1,665,881.00	$ 1,449,316.47
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 1YR - Platinum	RN-TAP-40KEPS-SS-1Y-P	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 1YR - Platinum	RN-TAP-45KEPS-SS-1Y-P	$ 2,141,847.00	$ 1,863,406.89
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 1YR - Platinum	RN-TAP-50KEPS-SS-1Y-P	$ 2,379,830.00	$ 2,070,452.10
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 1YR - Platinum	RN-TAP-55KEPS-SS-1Y-P	$ 2,617,813.00	$ 2,277,497.31
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 1YR - Platinum	RN-TAP-60KEPS-SS-1Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 1YR - Platinum	RN-TAP-65KEPS-SS-1Y-P	$ 3,093,779.00	$ 2,691,587.73
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 1YR - Platinum	RN-TAP-70KEPS-SS-1Y-P	$ 3,331,762.00	$ 2,898,632.94
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 1YR - Platinum	RN-TAP-75KEPS-SS-1Y-P	$ 3,569,745.00	$ 3,105,678.15
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 1YR - Platinum	RN-TAP-80KEPS-SS-1Y-P	$ 3,807,728.00	$ 3,312,723.36

FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 2YR - Platinum	RN-TAP-1KEPS-SS-2Y-P	$ 465,270.00	$ 404,784.90
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 2YR - Platinum	RN-TAP-2.5KEPS-SS-2Y-P	$ 552,516.00	$ 480,688.92
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 2YR - Platinum	RN-TAP-5KEPS-SS-2Y-P	$ 629,226.00	$ 547,426.62
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 2YR - Platinum	RN-TAP-10KEPS-SS-2Y-P	$ 951,932.00	$ 828,180.84
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 2YR - Platinum	RN-TAP-15KEPS-SS-2Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 2YR - Platinum	RN-TAP-20KEPS-SS-2Y-P	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 2YR - Platinum	RN-TAP-25KEPS-SS-2Y-P	$ 2,379,830.00	$ 2,070,452.10
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 2YR - Platinum	RN-TAP-30KEPS-SS-2Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 2YR - Platinum	RN-TAP-35KEPS-SS-2Y-P	$ 3,331,762.00	$ 2,898,632.94
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 2YR - Platinum	RN-TAP-40KEPS-SS-2Y-P	$ 3,807,728.00	$ 3,312,723.36
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 2YR - Platinum	RN-TAP-45KEPS-SS-2Y-P	$ 4,283,694.00	$ 3,726,813.78
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 2YR - Platinum	RN-TAP-50KEPS-SS-2Y-P	$ 4,759,660.00	$ 4,140,904.20
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 2YR - Platinum	RN-TAP-55KEPS-SS-2Y-P	$ 5,235,626.00	$ 4,554,994.62
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 2YR - Platinum	RN-TAP-60KEPS-SS-2Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 2YR - Platinum	RN-TAP-65KEPS-SS-2Y-P	$ 6,187,558.00	$ 5,383,175.46
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 2YR - Platinum	RN-TAP-70KEPS-SS-2Y-P	$ 6,663,524.00	$ 5,797,265.88
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 2YR - Platinum	RN-TAP-75KEPS-SS-2Y-P	$ 7,139,490.00	$ 6,211,356.30
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 2YR - Platinum	RN-TAP-80KEPS-SS-2Y-P	$ 7,615,456.00	$ 6,625,446.72
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 3YR - Platinum	RN-TAP-1KEPS-SS-3Y-P	$ 697,905.00	$ 607,177.35
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 3YR - Platinum	RN-TAP-2.5KEPS-SS-3Y-P	$ 828,774.00	$ 721,033.38
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 3YR - Platinum	RN-TAP-5KEPS-SS-3Y-P	$ 943,839.00	$ 821,139.93
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 3YR - Platinum	RN-TAP-10KEPS-SS-3Y-P	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 3YR - Platinum	RN-TAP-15KEPS-SS-3Y-P	$ 2,141,847.00	$ 1,863,406.89
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 3YR - Platinum	RN-TAP-20KEPS-SS-3Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 3YR - Platinum	RN-TAP-25KEPS-SS-3Y-P	$ 3,569,745.00	$ 3,105,678.15
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 3YR - Platinum	RN-TAP-30KEPS-SS-3Y-P	$ 4,283,694.00	$ 3,726,813.78
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 3YR - Platinum	RN-TAP-35KEPS-SS-3Y-P	$ 4,997,643.00	$ 4,347,949.41
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 3YR - Platinum	RN-TAP-40KEPS-SS-3Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 3YR - Platinum	RN-TAP-45KEPS-SS-3Y-P	$ 6,425,541.00	$ 5,590,220.67
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 3YR - Platinum	RN-TAP-50KEPS-SS-3Y-P	$ 7,139,490.00	$ 6,211,356.30
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 3YR - Platinum	RN-TAP-55KEPS-SS-3Y-P	$ 7,853,439.00	$ 6,832,491.93
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 3YR - Platinum	RN-TAP-60KEPS-SS-3Y-P	$ 8,567,388.00	$ 7,453,627.56
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 3YR - Platinum	RN-TAP-65KEPS-SS-3Y-P	$ 9,281,337.00	$ 8,074,763.19
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 3YR - Platinum	RN-TAP-70KEPS-SS-3Y-P	$ 9,995,286.00	$ 8,695,898.82
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 3YR - Platinum	RN-TAP-75KEPS-SS-3Y-P	##############	$ 9,317,034.45
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 3YR - Platinum	RN-TAP-80KEPS-SS-3Y-P	##############	$ 9,938,170.08
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 4YR - Platinum	RN-TAP-1KEPS-SS-4Y-P	$ 930,540.00	$ 809,569.80
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 4YR - Platinum	RN-TAP-2.5KEPS-SS-4Y-P	$ 1,105,032.00	$ 961,377.84
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 4YR - Platinum	RN-TAP-5KEPS-SS-4Y-P	$ 1,258,452.00	$ 1,094,853.24
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 4YR - Platinum	RN-TAP-10KEPS-SS-4Y-P	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 4YR - Platinum	RN-TAP-15KEPS-SS-4Y-P	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 4YR - Platinum	RN-TAP-20KEPS-SS-4Y-P	$ 3,807,728.00	$ 3,312,723.36
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 4YR - Platinum	RN-TAP-25KEPS-SS-4Y-P	$ 4,759,660.00	$ 4,140,904.20
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 4YR - Platinum	RN-TAP-30KEPS-SS-4Y-P	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 4YR - Platinum	RN-TAP-35KEPS-SS-4Y-P	$ 6,663,524.00	$ 5,797,265.88
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 4YR - Platinum	RN-TAP-40KEPS-SS-4Y-P	$ 7,615,456.00	$ 6,625,446.72
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 4YR - Platinum	RN-TAP-45KEPS-SS-4Y-P	$ 8,567,388.00	$ 7,453,627.56
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 4YR - Platinum	RN-TAP-50KEPS-SS-4Y-P	$ 9,519,320.00	$ 8,281,808.40
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 4YR - Platinum	RN-TAP-55KEPS-SS-4Y-P	##############	$ 9,109,989.24

FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 4YR - Platinum	RN-TAP-60KEPS-SS-4Y-P	##########	$ 9,938,170.08
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 4YR - Platinum	RN-TAP-65KEPS-SS-4Y-P	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 4YR - Platinum	RN-TAP-70KEPS-SS-4Y-P	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 4YR - Platinum	RN-TAP-75KEPS-SS-4Y-P	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 4YR - Platinum	RN-TAP-80KEPS-SS-4Y-P	##########	##########
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-SS-1Y-PPP	$ 244,267.00	$ 212,512.29
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-SS-1Y-PPP	$ 290,071.00	$ 252,361.77
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-SS-1Y-PPP	$ 330,344.00	$ 287,399.28
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-SS-1Y-PPP	$ 499,764.00	$ 434,794.68
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-SS-1Y-PPP	$ 749,646.00	$ 652,192.02
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-SS-1Y-PPP	$ 999,529.00	$ 869,590.23
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-SS-1Y-PPP	$ 1,249,411.00	$ 1,086,987.57
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-SS-1Y-PPP	$ 1,499,293.00	$ 1,304,384.91
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-SS-1Y-PPP	$ 1,749,175.00	$ 1,521,782.25
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-SS-1Y-PPP	$ 1,999,057.00	$ 1,739,179.59
FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - Plat Prio Plus	TAP-45KEPS-SS-1Y-PPP	$ 2,248,939.00	$ 1,956,576.93
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - Plat Prio Plus	TAP-50KEPS-SS-1Y-PPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - Plat Prio Plus	TAP-55KEPS-SS-1Y-PPP	$ 2,748,704.00	$ 2,391,372.48
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - Plat Prio Plus	TAP-60KEPS-SS-1Y-PPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - Plat Prio Plus	TAP-65KEPS-SS-1Y-PPP	$ 3,248,468.00	$ 2,826,167.16
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - Plat Prio Plus	TAP-70KEPS-SS-1Y-PPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - Plat Prio Plus	TAP-75KEPS-SS-1Y-PPP	$ 3,748,232.00	$ 3,260,961.84
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - Plat Prio Plus	TAP-80KEPS-SS-1Y-PPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-SS-2Y-PPP	$ 488,534.00	$ 425,024.58
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-SS-2Y-PPP	$ 580,142.00	$ 504,723.54
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-SS-2Y-PPP	$ 660,688.00	$ 574,798.56
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-SS-2Y-PPP	$ 999,528.00	$ 869,589.36
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-SS-2Y-PPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-SS-2Y-PPP	$ 1,999,058.00	$ 1,739,180.46
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-SS-2Y-PPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-SS-2Y-PPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-SS-2Y-PPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-SS-2Y-PPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - Plat Prio Plus	TAP-45KEPS-SS-2Y-PPP	$ 4,497,878.00	$ 3,913,153.86
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - Plat Prio Plus	TAP-50KEPS-SS-2Y-PPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - Plat Prio Plus	TAP-55KEPS-SS-2Y-PPP	$ 5,497,408.00	$ 4,782,744.96
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - Plat Prio Plus	TAP-60KEPS-SS-2Y-PPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - Plat Prio Plus	TAP-65KEPS-SS-2Y-PPP	$ 6,496,936.00	$ 5,652,334.32
FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - Plat Prio Plus	TAP-70KEPS-SS-2Y-PPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - Plat Prio Plus	TAP-75KEPS-SS-2Y-PPP	$ 7,496,464.00	$ 6,521,923.68
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - Plat Prio Plus	TAP-80KEPS-SS-2Y-PPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-SS-3Y-PPP	$ 732,801.00	$ 637,536.87
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-SS-3Y-PPP	$ 870,213.00	$ 757,085.31
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-SS-3Y-PPP	$ 991,032.00	$ 862,197.84
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-SS-3Y-PPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-SS-3Y-PPP	$ 2,248,938.00	$ 1,956,576.06
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-SS-3Y-PPP	$ 2,998,587.00	$ 2,608,770.69
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-SS-3Y-PPP	$ 3,748,233.00	$ 3,260,962.71
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-SS-3Y-PPP	$ 4,497,879.00	$ 3,913,154.73

FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-SS-3Y-PPP	$ 5,247,525.00	$ 4,565,346.75
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-SS-3Y-PPP	$ 5,997,171.00	$ 5,217,538.77
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - Plat Prio Plus	TAP-45KEPS-SS-3Y-PPP	$ 6,746,817.00	$ 5,869,730.79
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - Plat Prio Plus	TAP-50KEPS-SS-3Y-PPP	$ 7,496,466.00	$ 6,521,925.42
FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - Plat Prio Plus	TAP-55KEPS-SS-3Y-PPP	$ 8,246,112.00	$ 7,174,117.44
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - Plat Prio Plus	TAP-60KEPS-SS-3Y-PPP	$ 8,995,758.00	$ 7,826,309.46
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - Plat Prio Plus	TAP-65KEPS-SS-3Y-PPP	$ 9,745,404.00	$ 8,478,501.48
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - Plat Prio Plus	TAP-70KEPS-SS-3Y-PPP	##############	$ 9,130,693.50
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - Plat Prio Plus	TAP-75KEPS-SS-3Y-PPP	##############	$ 9,782,885.52
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - Plat Prio Plus	TAP-80KEPS-SS-3Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-SS-4Y-PPP	$ 977,068.00	$ 850,049.16
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-SS-4Y-PPP	$ 1,160,284.00	$ 1,009,447.08
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-SS-4Y-PPP	$ 1,321,376.00	$ 1,149,597.12
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-SS-4Y-PPP	$ 1,999,056.00	$ 1,739,178.72
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-SS-4Y-PPP	$ 2,998,584.00	$ 2,608,768.08
FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-SS-4Y-PPP	$ 3,998,116.00	$ 3,478,360.92
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-SS-4Y-PPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-SS-4Y-PPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-SS-4Y-PPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-SS-4Y-PPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - Plat Prio Plus	TAP-45KEPS-SS-4Y-PPP	$ 8,995,756.00	$ 7,826,307.72
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - Plat Prio Plus	TAP-50KEPS-SS-4Y-PPP	$ 9,995,288.00	$ 8,695,900.56
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - Plat Prio Plus	TAP-55KEPS-SS-4Y-PPP	##############	$ 9,565,489.92
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - Plat Prio Plus	TAP-60KEPS-SS-4Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - Plat Prio Plus	TAP-65KEPS-SS-4Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - Plat Prio Plus	TAP-70KEPS-SS-4Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - Plat Prio Plus	TAP-75KEPS-SS-4Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - Plat Prio Plus	TAP-80KEPS-SS-4Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-SS-5Y-PPP	$ 1,221,335.00	$ 1,062,561.45
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-SS-5Y-PPP	$ 1,450,355.00	$ 1,261,808.85
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-SS-5Y-PPP	$ 1,651,720.00	$ 1,436,996.40
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-SS-5Y-PPP	$ 2,498,820.00	$ 2,173,973.40
FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-SS-5Y-PPP	$ 3,748,230.00	$ 3,260,960.10
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-SS-5Y-PPP	$ 4,997,645.00	$ 4,347,951.15
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-SS-5Y-PPP	$ 6,247,055.00	$ 5,434,937.85
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-SS-5Y-PPP	$ 7,496,465.00	$ 6,521,924.55
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-SS-5Y-PPP	$ 8,745,875.00	$ 7,608,911.25
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-SS-5Y-PPP	$ 9,995,285.00	$ 8,695,897.95
FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - Plat Prio Plus	TAP-45KEPS-SS-5Y-PPP	##############	$ 9,782,884.65
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - Plat Prio Plus	TAP-50KEPS-SS-5Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - Plat Prio Plus	TAP-55KEPS-SS-5Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - Plat Prio Plus	TAP-60KEPS-SS-5Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - Plat Prio Plus	TAP-65KEPS-SS-5Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - Plat Prio Plus	TAP-70KEPS-SS-5Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - Plat Prio Plus	TAP-75KEPS-SS-5Y-PPP	##############	##############
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - Plat Prio Plus	TAP-80KEPS-SS-5Y-PPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 1YR - Plat Prio Plus	RN-TAP-1KEPS-SS-1Y-PPP	$ 244,267.00	$ 212,512.29
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 1YR - Plat Prio Plus	RN-TAP-2.5KEPS-SS-1Y-PPP	$ 290,071.00	$ 252,361.77
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 1YR - Plat Prio Plus	RN-TAP-5KEPS-SS-1Y-PPP	$ 330,344.00	$ 287,399.28

FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 1YR - Plat Prio Plus	RN-TAP-10KEPS-SS-1Y-PPP	$ 499,764.00	$ 434,794.68
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 1YR - Plat Prio Plus	RN-TAP-15KEPS-SS-1Y-PPP	$ 749,646.00	$ 652,192.02
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 1YR - Plat Prio Plus	RN-TAP-20KEPS-SS-1Y-PPP	$ 999,529.00	$ 869,590.23
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 1YR - Plat Prio Plus	RN-TAP-25KEPS-SS-1Y-PPP	$ 1,249,411.00	$ 1,086,987.57
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 1YR - Plat Prio Plus	RN-TAP-30KEPS-SS-1Y-PPP	$ 1,499,293.00	$ 1,304,384.91
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 1YR - Plat Prio Plus	RN-TAP-35KEPS-SS-1Y-PPP	$ 1,749,175.00	$ 1,521,782.25
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 1YR - Plat Prio Plus	RN-TAP-40KEPS-SS-1Y-PPP	$ 1,999,057.00	$ 1,739,179.59
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 1YR - Plat Prio Plus	RN-TAP-45KEPS-SS-1Y-PPP	$ 2,248,939.00	$ 1,956,576.93
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 1YR - Plat Prio Plus	RN-TAP-50KEPS-SS-1Y-PPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 1YR - Plat Prio Plus	RN-TAP-55KEPS-SS-1Y-PPP	$ 2,748,704.00	$ 2,391,372.48
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 1YR - Plat Prio Plus	RN-TAP-60KEPS-SS-1Y-PPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 1YR - Plat Prio Plus	RN-TAP-65KEPS-SS-1Y-PPP	$ 3,248,468.00	$ 2,826,167.16
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 1YR - Plat Prio Plus	RN-TAP-70KEPS-SS-1Y-PPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 1YR - Plat Prio Plus	RN-TAP-75KEPS-SS-1Y-PPP	$ 3,748,232.00	$ 3,260,961.84
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 1YR - Plat Prio Plus	RN-TAP-80KEPS-SS-1Y-PPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 2YR - Plat Prio Plus	RN-TAP-1KEPS-SS-2Y-PPP	$ 488,534.00	$ 425,024.58
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 2YR - Plat Prio Plus	RN-TAP-2.5KEPS-SS-2Y-PPP	$ 580,142.00	$ 504,723.54
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 2YR - Plat Prio Plus	RN-TAP-5KEPS-SS-2Y-PPP	$ 660,688.00	$ 574,798.56
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 2YR - Plat Prio Plus	RN-TAP-10KEPS-SS-2Y-PPP	$ 999,528.00	$ 869,589.36
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 2YR - Plat Prio Plus	RN-TAP-15KEPS-SS-2Y-PPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 2YR - Plat Prio Plus	RN-TAP-20KEPS-SS-2Y-PPP	$ 1,999,058.00	$ 1,739,180.46
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 2YR - Plat Prio Plus	RN-TAP-25KEPS-SS-2Y-PPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 2YR - Plat Prio Plus	RN-TAP-30KEPS-SS-2Y-PPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 2YR - Plat Prio Plus	RN-TAP-35KEPS-SS-2Y-PPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 2YR - Plat Prio Plus	RN-TAP-40KEPS-SS-2Y-PPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 2YR - Plat Prio Plus	RN-TAP-45KEPS-SS-2Y-PPP	$ 4,497,878.00	$ 3,913,153.86
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 2YR - Plat Prio Plus	RN-TAP-50KEPS-SS-2Y-PPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 2YR - Plat Prio Plus	RN-TAP-55KEPS-SS-2Y-PPP	$ 5,497,408.00	$ 4,782,744.96
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 2YR - Plat Prio Plus	RN-TAP-60KEPS-SS-2Y-PPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 2YR - Plat Prio Plus	RN-TAP-65KEPS-SS-2Y-PPP	$ 6,496,936.00	$ 5,652,334.32
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 2YR - Plat Prio Plus	RN-TAP-70KEPS-SS-2Y-PPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 2YR - Plat Prio Plus	RN-TAP-75KEPS-SS-2Y-PPP	$ 7,496,464.00	$ 6,521,923.68
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 2YR - Plat Prio Plus	RN-TAP-80KEPS-SS-2Y-PPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 3YR - Plat Prio Plus	RN-TAP-1KEPS-SS-3Y-PPP	$ 732,801.00	$ 637,536.87
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 3YR - Plat Prio Plus	RN-TAP-2.5KEPS-SS-3Y-PPP	$ 870,213.00	$ 757,085.31
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 3YR - Plat Prio Plus	RN-TAP-5KEPS-SS-3Y-PPP	$ 991,032.00	$ 862,197.84
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 3YR - Plat Prio Plus	RN-TAP-10KEPS-SS-3Y-PPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 3YR - Plat Prio Plus	RN-TAP-15KEPS-SS-3Y-PPP	$ 2,248,938.00	$ 1,956,576.06
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 3YR - Plat Prio Plus	RN-TAP-20KEPS-SS-3Y-PPP	$ 2,998,587.00	$ 2,608,770.69
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 3YR - Plat Prio Plus	RN-TAP-25KEPS-SS-3Y-PPP	$ 3,748,233.00	$ 3,260,962.71
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 3YR - Plat Prio Plus	RN-TAP-30KEPS-SS-3Y-PPP	$ 4,497,879.00	$ 3,913,154.73
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 3YR - Plat Prio Plus	RN-TAP-35KEPS-SS-3Y-PPP	$ 5,247,525.00	$ 4,565,346.75
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 3YR - Plat Prio Plus	RN-TAP-40KEPS-SS-3Y-PPP	$ 5,997,171.00	$ 5,217,538.77
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 3YR - Plat Prio Plus	RN-TAP-45KEPS-SS-3Y-PPP	$ 6,746,817.00	$ 5,869,730.79
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 3YR - Plat Prio Plus	RN-TAP-50KEPS-SS-3Y-PPP	$ 7,496,466.00	$ 6,521,925.42
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 3YR - Plat Prio Plus	RN-TAP-55KEPS-SS-3Y-PPP	$ 8,246,112.00	$ 7,174,117.44
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 3YR - Plat Prio Plus	RN-TAP-60KEPS-SS-3Y-PPP	$ 8,995,758.00	$ 7,826,309.46
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 3YR - Plat Prio Plus	RN-TAP-65KEPS-SS-3Y-PPP	$ 9,745,404.00	$ 8,478,501.48
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 3YR - Plat Prio Plus	RN-TAP-70KEPS-SS-3Y-PPP	##############	$ 9,130,693.50

FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 3YR - Plat Prio Plus	RN-TAP-75KEPS-SS-3Y-PPP	############	$ 9,782,885.52
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 3YR - Plat Prio Plus	RN-TAP-80KEPS-SS-3Y-PPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 4YR - Plat Prio Plus	RN-TAP-1KEPS-SS-4Y-PPP	$ 977,068.00	$ 850,049.16
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 4YR - Plat Prio Plus	RN-TAP-2.5KEPS-SS-4Y-PPP	$ 1,160,284.00	$ 1,009,447.08
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 4YR - Plat Prio Plus	RN-TAP-5KEPS-SS-4Y-PPP	$ 1,321,376.00	$ 1,149,597.12
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 4YR - Plat Prio Plus	RN-TAP-10KEPS-SS-4Y-PPP	$ 1,999,056.00	$ 1,739,178.72
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 4YR - Plat Prio Plus	RN-TAP-15KEPS-SS-4Y-PPP	$ 2,998,584.00	$ 2,608,768.08
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 4YR - Plat Prio Plus	RN-TAP-20KEPS-SS-4Y-PPP	$ 3,998,116.00	$ 3,478,360.92
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 4YR - Plat Prio Plus	RN-TAP-25KEPS-SS-4Y-PPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 4YR - Plat Prio Plus	RN-TAP-30KEPS-SS-4Y-PPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 4YR - Plat Prio Plus	RN-TAP-35KEPS-SS-4Y-PPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 4YR - Plat Prio Plus	RN-TAP-40KEPS-SS-4Y-PPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 4YR - Plat Prio Plus	RN-TAP-45KEPS-SS-4Y-PPP	$ 8,995,756.00	$ 7,826,307.72
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 4YR - Plat Prio Plus	RN-TAP-50KEPS-SS-4Y-PPP	$ 9,995,288.00	$ 8,695,900.56
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 4YR - Plat Prio Plus	RN-TAP-55KEPS-SS-4Y-PPP	############	$ 9,565,489.92
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 4YR - Plat Prio Plus	RN-TAP-60KEPS-SS-4Y-PPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 4YR - Plat Prio Plus	RN-TAP-65KEPS-SS-4Y-PPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 4YR - Plat Prio Plus	RN-TAP-70KEPS-SS-4Y-PPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 4YR - Plat Prio Plus	RN-TAP-75KEPS-SS-4Y-PPP	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 4YR - Plat Prio Plus	RN-TAP-80KEPS-SS-4Y-PPP	############	############
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - Platinum	TAP-1KEPS-LS-1Y-P	$ 492,411.00	$ 428,397.57
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-LS-1Y-P	$ 600,978.00	$ 522,850.86
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - Platinum	TAP-5KEPS-LS-1Y-P	$ 704,277.00	$ 612,720.99
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - Platinum	TAP-10KEPS-LS-1Y-P	$ 1,125,406.00	$ 979,103.22
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - Platinum	TAP-15KEPS-LS-1Y-P	$ 1,688,109.00	$ 1,468,654.83
FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - Platinum	TAP-20KEPS-LS-1Y-P	$ 2,250,812.00	$ 1,958,206.44
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - Platinum	TAP-25KEPS-LS-1Y-P	$ 2,813,515.00	$ 2,447,758.05
FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - Platinum	TAP-30KEPS-LS-1Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - Platinum	TAP-35KEPS-LS-1Y-P	$ 3,938,921.00	$ 3,426,861.27
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - Platinum	TAP-40KEPS-LS-1Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - Platinum	TAP-1KEPS-LS-2Y-P	$ 984,822.00	$ 856,795.14
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-LS-2Y-P	$ 1,201,956.00	$ 1,045,701.72
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - Platinum	TAP-5KEPS-LS-2Y-P	$ 1,408,554.00	$ 1,225,441.98
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - Platinum	TAP-10KEPS-LS-2Y-P	$ 2,250,812.00	$ 1,958,206.44
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - Platinum	TAP-15KEPS-LS-2Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - Platinum	TAP-20KEPS-LS-2Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - Platinum	TAP-25KEPS-LS-2Y-P	$ 5,627,030.00	$ 4,895,516.10
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - Platinum	TAP-30KEPS-LS-2Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - Platinum	TAP-35KEPS-LS-2Y-P	$ 7,877,842.00	$ 6,853,722.54
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - Platinum	TAP-40KEPS-LS-2Y-P	$ 9,003,248.00	$ 7,832,825.76
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - Platinum	TAP-1KEPS-LS-3Y-P	$ 1,477,233.00	$ 1,285,192.71
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-LS-3Y-P	$ 1,802,934.00	$ 1,568,552.58
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - Platinum	TAP-5KEPS-LS-3Y-P	$ 2,112,831.00	$ 1,838,162.97
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - Platinum	TAP-10KEPS-LS-3Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - Platinum	TAP-15KEPS-LS-3Y-P	$ 5,064,327.00	$ 4,405,964.49
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - Platinum	TAP-20KEPS-LS-3Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - Platinum	TAP-25KEPS-LS-3Y-P	$ 8,440,545.00	$ 7,343,274.15
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - Platinum	TAP-30KEPS-LS-3Y-P	############	$ 8,811,928.98
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - Platinum	TAP-35KEPS-LS-3Y-P	############	############

FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - Platinum	TAP-40KEPS-LS-3Y-P	############	############
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - Platinum	TAP-1KEPS-LS-4Y-P	$ 1,969,644.00	$ 1,713,590.28
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-LS-4Y-P	$ 2,403,912.00	$ 2,091,403.44
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - Platinum	TAP-5KEPS-LS-4Y-P	$ 2,817,108.00	$ 2,450,883.96
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - Platinum	TAP-10KEPS-LS-4Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - Platinum	TAP-15KEPS-LS-4Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - Platinum	TAP-20KEPS-LS-4Y-P	$ 9,003,248.00	$ 7,832,825.76
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - Platinum	TAP-25KEPS-LS-4Y-P	############	$ 9,791,032.20
FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - Platinum	TAP-30KEPS-LS-4Y-P	############	############
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - Platinum	TAP-35KEPS-LS-4Y-P	############	############
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - Platinum	TAP-40KEPS-LS-4Y-P	############	############
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - Platinum	TAP-1KEPS-LS-5Y-P	$ 2,462,055.00	$ 2,141,987.85
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-LS-5Y-P	$ 3,004,890.00	$ 2,614,254.30
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - Platinum	TAP-5KEPS-LS-5Y-P	$ 3,521,385.00	$ 3,063,604.95
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - Platinum	TAP-10KEPS-LS-5Y-P	$ 5,627,030.00	$ 4,895,516.10
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - Platinum	TAP-15KEPS-LS-5Y-P	$ 8,440,545.00	$ 7,343,274.15
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - Platinum	TAP-20KEPS-LS-5Y-P	############	$ 9,791,032.20
FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - Platinum	TAP-25KEPS-LS-5Y-P	############	############
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - Platinum	TAP-30KEPS-LS-5Y-P	############	############
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - Platinum	TAP-35KEPS-LS-5Y-P	############	############
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - Platinum	TAP-40KEPS-LS-5Y-P	############	############
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 1YR - Platinum	RN-TAP-1KEPS-LS-1Y-P	$ 492,411.00	$ 428,397.57
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 1YR - Platinum	RN-TAP-2.5KEPS-LS-1Y-P	$ 600,978.00	$ 522,850.86
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 1YR - Platinum	RN-TAP-5KEPS-LS-1Y-P	$ 704,277.00	$ 612,720.99
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 1YR - Platinum	RN-TAP-10KEPS-LS-1Y-P	$ 1,125,406.00	$ 979,103.22
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 1YR - Platinum	RN-TAP-15KEPS-LS-1Y-P	$ 1,688,109.00	$ 1,468,654.83
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 1YR - Platinum	RN-TAP-20KEPS-LS-1Y-P	$ 2,250,812.00	$ 1,958,206.44
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 1YR - Platinum	RN-TAP-25KEPS-LS-1Y-P	$ 2,813,515.00	$ 2,447,758.05
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 1YR - Platinum	RN-TAP-30KEPS-LS-1Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 1YR - Platinum	RN-TAP-35KEPS-LS-1Y-P	$ 3,938,921.00	$ 3,426,861.27
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 1YR - Platinum	RN-TAP-40KEPS-LS-1Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 2YR - Platinum	RN-TAP-1KEPS-LS-2Y-P	$ 984,822.00	$ 856,795.14
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 2YR - Platinum	RN-TAP-2.5KEPS-LS-2Y-P	$ 1,201,956.00	$ 1,045,701.72
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 2YR - Platinum	RN-TAP-5KEPS-LS-2Y-P	$ 1,408,554.00	$ 1,225,441.98
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 2YR - Platinum	RN-TAP-10KEPS-LS-2Y-P	$ 2,250,812.00	$ 1,958,206.44
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 2YR - Platinum	RN-TAP-15KEPS-LS-2Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 2YR - Platinum	RN-TAP-20KEPS-LS-2Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 2YR - Platinum	RN-TAP-25KEPS-LS-2Y-P	$ 5,627,030.00	$ 4,895,516.10
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 2YR - Platinum	RN-TAP-30KEPS-LS-2Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 2YR - Platinum	RN-TAP-35KEPS-LS-2Y-P	$ 7,877,842.00	$ 6,853,722.54
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 2YR - Platinum	RN-TAP-40KEPS-LS-2Y-P	$ 9,003,248.00	$ 7,832,825.76
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 3YR - Platinum	RN-TAP-1KEPS-LS-3Y-P	$ 1,477,233.00	$ 1,285,192.71
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 3YR - Platinum	RN-TAP-2.5KEPS-LS-3Y-P	$ 1,802,934.00	$ 1,568,552.58
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 3YR - Platinum	RN-TAP-5KEPS-LS-3Y-P	$ 2,112,831.00	$ 1,838,162.97
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 3YR - Platinum	RN-TAP-10KEPS-LS-3Y-P	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 3YR - Platinum	RN-TAP-15KEPS-LS-3Y-P	$ 5,064,327.00	$ 4,405,964.49
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 3YR - Platinum	RN-TAP-20KEPS-LS-3Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 3YR - Platinum	RN-TAP-25KEPS-LS-3Y-P	$ 8,440,545.00	$ 7,343,274.15
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 3YR - Platinum	RN-TAP-30KEPS-LS-3Y-P	############	$ 8,811,928.98

FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 3YR - Platinum	RN-TAP-35KEPS-LS-3Y-P	############	############
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 3YR - Platinum	RN-TAP-40KEPS-LS-3Y-P	############	############
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 4YR - Platinum	RN-TAP-1KEPS-LS-4Y-P	$ 1,969,644.00	$ 1,713,590.28
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 4YR - Platinum	RN-TAP-2.5KEPS-LS-4Y-P	$ 2,403,912.00	$ 2,091,403.44
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 4YR - Platinum	RN-TAP-5KEPS-LS-4Y-P	$ 2,817,108.00	$ 2,450,883.96
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 4YR - Platinum	RN-TAP-10KEPS-LS-4Y-P	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 4YR - Platinum	RN-TAP-15KEPS-LS-4Y-P	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 4YR - Platinum	RN-TAP-20KEPS-LS-4Y-P	$ 9,003,248.00	$ 7,832,825.76
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 4YR - Platinum	RN-TAP-25KEPS-LS-4Y-P	############	$ 9,791,032.20
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 4YR - Platinum	RN-TAP-30KEPS-LS-4Y-P	############	############
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 4YR - Platinum	RN-TAP-35KEPS-LS-4Y-P	############	############
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 4YR - Platinum	RN-TAP-40KEPS-LS-4Y-P	############	############
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-LS-1Y-PPP	$ 517,032.00	$ 449,817.84
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-LS-1Y-PPP	$ 631,027.00	$ 548,993.49
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-LS-1Y-PPP	$ 739,491.00	$ 643,357.17
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-LS-1Y-PPP	$ 1,181,676.00	$ 1,028,058.12
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-LS-1Y-PPP	$ 1,772,514.00	$ 1,542,087.18
FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-LS-1Y-PPP	$ 2,363,353.00	$ 2,056,117.11
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-LS-1Y-PPP	$ 2,954,191.00	$ 2,570,146.17
FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-LS-1Y-PPP	$ 3,545,029.00	$ 3,084,175.23
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-LS-1Y-PPP	$ 4,135,867.00	$ 3,598,204.29
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-LS-1Y-PPP	$ 4,726,705.00	$ 4,112,233.35
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-LS-2Y-PPP	$ 1,034,064.00	$ 899,635.68
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-LS-2Y-PPP	$ 1,262,054.00	$ 1,097,986.98
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-LS-2Y-PPP	$ 1,478,982.00	$ 1,286,714.34
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-LS-2Y-PPP	$ 2,363,352.00	$ 2,056,116.24
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-LS-2Y-PPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-LS-2Y-PPP	$ 4,726,706.00	$ 4,112,234.22
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-LS-2Y-PPP	$ 5,908,382.00	$ 5,140,292.34
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-LS-2Y-PPP	$ 7,090,058.00	$ 6,168,350.46
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-LS-2Y-PPP	$ 8,271,734.00	$ 7,196,408.58
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-LS-2Y-PPP	$ 9,453,410.00	$ 8,224,466.70
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-LS-3Y-PPP	$ 1,551,096.00	$ 1,349,453.52
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-LS-3Y-PPP	$ 1,893,081.00	$ 1,646,980.47
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-LS-3Y-PPP	$ 2,218,473.00	$ 1,930,071.51
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-LS-3Y-PPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-LS-3Y-PPP	$ 5,317,542.00	$ 4,626,261.54
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-LS-3Y-PPP	$ 7,090,059.00	$ 6,168,351.33
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-LS-3Y-PPP	$ 8,862,573.00	$ 7,710,438.51
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-LS-3Y-PPP	############	$ 9,252,525.69
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-LS-3Y-PPP	############	############
FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-LS-3Y-PPP	############	############
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-LS-4Y-PPP	$ 2,068,128.00	$ 1,799,271.36
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-LS-4Y-PPP	$ 2,524,108.00	$ 2,195,973.96
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-LS-4Y-PPP	$ 2,957,964.00	$ 2,573,428.68
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-LS-4Y-PPP	$ 4,726,704.00	$ 4,112,232.48
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-LS-4Y-PPP	$ 7,090,056.00	$ 6,168,348.72
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-LS-4Y-PPP	$ 9,453,412.00	$ 8,224,468.44
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-LS-4Y-PPP	############	############

FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-LS-4Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-LS-4Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-LS-4Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-LS-5Y-PPP	$ 2,585,160.00	$ 2,249,089.20
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-LS-5Y-PPP	$ 3,155,135.00	$ 2,744,967.45
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-LS-5Y-PPP	$ 3,697,455.00	$ 3,216,785.85
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-LS-5Y-PPP	$ 5,908,380.00	$ 5,140,290.60
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-LS-5Y-PPP	$ 8,862,570.00	$ 7,710,435.90
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-LS-5Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-LS-5Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-LS-5Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-LS-5Y-PPP	##########	##########
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-LS-5Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 1YR - Plat Prio Plus	RN-TAP-1KEPS-LS-1Y-PPP	$ 517,032.00	$ 449,817.84
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 1YR - Plat Prio Plus	RN-TAP-2.5KEPS-LS-1Y-PPP	$ 631,027.00	$ 548,993.49
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 1YR - Plat Prio Plus	RN-TAP-5KEPS-LS-1Y-PPP	$ 739,491.00	$ 643,357.17
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 1YR - Plat Prio Plus	RN-TAP-10KEPS-LS-1Y-PPP	$ 1,181,676.00	$ 1,028,058.12
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 1YR - Plat Prio Plus	RN-TAP-15KEPS-LS-1Y-PPP	$ 1,772,514.00	$ 1,542,087.18
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 1YR - Plat Prio Plus	RN-TAP-20KEPS-LS-1Y-PPP	$ 2,363,353.00	$ 2,056,117.11
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 1YR - Plat Prio Plus	RN-TAP-25KEPS-LS-1Y-PPP	$ 2,954,191.00	$ 2,570,146.17
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 1YR - Plat Prio Plus	RN-TAP-30KEPS-LS-1Y-PPP	$ 3,545,029.00	$ 3,084,175.23
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 1YR - Plat Prio Plus	RN-TAP-35KEPS-LS-1Y-PPP	$ 4,135,867.00	$ 3,598,204.29
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 1YR - Plat Prio Plus	RN-TAP-40KEPS-LS-1Y-PPP	$ 4,726,705.00	$ 4,112,233.35
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 2YR - Plat Prio Plus	RN-TAP-1KEPS-LS-2Y-PPP	$ 1,034,064.00	$ 899,635.68
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 2YR - Plat Prio Plus	RN-TAP-2.5KEPS-LS-2Y-PPP	$ 1,262,054.00	$ 1,097,986.98
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 2YR - Plat Prio Plus	RN-TAP-5KEPS-LS-2Y-PPP	$ 1,478,982.00	$ 1,286,714.34
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 2YR - Plat Prio Plus	RN-TAP-10KEPS-LS-2Y-PPP	$ 2,363,352.00	$ 2,056,116.24
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 2YR - Plat Prio Plus	RN-TAP-15KEPS-LS-2Y-PPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 2YR - Plat Prio Plus	RN-TAP-20KEPS-LS-2Y-PPP	$ 4,726,706.00	$ 4,112,234.22
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 2YR - Plat Prio Plus	RN-TAP-25KEPS-LS-2Y-PPP	$ 5,908,382.00	$ 5,140,292.34
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 2YR - Plat Prio Plus	RN-TAP-30KEPS-LS-2Y-PPP	$ 7,090,058.00	$ 6,168,350.46
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 2YR - Plat Prio Plus	RN-TAP-35KEPS-LS-2Y-PPP	$ 8,271,734.00	$ 7,196,408.58
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 2YR - Plat Prio Plus	RN-TAP-40KEPS-LS-2Y-PPP	$ 9,453,410.00	$ 8,224,466.70
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 3YR - Plat Prio Plus	RN-TAP-1KEPS-LS-3Y-PPP	$ 1,551,096.00	$ 1,349,453.52
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 3YR - Plat Prio Plus	RN-TAP-2.5KEPS-LS-3Y-PPP	$ 1,893,081.00	$ 1,646,980.47
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 3YR - Plat Prio Plus	RN-TAP-5KEPS-LS-3Y-PPP	$ 2,218,473.00	$ 1,930,071.51
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 3YR - Plat Prio Plus	RN-TAP-10KEPS-LS-3Y-PPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 3YR - Plat Prio Plus	RN-TAP-15KEPS-LS-3Y-PPP	$ 5,317,542.00	$ 4,626,261.54
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 3YR - Plat Prio Plus	RN-TAP-20KEPS-LS-3Y-PPP	$ 7,090,059.00	$ 6,168,351.33
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 3YR - Plat Prio Plus	RN-TAP-25KEPS-LS-3Y-PPP	$ 8,862,573.00	$ 7,710,438.51
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 3YR - Plat Prio Plus	RN-TAP-30KEPS-LS-3Y-PPP	##########	$ 9,252,525.69
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 3YR - Plat Prio Plus	RN-TAP-35KEPS-LS-3Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 3YR - Plat Prio Plus	RN-TAP-40KEPS-LS-3Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 4YR - Plat Prio Plus	RN-TAP-1KEPS-LS-4Y-PPP	$ 2,068,128.00	$ 1,799,271.36
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 4YR - Plat Prio Plus	RN-TAP-2.5KEPS-LS-4Y-PPP	$ 2,524,108.00	$ 2,195,973.96
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 4YR - Plat Prio Plus	RN-TAP-5KEPS-LS-4Y-PPP	$ 2,957,964.00	$ 2,573,428.68
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 4YR - Plat Prio Plus	RN-TAP-10KEPS-LS-4Y-PPP	$ 4,726,704.00	$ 4,112,232.48
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 4YR - Plat Prio Plus	RN-TAP-15KEPS-LS-4Y-PPP	$ 7,090,056.00	$ 6,168,348.72
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 4YR - Plat Prio Plus	RN-TAP-20KEPS-LS-4Y-PPP	$ 9,453,412.00	$ 8,224,468.44

FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 4YR - Plat Prio Plus	RN-TAP-25KEPS-LS-4Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 4YR - Plat Prio Plus	RN-TAP-30KEPS-LS-4Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 4YR - Plat Prio Plus	RN-TAP-35KEPS-LS-4Y-PPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 4YR - Plat Prio Plus	RN-TAP-40KEPS-LS-4Y-PPP	##########	##########
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 1YR - Platinum	TAP-1KEPS-DT2SS-1Y-P-A	$ 122,185.00	$ 106,300.95
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-DT2SS-1Y-P-A	$ 157,270.00	$ 136,824.90
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 1YR - Platinum	TAP-5KEPS-DT2SS-1Y-P-A	$ 193,405.00	$ 168,262.35
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 1YR - Platinum	TAP-10KEPS-DT2SS-1Y-P-A	$ 327,834.00	$ 285,215.58
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 1YR - Platinum	TAP-15KEPS-DT2SS-1Y-P-A	$ 491,751.00	$ 427,823.37
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 1YR - Platinum	TAP-20KEPS-DT2SS-1Y-P-A	$ 686,854.00	$ 597,562.98
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 1YR - Platinum	TAP-25KEPS-DT2SS-1Y-P-A	$ 875,135.00	$ 761,367.45
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 1YR - Platinum	TAP-30KEPS-DT2SS-1Y-P-A	$ 1,050,162.00	$ 913,640.94
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 1YR - Platinum	TAP-35KEPS-DT2SS-1Y-P-A	$ 1,225,189.00	$ 1,065,914.43
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 1YR - Platinum	TAP-40KEPS-DT2SS-1Y-P-A	$ 1,400,216.00	$ 1,218,187.92
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 1YR - Platinum	TAP-45KEPS-DT2SS-1Y-P-A	$ 1,575,243.00	$ 1,370,461.41
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 1YR - Platinum	TAP-50KEPS-DT2SS-1Y-P-A	$ 1,750,270.00	$ 1,522,734.90
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 1YR - Platinum	TAP-55KEPS-DT2SS-1Y-P-A	$ 1,925,297.00	$ 1,675,008.39
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 1YR - Platinum	TAP-60KEPS-DT2SS-1Y-P-A	$ 2,100,324.00	$ 1,827,281.88
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 1YR - Platinum	TAP-65KEPS-DT2SS-1Y-P-A	$ 2,275,351.00	$ 1,979,555.37
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 1YR - Platinum	TAP-70KEPS-DT2SS-1Y-P-A	$ 2,450,378.00	$ 2,131,828.86
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 1YR - Platinum	TAP-75KEPS-DT2SS-1Y-P-A	$ 2,625,405.00	$ 2,284,102.35
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 1YR - Platinum	TAP-80KEPS-DT2SS-1Y-P-A	$ 2,800,432.00	$ 2,436,375.84
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 2YR - Platinum	TAP-1KEPS-DT2SS-2Y-P-A	$ 244,370.00	$ 212,601.90
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-DT2SS-2Y-P-A	$ 314,540.00	$ 273,649.80
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 2YR - Platinum	TAP-5KEPS-DT2SS-2Y-P-A	$ 386,810.00	$ 336,524.70
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 2YR - Platinum	TAP-10KEPS-DT2SS-2Y-P-A	$ 655,668.00	$ 570,431.16
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 2YR - Platinum	TAP-15KEPS-DT2SS-2Y-P-A	$ 983,502.00	$ 855,646.74
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 2YR - Platinum	TAP-20KEPS-DT2SS-2Y-P-A	$ 1,373,708.00	$ 1,195,125.96
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 2YR - Platinum	TAP-25KEPS-DT2SS-2Y-P-A	$ 1,750,270.00	$ 1,522,734.90
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 2YR - Platinum	TAP-30KEPS-DT2SS-2Y-P-A	$ 2,100,324.00	$ 1,827,281.88
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 2YR - Platinum	TAP-35KEPS-DT2SS-2Y-P-A	$ 2,450,378.00	$ 2,131,828.86
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 2YR - Platinum	TAP-40KEPS-DT2SS-2Y-P-A	$ 2,800,432.00	$ 2,436,375.84
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 2YR - Platinum	TAP-45KEPS-DT2SS-2Y-P-A	$ 3,150,486.00	$ 2,740,922.82
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 2YR - Platinum	TAP-50KEPS-DT2SS-2Y-P-A	$ 3,500,540.00	$ 3,045,469.80
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 2YR - Platinum	TAP-55KEPS-DT2SS-2Y-P-A	$ 3,850,594.00	$ 3,350,016.78
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 2YR - Platinum	TAP-60KEPS-DT2SS-2Y-P-A	$ 4,200,648.00	$ 3,654,563.76
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 2YR - Platinum	TAP-65KEPS-DT2SS-2Y-P-A	$ 4,550,702.00	$ 3,959,110.74
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 2YR - Platinum	TAP-70KEPS-DT2SS-2Y-P-A	$ 4,900,756.00	$ 4,263,657.72
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 2YR - Platinum	TAP-75KEPS-DT2SS-2Y-P-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 2YR - Platinum	TAP-80KEPS-DT2SS-2Y-P-A	$ 5,600,864.00	$ 4,872,751.68
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 3YR - Platinum	TAP-1KEPS-DT2SS-3Y-P-A	$ 366,555.00	$ 318,902.85
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-DT2SS-3Y-P-A	$ 471,810.00	$ 410,474.70
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 3YR - Platinum	TAP-5KEPS-DT2SS-3Y-P-A	$ 580,215.00	$ 504,787.05
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 3YR - Platinum	TAP-10KEPS-DT2SS-3Y-P-A	$ 983,502.00	$ 855,646.74
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 3YR - Platinum	TAP-15KEPS-DT2SS-3Y-P-A	$ 1,475,253.00	$ 1,283,470.11
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 3YR - Platinum	TAP-20KEPS-DT2SS-3Y-P-A	$ 2,060,562.00	$ 1,792,688.94
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 3YR - Platinum	TAP-25KEPS-DT2SS-3Y-P-A	$ 2,625,405.00	$ 2,284,102.35
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 3YR - Platinum	TAP-30KEPS-DT2SS-3Y-P-A	$ 3,150,486.00	$ 2,740,922.82
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 3YR - Platinum	TAP-35KEPS-DT2SS-3Y-P-A	$ 3,675,567.00	$ 3,197,743.29

FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 3YR - Platinum	TAP-40KEPS-DT2SS-3Y-P-A	$ 4,200,648.00	$ 3,654,563.76
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 3YR - Platinum	TAP-45KEPS-DT2SS-3Y-P-A	$ 4,725,729.00	$ 4,111,384.23
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 3YR - Platinum	TAP-50KEPS-DT2SS-3Y-P-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 3YR - Platinum	TAP-55KEPS-DT2SS-3Y-P-A	$ 5,775,891.00	$ 5,025,025.17
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 3YR - Platinum	TAP-60KEPS-DT2SS-3Y-P-A	$ 6,300,972.00	$ 5,481,845.64
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 3YR - Platinum	TAP-65KEPS-DT2SS-3Y-P-A	$ 6,826,053.00	$ 5,938,666.11
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 3YR - Platinum	TAP-70KEPS-DT2SS-3Y-P-A	$ 7,351,134.00	$ 6,395,486.58
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 3YR - Platinum	TAP-75KEPS-DT2SS-3Y-P-A	$ 7,876,215.00	$ 6,852,307.05
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 3YR - Platinum	TAP-80KEPS-DT2SS-3Y-P-A	$ 8,401,296.00	$ 7,309,127.52
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 4YR - Platinum	TAP-1KEPS-DT2SS-4Y-P-A	$ 488,740.00	$ 425,203.80
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-DT2SS-4Y-P-A	$ 629,080.00	$ 547,299.60
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 4YR - Platinum	TAP-5KEPS-DT2SS-4Y-P-A	$ 773,620.00	$ 673,049.40
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 4YR - Platinum	TAP-10KEPS-DT2SS-4Y-P-A	$ 1,311,336.00	$ 1,140,862.32
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 4YR - Platinum	TAP-15KEPS-DT2SS-4Y-P-A	$ 1,967,004.00	$ 1,711,293.48
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 4YR - Platinum	TAP-20KEPS-DT2SS-4Y-P-A	$ 2,747,416.00	$ 2,390,251.92
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 4YR - Platinum	TAP-25KEPS-DT2SS-4Y-P-A	$ 3,500,540.00	$ 3,045,469.80
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 4YR - Platinum	TAP-30KEPS-DT2SS-4Y-P-A	$ 4,200,648.00	$ 3,654,563.76
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 4YR - Platinum	TAP-35KEPS-DT2SS-4Y-P-A	$ 4,900,756.00	$ 4,263,657.72
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 4YR - Platinum	TAP-40KEPS-DT2SS-4Y-P-A	$ 5,600,864.00	$ 4,872,751.68
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 4YR - Platinum	TAP-45KEPS-DT2SS-4Y-P-A	$ 6,300,972.00	$ 5,481,845.64
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 4YR - Platinum	TAP-50KEPS-DT2SS-4Y-P-A	$ 7,001,080.00	$ 6,090,939.60
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 4YR - Platinum	TAP-55KEPS-DT2SS-4Y-P-A	$ 7,701,188.00	$ 6,700,033.56
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 4YR - Platinum	TAP-60KEPS-DT2SS-4Y-P-A	$ 8,401,296.00	$ 7,309,127.52
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 4YR - Platinum	TAP-65KEPS-DT2SS-4Y-P-A	$ 9,101,404.00	$ 7,918,221.48
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 4YR - Platinum	TAP-70KEPS-DT2SS-4Y-P-A	$ 9,801,512.00	$ 8,527,315.44
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 4YR - Platinum	TAP-75KEPS-DT2SS-4Y-P-A	##############	$ 9,136,409.40
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 4YR - Platinum	TAP-80KEPS-DT2SS-4Y-P-A	##############	$ 9,745,503.36
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 5YR - Platinum	TAP-1KEPS-DT2SS-5Y-P-A	$ 610,925.00	$ 531,504.75
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-DT2SS-5Y-P-A	$ 786,350.00	$ 684,124.50
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 5YR - Platinum	TAP-5KEPS-DT2SS-5Y-P-A	$ 967,025.00	$ 841,311.75
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 5YR - Platinum	TAP-10KEPS-DT2SS-5Y-P-A	$ 1,639,170.00	$ 1,426,077.90
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 5YR - Platinum	TAP-15KEPS-DT2SS-5Y-P-A	$ 2,458,755.00	$ 2,139,116.85
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 5YR - Platinum	TAP-20KEPS-DT2SS-5Y-P-A	$ 3,434,270.00	$ 2,987,814.90
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 5YR - Platinum	TAP-25KEPS-DT2SS-5Y-P-A	$ 4,375,675.00	$ 3,806,837.25
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 5YR - Platinum	TAP-30KEPS-DT2SS-5Y-P-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 5YR - Platinum	TAP-35KEPS-DT2SS-5Y-P-A	$ 6,125,945.00	$ 5,329,572.15
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 5YR - Platinum	TAP-40KEPS-DT2SS-5Y-P-A	$ 7,001,080.00	$ 6,090,939.60
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 5YR - Platinum	TAP-45KEPS-DT2SS-5Y-P-A	$ 7,876,215.00	$ 6,852,307.05
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 5YR - Platinum	TAP-50KEPS-DT2SS-5Y-P-A	$ 8,751,350.00	$ 7,613,674.50
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 5YR - Platinum	TAP-55KEPS-DT2SS-5Y-P-A	$ 9,626,485.00	$ 8,375,041.95
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 5YR - Platinum	TAP-60KEPS-DT2SS-5Y-P-A	##############	$ 9,136,409.40
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 5YR - Platinum	TAP-65KEPS-DT2SS-5Y-P-A	##############	$ 9,897,776.85
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 5YR - Platinum	TAP-70KEPS-DT2SS-5Y-P-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 5YR - Platinum	TAP-75KEPS-DT2SS-5Y-P-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 5YR - Platinum	TAP-80KEPS-DT2SS-5Y-P-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-DT2SS-1Y-PPP-A	$ 128,294.00	$ 111,615.78
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-DT2SS-1Y-PPP-	$ 165,134.00	$ 143,666.58
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-DT2SS-1Y-PPP-A	$ 203,076.00	$ 176,676.12
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-DT2SS-1Y-PPP-A	$ 344,225.00	$ 299,475.75

FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-DT2SS-1Y-PPP-A	$ 516,338.00	$ 449,214.06
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-DT2SS-1Y-PPP-A	$ 721,197.00	$ 627,441.39
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-DT2SS-1Y-PPP-A	$ 918,892.00	$ 799,436.04
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-DT2SS-1Y-PPP-A	$ 1,102,670.00	$ 959,322.90
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-DT2SS-1Y-PPP-A	$ 1,286,448.00	$ 1,119,209.76
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-DT2SS-1Y-PPP-A	$ 1,470,227.00	$ 1,279,097.49
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 1YR - Plat Prio Plus	TAP-45KEPS-DT2SS-1Y-PPP-A	$ 1,654,005.00	$ 1,438,984.35
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 1YR - Plat Prio Plus	TAP-50KEPS-DT2SS-1Y-PPP-A	$ 1,837,784.00	$ 1,598,872.08
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 1YR - Plat Prio Plus	TAP-55KEPS-DT2SS-1Y-PPP-A	$ 2,021,562.00	$ 1,758,758.94
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 1YR - Plat Prio Plus	TAP-60KEPS-DT2SS-1Y-PPP-A	$ 2,205,340.00	$ 1,918,645.80
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 1YR - Plat Prio Plus	TAP-65KEPS-DT2SS-1Y-PPP-A	$ 2,389,119.00	$ 2,078,533.53
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 1YR - Plat Prio Plus	TAP-70KEPS-DT2SS-1Y-PPP-A	$ 2,572,897.00	$ 2,238,420.39
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 1YR - Plat Prio Plus	TAP-75KEPS-DT2SS-1Y-PPP-A	$ 2,756,675.00	$ 2,398,307.25
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 1YR - Plat Prio Plus	TAP-80KEPS-DT2SS-1Y-PPP-A	$ 2,940,453.00	$ 2,558,194.11
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-DT2SS-2Y-PPP-A	$ 256,588.00	$ 223,231.56
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-DT2SS-2Y-PPP-	$ 330,268.00	$ 287,333.16
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-DT2SS-2Y-PPP-A	$ 406,152.00	$ 353,352.24
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-DT2SS-2Y-PPP-A	$ 688,450.00	$ 598,951.50
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-DT2SS-2Y-PPP-A	$ 1,032,676.00	$ 898,428.12
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-DT2SS-2Y-PPP-A	$ 1,442,394.00	$ 1,254,882.78
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-DT2SS-2Y-PPP-A	$ 1,837,784.00	$ 1,598,872.08
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-DT2SS-2Y-PPP-A	$ 2,205,340.00	$ 1,918,645.80
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-DT2SS-2Y-PPP-A	$ 2,572,896.00	$ 2,238,419.52
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-DT2SS-2Y-PPP-A	$ 2,940,454.00	$ 2,558,194.98
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 2YR - Plat Prio Plus	TAP-45KEPS-DT2SS-2Y-PPP-A	$ 3,308,010.00	$ 2,877,968.70
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 2YR - Plat Prio Plus	TAP-50KEPS-DT2SS-2Y-PPP-A	$ 3,675,568.00	$ 3,197,744.16
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 2YR - Plat Prio Plus	TAP-55KEPS-DT2SS-2Y-PPP-A	$ 4,043,124.00	$ 3,517,517.88
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 2YR - Plat Prio Plus	TAP-60KEPS-DT2SS-2Y-PPP-A	$ 4,410,680.00	$ 3,837,291.60
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 2YR - Plat Prio Plus	TAP-65KEPS-DT2SS-2Y-PPP-A	$ 4,778,238.00	$ 4,157,067.06
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 2YR - Plat Prio Plus	TAP-70KEPS-DT2SS-2Y-PPP-A	$ 5,145,794.00	$ 4,476,840.78
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 2YR - Plat Prio Plus	TAP-75KEPS-DT2SS-2Y-PPP-A	$ 5,513,350.00	$ 4,796,614.50
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 2YR - Plat Prio Plus	TAP-80KEPS-DT2SS-2Y-PPP-A	$ 5,880,906.00	$ 5,116,388.22
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-DT2SS-3Y-PPP-A	$ 384,882.00	$ 334,847.34
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-DT2SS-3Y-PPP-	$ 495,402.00	$ 430,999.74
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-DT2SS-3Y-PPP-A	$ 609,228.00	$ 530,028.36
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-DT2SS-3Y-PPP-A	$ 1,032,675.00	$ 898,427.25
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-DT2SS-3Y-PPP-A	$ 1,549,014.00	$ 1,347,642.18
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-DT2SS-3Y-PPP-A	$ 2,163,591.00	$ 1,882,324.17
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-DT2SS-3Y-PPP-A	$ 2,756,676.00	$ 2,398,308.12
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-DT2SS-3Y-PPP-A	$ 3,308,010.00	$ 2,877,968.70
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-DT2SS-3Y-PPP-A	$ 3,859,344.00	$ 3,357,629.28
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-DT2SS-3Y-PPP-A	$ 4,410,681.00	$ 3,837,292.47
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 3YR - Plat Prio Plus	TAP-45KEPS-DT2SS-3Y-PPP-A	$ 4,962,015.00	$ 4,316,953.05
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 3YR - Plat Prio Plus	TAP-50KEPS-DT2SS-3Y-PPP-A	$ 5,513,352.00	$ 4,796,616.24
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 3YR - Plat Prio Plus	TAP-55KEPS-DT2SS-3Y-PPP-A	$ 6,064,686.00	$ 5,276,276.82
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 3YR - Plat Prio Plus	TAP-60KEPS-DT2SS-3Y-PPP-A	$ 6,616,020.00	$ 5,755,937.40
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 3YR - Plat Prio Plus	TAP-65KEPS-DT2SS-3Y-PPP-A	$ 7,167,357.00	$ 6,235,600.59
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 3YR - Plat Prio Plus	TAP-70KEPS-DT2SS-3Y-PPP-A	$ 7,718,691.00	$ 6,715,261.17
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 3YR - Plat Prio Plus	TAP-75KEPS-DT2SS-3Y-PPP-A	$ 8,270,025.00	$ 7,194,921.75

FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 3YR - Plat Prio Plus	TAP-80KEPS-DT2SS-3Y-PPP-A	$ 8,821,359.00	$ 7,674,582.33
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-DT2SS-4Y-PPP-A	$ 513,176.00	$ 446,463.12
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-DT2SS-4Y-PPP-	$ 660,536.00	$ 574,666.32
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-DT2SS-4Y-PPP-A	$ 812,304.00	$ 706,704.48
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-DT2SS-4Y-PPP-A	$ 1,376,900.00	$ 1,197,903.00
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-DT2SS-4Y-PPP-A	$ 2,065,352.00	$ 1,796,856.24
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-DT2SS-4Y-PPP-A	$ 2,884,788.00	$ 2,509,765.56
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-DT2SS-4Y-PPP-A	$ 3,675,568.00	$ 3,197,744.16
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-DT2SS-4Y-PPP-A	$ 4,410,680.00	$ 3,837,291.60
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-DT2SS-4Y-PPP-A	$ 5,145,792.00	$ 4,476,839.04
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-DT2SS-4Y-PPP-A	$ 5,880,908.00	$ 5,116,389.96
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 4YR - Plat Prio Plus	TAP-45KEPS-DT2SS-4Y-PPP-A	$ 6,616,020.00	$ 5,755,937.40
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 4YR - Plat Prio Plus	TAP-50KEPS-DT2SS-4Y-PPP-A	$ 7,351,136.00	$ 6,395,488.32
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 4YR - Plat Prio Plus	TAP-55KEPS-DT2SS-4Y-PPP-A	$ 8,086,248.00	$ 7,035,035.76
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 4YR - Plat Prio Plus	TAP-60KEPS-DT2SS-4Y-PPP-A	$ 8,821,360.00	$ 7,674,583.20
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 4YR - Plat Prio Plus	TAP-65KEPS-DT2SS-4Y-PPP-A	$ 9,556,476.00	$ 8,314,134.12
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 4YR - Plat Prio Plus	TAP-70KEPS-DT2SS-4Y-PPP-A	############	$ 8,953,681.56
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 4YR - Plat Prio Plus	TAP-75KEPS-DT2SS-4Y-PPP-A	############	$ 9,593,229.00
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 4YR - Plat Prio Plus	TAP-80KEPS-DT2SS-4Y-PPP-A	############	############
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-DT2SS-5Y-PPP-A	$ 641,470.00	$ 558,078.90
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-DT2SS-5Y-PPP-	$ 825,670.00	$ 718,332.90
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-DT2SS-5Y-PPP-A	$ 1,015,380.00	$ 883,380.60
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-DT2SS-5Y-PPP-A	$ 1,721,125.00	$ 1,497,378.75
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-DT2SS-5Y-PPP-A	$ 2,581,690.00	$ 2,246,070.30
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-DT2SS-5Y-PPP-A	$ 3,605,985.00	$ 3,137,206.95
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-DT2SS-5Y-PPP-A	$ 4,594,460.00	$ 3,997,180.20
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-DT2SS-5Y-PPP-A	$ 5,513,350.00	$ 4,796,614.50
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-DT2SS-5Y-PPP-A	$ 6,432,240.00	$ 5,596,048.80
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-DT2SS-5Y-PPP-A	$ 7,351,135.00	$ 6,395,487.45
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 5YR - Plat Prio Plus	TAP-45KEPS-DT2SS-5Y-PPP-A	$ 8,270,025.00	$ 7,194,921.75
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 5YR - Plat Prio Plus	TAP-50KEPS-DT2SS-5Y-PPP-A	$ 9,188,920.00	$ 7,994,360.40
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 5YR - Plat Prio Plus	TAP-55KEPS-DT2SS-5Y-PPP-A	############	$ 8,793,794.70
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 5YR - Plat Prio Plus	TAP-60KEPS-DT2SS-5Y-PPP-A	############	$ 9,593,229.00
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 5YR - Plat Prio Plus	TAP-65KEPS-DT2SS-5Y-PPP-A	############	############
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 5YR - Plat Prio Plus	TAP-70KEPS-DT2SS-5Y-PPP-A	############	############
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 5YR - Plat Prio Plus	TAP-75KEPS-DT2SS-5Y-PPP-A	############	############
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 5YR - Plat Prio Plus	TAP-80KEPS-DT2SS-5Y-PPP-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 1YR - Platinum	TAP-1KEPS-DT2LS-1Y-P-A	$ 381,961.00	$ 332,306.07
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-DT2LS-1Y-P-A	$ 481,990.00	$ 419,331.30
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 1YR - Platinum	TAP-5KEPS-DT2LS-1Y-P-A	$ 583,069.00	$ 507,270.03
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 1YR - Platinum	TAP-10KEPS-DT2LS-1Y-P-A	$ 977,274.00	$ 850,228.38
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 1YR - Platinum	TAP-15KEPS-DT2LS-1Y-P-A	$ 1,465,911.00	$ 1,275,342.57
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 1YR - Platinum	TAP-20KEPS-DT2LS-1Y-P-A	$ 1,985,734.00	$ 1,727,588.58
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 1YR - Platinum	TAP-25KEPS-DT2LS-1Y-P-A	$ 2,498,735.00	$ 2,173,899.45
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 1YR - Platinum	TAP-30KEPS-DT2LS-1Y-P-A	$ 2,998,482.00	$ 2,608,679.34
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 1YR - Platinum	TAP-35KEPS-DT2LS-1Y-P-A	$ 3,498,229.00	$ 3,043,459.23
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 1YR - Platinum	TAP-40KEPS-DT2LS-1Y-P-A	$ 3,997,976.00	$ 3,478,239.12
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 2YR - Platinum	TAP-1KEPS-DT2LS-2Y-P-A	$ 763,922.00	$ 664,612.14
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-DT2LS-2Y-P-A	$ 963,980.00	$ 838,662.60

FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 2YR - Platinum	TAP-5KEPS-DT2LS-2Y-P-A	$ 1,166,138.00	$ 1,014,540.06
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 2YR - Platinum	TAP-10KEPS-DT2LS-2Y-P-A	$ 1,954,548.00	$ 1,700,456.76
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 2YR - Platinum	TAP-15KEPS-DT2LS-2Y-P-A	$ 2,931,822.00	$ 2,550,685.14
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 2YR - Platinum	TAP-20KEPS-DT2LS-2Y-P-A	$ 3,971,468.00	$ 3,455,177.16
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 2YR - Platinum	TAP-25KEPS-DT2LS-2Y-P-A	$ 4,997,470.00	$ 4,347,798.90
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 2YR - Platinum	TAP-30KEPS-DT2LS-2Y-P-A	$ 5,996,964.00	$ 5,217,358.68
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 2YR - Platinum	TAP-35KEPS-DT2LS-2Y-P-A	$ 6,996,458.00	$ 6,086,918.46
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 2YR - Platinum	TAP-40KEPS-DT2LS-2Y-P-A	$ 7,995,952.00	$ 6,956,478.24
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 3YR - Platinum	TAP-1KEPS-DT2LS-3Y-P-A	$ 1,145,883.00	$ 996,918.21
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-DT2LS-3Y-P-A	$ 1,445,970.00	$ 1,257,993.90
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 3YR - Platinum	TAP-5KEPS-DT2LS-3Y-P-A	$ 1,749,207.00	$ 1,521,810.09
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 3YR - Platinum	TAP-10KEPS-DT2LS-3Y-P-A	$ 2,931,822.00	$ 2,550,685.14
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 3YR - Platinum	TAP-15KEPS-DT2LS-3Y-P-A	$ 4,397,733.00	$ 3,826,027.71
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 3YR - Platinum	TAP-20KEPS-DT2LS-3Y-P-A	$ 5,957,202.00	$ 5,182,765.74
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 3YR - Platinum	TAP-25KEPS-DT2LS-3Y-P-A	$ 7,496,205.00	$ 6,521,698.35
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 3YR - Platinum	TAP-30KEPS-DT2LS-3Y-P-A	$ 8,995,446.00	$ 7,826,038.02
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 3YR - Platinum	TAP-35KEPS-DT2LS-3Y-P-A	##########	$ 9,130,377.69
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 3YR - Platinum	TAP-40KEPS-DT2LS-3Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 4YR - Platinum	TAP-1KEPS-DT2LS-4Y-P-A	$ 1,527,844.00	$ 1,329,224.28
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-DT2LS-4Y-P-A	$ 1,927,960.00	$ 1,677,325.20
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 4YR - Platinum	TAP-5KEPS-DT2LS-4Y-P-A	$ 2,332,276.00	$ 2,029,080.12
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 4YR - Platinum	TAP-10KEPS-DT2LS-4Y-P-A	$ 3,909,096.00	$ 3,400,913.52
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 4YR - Platinum	TAP-15KEPS-DT2LS-4Y-P-A	$ 5,863,644.00	$ 5,101,370.28
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 4YR - Platinum	TAP-20KEPS-DT2LS-4Y-P-A	$ 7,942,936.00	$ 6,910,354.32
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 4YR - Platinum	TAP-25KEPS-DT2LS-4Y-P-A	$ 9,994,940.00	$ 8,695,597.80
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 4YR - Platinum	TAP-30KEPS-DT2LS-4Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 4YR - Platinum	TAP-35KEPS-DT2LS-4Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 4YR - Platinum	TAP-40KEPS-DT2LS-4Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 5YR - Platinum	TAP-1KEPS-DT2LS-5Y-P-A	$ 1,909,805.00	$ 1,661,530.35
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-DT2LS-5Y-P-A	$ 2,409,950.00	$ 2,096,656.50
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 5YR - Platinum	TAP-5KEPS-DT2LS-5Y-P-A	$ 2,915,345.00	$ 2,536,350.15
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 5YR - Platinum	TAP-10KEPS-DT2LS-5Y-P-A	$ 4,886,370.00	$ 4,251,141.90
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 5YR - Platinum	TAP-15KEPS-DT2LS-5Y-P-A	$ 7,329,555.00	$ 6,376,712.85
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 5YR - Platinum	TAP-20KEPS-DT2LS-5Y-P-A	$ 9,928,670.00	$ 8,637,942.90
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 5YR - Platinum	TAP-25KEPS-DT2LS-5Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 5YR - Platinum	TAP-30KEPS-DT2LS-5Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 5YR - Platinum	TAP-35KEPS-DT2LS-5Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 5YR - Platinum	TAP-40KEPS-DT2LS-5Y-P-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-DT2LS-1Y-PPP-A	$ 401,059.00	$ 348,921.33
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-DT2LS-1Y-PPP-A	$ 506,090.00	$ 440,298.30
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-DT2LS-1Y-PPP-A	$ 612,223.00	$ 532,634.01
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-DT2LS-1Y-PPP-A	$ 1,026,137.00	$ 892,739.19
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-DT2LS-1Y-PPP-A	$ 1,539,206.00	$ 1,339,109.22
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-DT2LS-1Y-PPP-A	$ 2,085,021.00	$ 1,813,968.27
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-DT2LS-1Y-PPP-A	$ 2,623,672.00	$ 2,282,594.64
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-DT2LS-1Y-PPP-A	$ 3,148,406.00	$ 2,739,113.22
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-DT2LS-1Y-PPP-A	$ 3,673,140.00	$ 3,195,631.80
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-DT2LS-1Y-PPP-A	$ 4,197,875.00	$ 3,652,151.25
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-DT2LS-2Y-PPP-A	$ 802,118.00	$ 697,842.66

FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-DT2LS-2Y-PPP-A	$ 1,012,180.00	$ 880,596.60
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-DT2LS-2Y-PPP-A	$ 1,224,446.00	$ 1,065,268.02
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-DT2LS-2Y-PPP-A	$ 2,052,274.00	$ 1,785,478.38
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-DT2LS-2Y-PPP-A	$ 3,078,412.00	$ 2,678,218.44
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-DT2LS-2Y-PPP-A	$ 4,170,042.00	$ 3,627,936.54
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-DT2LS-2Y-PPP-A	$ 5,247,344.00	$ 4,565,189.28
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-DT2LS-2Y-PPP-A	$ 6,296,812.00	$ 5,478,226.44
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-DT2LS-2Y-PPP-A	$ 7,346,280.00	$ 6,391,263.60
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-DT2LS-2Y-PPP-A	$ 8,395,750.00	$ 7,304,302.50
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-DT2LS-3Y-PPP-A	$ 1,203,177.00	$ 1,046,763.99
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-DT2LS-3Y-PPP-A	$ 1,518,270.00	$ 1,320,894.90
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-DT2LS-3Y-PPP-A	$ 1,836,669.00	$ 1,597,902.03
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-DT2LS-3Y-PPP-A	$ 3,078,411.00	$ 2,678,217.57
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-DT2LS-3Y-PPP-A	$ 4,617,618.00	$ 4,017,327.66
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-DT2LS-3Y-PPP-A	$ 6,255,063.00	$ 5,441,904.81
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-DT2LS-3Y-PPP-A	$ 7,871,016.00	$ 6,847,783.92
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-DT2LS-3Y-PPP-A	$ 9,445,218.00	$ 8,217,339.66
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-DT2LS-3Y-PPP-A	##########	$ 9,586,895.40
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-DT2LS-3Y-PPP-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-DT2LS-4Y-PPP-A	$ 1,604,236.00	$ 1,395,685.32
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-DT2LS-4Y-PPP-A	$ 2,024,360.00	$ 1,761,193.20
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-DT2LS-4Y-PPP-A	$ 2,448,892.00	$ 2,130,536.04
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-DT2LS-4Y-PPP-A	$ 4,104,548.00	$ 3,570,956.76
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-DT2LS-4Y-PPP-A	$ 6,156,824.00	$ 5,356,436.88
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-DT2LS-4Y-PPP-A	$ 8,340,084.00	$ 7,255,873.08
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-DT2LS-4Y-PPP-A	##########	$ 9,130,378.56
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-DT2LS-4Y-PPP-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-DT2LS-4Y-PPP-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-DT2LS-4Y-PPP-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-DT2LS-5Y-PPP-A	$ 2,005,295.00	$ 1,744,606.65
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-DT2LS-5Y-PPP-A	$ 2,530,450.00	$ 2,201,491.50
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-DT2LS-5Y-PPP-A	$ 3,061,115.00	$ 2,663,170.05
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-DT2LS-5Y-PPP-A	$ 5,130,685.00	$ 4,463,695.95
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-DT2LS-5Y-PPP-A	$ 7,696,030.00	$ 6,695,546.10
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-DT2LS-5Y-PPP-A	##########	$ 9,069,841.35
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-DT2LS-5Y-PPP-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-DT2LS-5Y-PPP-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-DT2LS-5Y-PPP-A	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-DT2LS-5Y-PPP-A	##########	##########
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 1YR - Platinum	TAP-1KEPS-SS2LS-1Y-P-A	$ 259,776.00	$ 226,005.12
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 1YR - Platinum	TAP-2.5KEPS-SS2LS-1Y-P-A	$ 324,720.00	$ 282,506.40
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 1YR - Platinum	TAP-5KEPS-SS2LS-1Y-P-A	$ 389,664.00	$ 339,007.68
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 1YR - Platinum	TAP-10KEPS-SS2LS-1Y-P-A	$ 649,440.00	$ 565,012.80
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 1YR - Platinum	TAP-15KEPS-SS2LS-1Y-P-A	$ 974,160.00	$ 847,519.20
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 1YR - Platinum	TAP-20KEPS-SS2LS-1Y-P-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 1YR - Platinum	TAP-25KEPS-SS2LS-1Y-P-A	$ 1,623,600.00	$ 1,412,532.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 1YR - Platinum	TAP-30KEPS-SS2LS-1Y-P-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 1YR - Platinum	TAP-35KEPS-SS2LS-1Y-P-A	$ 2,273,040.00	$ 1,977,544.80
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 1YR - Platinum	TAP-40KEPS-SS2LS-1Y-P-A	$ 2,597,760.00	$ 2,260,051.20

FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 2YR - Platinum	TAP-1KEPS-SS2LS-2Y-P-A	$ 519,552.00	$ 452,010.24
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 2YR - Platinum	TAP-2.5KEPS-SS2LS-2Y-P-A	$ 649,440.00	$ 565,012.80
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 2YR - Platinum	TAP-5KEPS-SS2LS-2Y-P-A	$ 779,328.00	$ 678,015.36
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 2YR - Platinum	TAP-10KEPS-SS2LS-2Y-P-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 2YR - Platinum	TAP-15KEPS-SS2LS-2Y-P-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 2YR - Platinum	TAP-20KEPS-SS2LS-2Y-P-A	$ 2,597,760.00	$ 2,260,051.20
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 2YR - Platinum	TAP-25KEPS-SS2LS-2Y-P-A	$ 3,247,200.00	$ 2,825,064.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 2YR - Platinum	TAP-30KEPS-SS2LS-2Y-P-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 2YR - Platinum	TAP-35KEPS-SS2LS-2Y-P-A	$ 4,546,080.00	$ 3,955,089.60
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 2YR - Platinum	TAP-40KEPS-SS2LS-2Y-P-A	$ 5,195,520.00	$ 4,520,102.40
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 3YR - Platinum	TAP-1KEPS-SS2LS-3Y-P-A	$ 779,328.00	$ 678,015.36
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 3YR - Platinum	TAP-2.5KEPS-SS2LS-3Y-P-A	$ 974,160.00	$ 847,519.20
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 3YR - Platinum	TAP-5KEPS-SS2LS-3Y-P-A	$ 1,168,992.00	$ 1,017,023.04
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 3YR - Platinum	TAP-10KEPS-SS2LS-3Y-P-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 3YR - Platinum	TAP-15KEPS-SS2LS-3Y-P-A	$ 2,922,480.00	$ 2,542,557.60
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 3YR - Platinum	TAP-20KEPS-SS2LS-3Y-P-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 3YR - Platinum	TAP-25KEPS-SS2LS-3Y-P-A	$ 4,870,800.00	$ 4,237,596.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 3YR - Platinum	TAP-30KEPS-SS2LS-3Y-P-A	$ 5,844,960.00	$ 5,085,115.20
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 3YR - Platinum	TAP-35KEPS-SS2LS-3Y-P-A	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 3YR - Platinum	TAP-40KEPS-SS2LS-3Y-P-A	$ 7,793,280.00	$ 6,780,153.60
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 4YR - Platinum	TAP-1KEPS-SS2LS-4Y-P-A	$ 1,039,104.00	$ 904,020.48
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 4YR - Platinum	TAP-2.5KEPS-SS2LS-4Y-P-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 4YR - Platinum	TAP-5KEPS-SS2LS-4Y-P-A	$ 1,558,656.00	$ 1,356,030.72
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 4YR - Platinum	TAP-10KEPS-SS2LS-4Y-P-A	$ 2,597,760.00	$ 2,260,051.20
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 4YR - Platinum	TAP-15KEPS-SS2LS-4Y-P-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 4YR - Platinum	TAP-20KEPS-SS2LS-4Y-P-A	$ 5,195,520.00	$ 4,520,102.40
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 4YR - Platinum	TAP-25KEPS-SS2LS-4Y-P-A	$ 6,494,400.00	$ 5,650,128.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 4YR - Platinum	TAP-30KEPS-SS2LS-4Y-P-A	$ 7,793,280.00	$ 6,780,153.60
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 4YR - Platinum	TAP-35KEPS-SS2LS-4Y-P-A	$ 9,092,160.00	$ 7,910,179.20
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 4YR - Platinum	TAP-40KEPS-SS2LS-4Y-P-A	##############	$ 9,040,204.80
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 5YR - Platinum	TAP-1KEPS-SS2LS-5Y-P-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 5YR - Platinum	TAP-2.5KEPS-SS2LS-5Y-P-A	$ 1,623,600.00	$ 1,412,532.00
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 5YR - Platinum	TAP-5KEPS-SS2LS-5Y-P-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 5YR - Platinum	TAP-10KEPS-SS2LS-5Y-P-A	$ 3,247,200.00	$ 2,825,064.00
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 5YR - Platinum	TAP-15KEPS-SS2LS-5Y-P-A	$ 4,870,800.00	$ 4,237,596.00
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 5YR - Platinum	TAP-20KEPS-SS2LS-5Y-P-A	$ 6,494,400.00	$ 5,650,128.00
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 5YR - Platinum	TAP-25KEPS-SS2LS-5Y-P-A	$ 8,118,000.00	$ 7,062,660.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 5YR - Platinum	TAP-30KEPS-SS2LS-5Y-P-A	$ 9,741,600.00	$ 8,475,192.00
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 5YR - Platinum	TAP-35KEPS-SS2LS-5Y-P-A	##############	$ 9,887,724.00
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 5YR - Platinum	TAP-40KEPS-SS2LS-5Y-P-A	##############	##############
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 1YR - Plat Prio Plus	TAP-1KEPS-SS2LS-1Y-PPP-A	$ 272,765.00	$ 237,305.55
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 1YR - Plat Prio Plus	TAP-2.5KEPS-SS2LS-1Y-PPP-A	$ 340,956.00	$ 296,631.72
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 1YR - Plat Prio Plus	TAP-5KEPS-SS2LS-1Y-PPP-A	$ 409,147.00	$ 355,957.89
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 1YR - Plat Prio Plus	TAP-10KEPS-SS2LS-1Y-PPP-A	$ 681,912.00	$ 593,263.44
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 1YR - Plat Prio Plus	TAP-15KEPS-SS2LS-1Y-PPP-A	$ 1,022,868.00	$ 889,895.16
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 1YR - Plat Prio Plus	TAP-20KEPS-SS2LS-1Y-PPP-A	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 1YR - Plat Prio Plus	TAP-25KEPS-SS2LS-1Y-PPP-A	$ 1,704,780.00	$ 1,483,158.60
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 1YR - Plat Prio Plus	TAP-30KEPS-SS2LS-1Y-PPP-A	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 1YR - Plat Prio Plus	TAP-35KEPS-SS2LS-1Y-PPP-A	$ 2,386,692.00	$ 2,076,422.04

FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 1YR - Plat Prio Plus	TAP-40KEPS-SS2LS-1Y-PPP-A	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 2YR - Plat Prio Plus	TAP-1KEPS-SS2LS-2Y-PPP-A	$ 545,530.00	$ 474,611.10
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 2YR - Plat Prio Plus	TAP-2.5KEPS-SS2LS-2Y-PPP-A	$ 681,912.00	$ 593,263.44
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 2YR - Plat Prio Plus	TAP-5KEPS-SS2LS-2Y-PPP-A	$ 818,294.00	$ 711,915.78
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 2YR - Plat Prio Plus	TAP-10KEPS-SS2LS-2Y-PPP-A	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 2YR - Plat Prio Plus	TAP-15KEPS-SS2LS-2Y-PPP-A	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 2YR - Plat Prio Plus	TAP-20KEPS-SS2LS-2Y-PPP-A	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 2YR - Plat Prio Plus	TAP-25KEPS-SS2LS-2Y-PPP-A	$ 3,409,560.00	$ 2,966,317.20
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 2YR - Plat Prio Plus	TAP-30KEPS-SS2LS-2Y-PPP-A	$ 4,091,472.00	$ 3,559,580.64
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 2YR - Plat Prio Plus	TAP-35KEPS-SS2LS-2Y-PPP-A	$ 4,773,384.00	$ 4,152,844.08
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 2YR - Plat Prio Plus	TAP-40KEPS-SS2LS-2Y-PPP-A	$ 5,455,296.00	$ 4,746,107.52
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 3YR - Plat Prio Plus	TAP-1KEPS-SS2LS-3Y-PPP-A	$ 818,295.00	$ 711,916.65
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 3YR - Plat Prio Plus	TAP-2.5KEPS-SS2LS-3Y-PPP-A	$ 1,022,868.00	$ 889,895.16
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 3YR - Plat Prio Plus	TAP-5KEPS-SS2LS-3Y-PPP-A	$ 1,227,441.00	$ 1,067,873.67
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 3YR - Plat Prio Plus	TAP-10KEPS-SS2LS-3Y-PPP-A	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 3YR - Plat Prio Plus	TAP-15KEPS-SS2LS-3Y-PPP-A	$ 3,068,604.00	$ 2,669,685.48
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 3YR - Plat Prio Plus	TAP-20KEPS-SS2LS-3Y-PPP-A	$ 4,091,472.00	$ 3,559,580.64
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 3YR - Plat Prio Plus	TAP-25KEPS-SS2LS-3Y-PPP-A	$ 5,114,340.00	$ 4,449,475.80
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 3YR - Plat Prio Plus	TAP-30KEPS-SS2LS-3Y-PPP-A	$ 6,137,208.00	$ 5,339,370.96
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 3YR - Plat Prio Plus	TAP-35KEPS-SS2LS-3Y-PPP-A	$ 7,160,076.00	$ 6,229,266.12
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 3YR - Plat Prio Plus	TAP-40KEPS-SS2LS-3Y-PPP-A	$ 8,182,944.00	$ 7,119,161.28
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 4YR - Plat Prio Plus	TAP-1KEPS-SS2LS-4Y-PPP-A	$ 1,091,060.00	$ 949,222.20
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 4YR - Plat Prio Plus	TAP-2.5KEPS-SS2LS-4Y-PPP-A	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 4YR - Plat Prio Plus	TAP-5KEPS-SS2LS-4Y-PPP-A	$ 1,636,588.00	$ 1,423,831.56
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 4YR - Plat Prio Plus	TAP-10KEPS-SS2LS-4Y-PPP-A	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 4YR - Plat Prio Plus	TAP-15KEPS-SS2LS-4Y-PPP-A	$ 4,091,472.00	$ 3,559,580.64
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 4YR - Plat Prio Plus	TAP-20KEPS-SS2LS-4Y-PPP-A	$ 5,455,296.00	$ 4,746,107.52
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 4YR - Plat Prio Plus	TAP-25KEPS-SS2LS-4Y-PPP-A	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 4YR - Plat Prio Plus	TAP-30KEPS-SS2LS-4Y-PPP-A	$ 8,182,944.00	$ 7,119,161.28
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 4YR - Plat Prio Plus	TAP-35KEPS-SS2LS-4Y-PPP-A	$ 9,546,768.00	$ 8,305,688.16
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 4YR - Plat Prio Plus	TAP-40KEPS-SS2LS-4Y-PPP-A	##############	$ 9,492,215.04
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 5YR - Plat Prio Plus	TAP-1KEPS-SS2LS-5Y-PPP-A	$ 1,363,825.00	$ 1,186,527.75
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 5YR - Plat Prio Plus	TAP-2.5KEPS-SS2LS-5Y-PPP-A	$ 1,704,780.00	$ 1,483,158.60
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 5YR - Plat Prio Plus	TAP-5KEPS-SS2LS-5Y-PPP-A	$ 2,045,735.00	$ 1,779,789.45
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 5YR - Plat Prio Plus	TAP-10KEPS-SS2LS-5Y-PPP-A	$ 3,409,560.00	$ 2,966,317.20
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 5YR - Plat Prio Plus	TAP-15KEPS-SS2LS-5Y-PPP-A	$ 5,114,340.00	$ 4,449,475.80
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 5YR - Plat Prio Plus	TAP-20KEPS-SS2LS-5Y-PPP-A	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 5YR - Plat Prio Plus	TAP-25KEPS-SS2LS-5Y-PPP-A	$ 8,523,900.00	$ 7,415,793.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 5YR - Plat Prio Plus	TAP-30KEPS-SS2LS-5Y-PPP-A	##############	$ 8,898,951.60
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 5YR - Plat Prio Plus	TAP-35KEPS-SS2LS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 5YR - Plat Prio Plus	TAP-40KEPS-SS2LS-5Y-PPP-A	##############	##############
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - GovUS	TAP-1KEPS-BD-1Y-US	$ 110,450.00	$ 96,091.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-BD-1Y-US	$ 118,988.00	$ 103,519.56
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - GovUS	TAP-5KEPS-BD-1Y-US	$ 121,208.00	$ 105,450.96
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - GovUS	TAP-10KEPS-BD-1Y-US	$ 148,132.00	$ 128,874.84
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - GovUS	TAP-15KEPS-BD-1Y-US	$ 222,198.00	$ 193,312.26
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - GovUS	TAP-20KEPS-BD-1Y-US	$ 265,078.00	$ 230,617.86
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - GovUS	TAP-25KEPS-BD-1Y-US	$ 314,780.00	$ 273,858.60
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - GovUS	TAP-30KEPS-BD-1Y-US	$ 377,736.00	$ 328,630.32

FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - GovUS	TAP-35KEPS-BD-1Y-US	$ 440,692.00	$ 383,402.04
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - GovUS	TAP-40KEPS-BD-1Y-US	$ 503,648.00	$ 438,173.76
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - GovUS	TAP-45KEPS-BD-1Y-US	$ 566,604.00	$ 492,945.48
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - GovUS	TAP-50KEPS-BD-1Y-US	$ 629,560.00	$ 547,717.20
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - GovUS	TAP-55KEPS-BD-1Y-US	$ 692,516.00	$ 602,488.92
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - GovUS	TAP-60KEPS-BD-1Y-US	$ 755,472.00	$ 657,260.64
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - GovUS	TAP-65KEPS-BD-1Y-US	$ 818,428.00	$ 712,032.36
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - GovUS	TAP-70KEPS-BD-1Y-US	$ 881,384.00	$ 766,804.08
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - GovUS	TAP-75KEPS-BD-1Y-US	$ 944,340.00	$ 821,575.80
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - GovUS	TAP-80KEPS-BD-1Y-US	$ 1,007,296.00	$ 876,347.52
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - GovUS	TAP-1KEPS-BD-2Y-US	$ 220,900.00	$ 192,183.00
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-BD-2Y-US	$ 237,976.00	$ 207,039.12
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - GovUS	TAP-5KEPS-BD-2Y-US	$ 242,416.00	$ 210,901.92
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - GovUS	TAP-10KEPS-BD-2Y-US	$ 296,264.00	$ 257,749.68
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - GovUS	TAP-15KEPS-BD-2Y-US	$ 444,396.00	$ 386,624.52
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - GovUS	TAP-20KEPS-BD-2Y-US	$ 530,156.00	$ 461,235.72
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - GovUS	TAP-25KEPS-BD-2Y-US	$ 629,560.00	$ 547,717.20
FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - GovUS	TAP-30KEPS-BD-2Y-US	$ 755,472.00	$ 657,260.64
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - GovUS	TAP-35KEPS-BD-2Y-US	$ 881,384.00	$ 766,804.08
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - GovUS	TAP-40KEPS-BD-2Y-US	$ 1,007,296.00	$ 876,347.52
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - GovUS	TAP-45KEPS-BD-2Y-US	$ 1,133,208.00	$ 985,890.96
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - GovUS	TAP-50KEPS-BD-2Y-US	$ 1,259,120.00	$ 1,095,434.40
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - GovUS	TAP-55KEPS-BD-2Y-US	$ 1,385,032.00	$ 1,204,977.84
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - GovUS	TAP-60KEPS-BD-2Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - GovUS	TAP-65KEPS-BD-2Y-US	$ 1,636,856.00	$ 1,424,064.72
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - GovUS	TAP-70KEPS-BD-2Y-US	$ 1,762,768.00	$ 1,533,608.16
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - GovUS	TAP-75KEPS-BD-2Y-US	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - GovUS	TAP-80KEPS-BD-2Y-US	$ 2,014,592.00	$ 1,752,695.04
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - GovUS	TAP-1KEPS-BD-3Y-US	$ 331,350.00	$ 288,274.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-BD-3Y-US	$ 356,964.00	$ 310,558.68
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - GovUS	TAP-5KEPS-BD-3Y-US	$ 363,624.00	$ 316,352.88
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - GovUS	TAP-10KEPS-BD-3Y-US	$ 444,396.00	$ 386,624.52
FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - GovUS	TAP-15KEPS-BD-3Y-US	$ 666,594.00	$ 579,936.78
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - GovUS	TAP-20KEPS-BD-3Y-US	$ 795,234.00	$ 691,853.58
FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - GovUS	TAP-25KEPS-BD-3Y-US	$ 944,340.00	$ 821,575.80
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - GovUS	TAP-30KEPS-BD-3Y-US	$ 1,133,208.00	$ 985,890.96
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - GovUS	TAP-35KEPS-BD-3Y-US	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - GovUS	TAP-40KEPS-BD-3Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - GovUS	TAP-45KEPS-BD-3Y-US	$ 1,699,812.00	$ 1,478,836.44
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - GovUS	TAP-50KEPS-BD-3Y-US	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - GovUS	TAP-55KEPS-BD-3Y-US	$ 2,077,548.00	$ 1,807,466.76
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - GovUS	TAP-60KEPS-BD-3Y-US	$ 2,266,416.00	$ 1,971,781.92
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - GovUS	TAP-65KEPS-BD-3Y-US	$ 2,455,284.00	$ 2,136,097.08
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - GovUS	TAP-70KEPS-BD-3Y-US	$ 2,644,152.00	$ 2,300,412.24
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - GovUS	TAP-75KEPS-BD-3Y-US	$ 2,833,020.00	$ 2,464,727.40
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - GovUS	TAP-80KEPS-BD-3Y-US	$ 3,021,888.00	$ 2,629,042.56
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - GovUS	TAP-1KEPS-BD-4Y-US	$ 441,800.00	$ 384,366.00
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-BD-4Y-US	$ 475,952.00	$ 414,078.24
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - GovUS	TAP-5KEPS-BD-4Y-US	$ 484,832.00	$ 421,803.84

FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - GovUS	TAP-10KEPS-BD-4Y-US	$ 592,528.00	$ 515,499.36
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - GovUS	TAP-15KEPS-BD-4Y-US	$ 888,792.00	$ 773,249.04
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - GovUS	TAP-20KEPS-BD-4Y-US	$ 1,060,312.00	$ 922,471.44
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - GovUS	TAP-25KEPS-BD-4Y-US	$ 1,259,120.00	$ 1,095,434.40
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - GovUS	TAP-30KEPS-BD-4Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - GovUS	TAP-35KEPS-BD-4Y-US	$ 1,762,768.00	$ 1,533,608.16
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - GovUS	TAP-40KEPS-BD-4Y-US	$ 2,014,592.00	$ 1,752,695.04
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - GovUS	TAP-45KEPS-BD-4Y-US	$ 2,266,416.00	$ 1,971,781.92
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - GovUS	TAP-50KEPS-BD-4Y-US	$ 2,518,240.00	$ 2,190,868.80
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - GovUS	TAP-55KEPS-BD-4Y-US	$ 2,770,064.00	$ 2,409,955.68
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - GovUS	TAP-60KEPS-BD-4Y-US	$ 3,021,888.00	$ 2,629,042.56
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - GovUS	TAP-65KEPS-BD-4Y-US	$ 3,273,712.00	$ 2,848,129.44
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - GovUS	TAP-70KEPS-BD-4Y-US	$ 3,525,536.00	$ 3,067,216.32
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - GovUS	TAP-75KEPS-BD-4Y-US	$ 3,777,360.00	$ 3,286,303.20
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - GovUS	TAP-80KEPS-BD-4Y-US	$ 4,029,184.00	$ 3,505,390.08
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - GovUS	TAP-1KEPS-BD-5Y-US	$ 552,250.00	$ 480,457.50
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-BD-5Y-US	$ 594,940.00	$ 517,597.80
FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - GovUS	TAP-5KEPS-BD-5Y-US	$ 606,040.00	$ 527,254.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - GovUS	TAP-10KEPS-BD-5Y-US	$ 740,660.00	$ 644,374.20
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - GovUS	TAP-15KEPS-BD-5Y-US	$ 1,110,990.00	$ 966,561.30
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - GovUS	TAP-20KEPS-BD-5Y-US	$ 1,325,390.00	$ 1,153,089.30
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - GovUS	TAP-25KEPS-BD-5Y-US	$ 1,573,900.00	$ 1,369,293.00
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - GovUS	TAP-30KEPS-BD-5Y-US	$ 1,888,680.00	$ 1,643,151.60
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - GovUS	TAP-35KEPS-BD-5Y-US	$ 2,203,460.00	$ 1,917,010.20
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - GovUS	TAP-40KEPS-BD-5Y-US	$ 2,518,240.00	$ 2,190,868.80
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - GovUS	TAP-45KEPS-BD-5Y-US	$ 2,833,020.00	$ 2,464,727.40
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - GovUS	TAP-50KEPS-BD-5Y-US	$ 3,147,800.00	$ 2,738,586.00
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - GovUS	TAP-55KEPS-BD-5Y-US	$ 3,462,580.00	$ 3,012,444.60
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - GovUS	TAP-60KEPS-BD-5Y-US	$ 3,777,360.00	$ 3,286,303.20
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - GovUS	TAP-65KEPS-BD-5Y-US	$ 4,092,140.00	$ 3,560,161.80
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - GovUS	TAP-70KEPS-BD-5Y-US	$ 4,406,920.00	$ 3,834,020.40
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - GovUS	TAP-75KEPS-BD-5Y-US	$ 4,721,700.00	$ 4,107,879.00
FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - GovUS	TAP-80KEPS-BD-5Y-US	$ 5,036,480.00	$ 4,381,737.60
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 1YR - GovUS	RN-TAP-1KEPS-BD-1Y-US	$ 110,450.00	$ 96,091.50
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 1YR - GovUS	RN-TAP-2.5KEPS-BD-1Y-US	$ 118,988.00	$ 103,519.56
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 1YR - GovUS	RN-TAP-5KEPS-BD-1Y-US	$ 121,208.00	$ 105,450.96
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 1YR - GovUS	RN-TAP-10KEPS-BD-1Y-US	$ 148,132.00	$ 128,874.84
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 1YR - GovUS	RN-TAP-15KEPS-BD-1Y-US	$ 222,198.00	$ 193,312.26
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 1YR - GovUS	RN-TAP-20KEPS-BD-1Y-US	$ 265,078.00	$ 230,617.86
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 1YR - GovUS	RN-TAP-25KEPS-BD-1Y-US	$ 314,780.00	$ 273,858.60
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 1YR - GovUS	RN-TAP-30KEPS-BD-1Y-US	$ 377,736.00	$ 328,630.32
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 1YR - GovUS	RN-TAP-35KEPS-BD-1Y-US	$ 440,692.00	$ 383,402.04
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 1YR - GovUS	RN-TAP-40KEPS-BD-1Y-US	$ 503,648.00	$ 438,173.76
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 1YR - GovUS	RN-TAP-45KEPS-BD-1Y-US	$ 566,604.00	$ 492,945.48
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 1YR - GovUS	RN-TAP-50KEPS-BD-1Y-US	$ 629,560.00	$ 547,717.20
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 1YR - GovUS	RN-TAP-55KEPS-BD-1Y-US	$ 692,516.00	$ 602,488.92
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 1YR - GovUS	RN-TAP-60KEPS-BD-1Y-US	$ 755,472.00	$ 657,260.64
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 1YR - GovUS	RN-TAP-65KEPS-BD-1Y-US	$ 818,428.00	$ 712,032.36
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 1YR - GovUS	RN-TAP-70KEPS-BD-1Y-US	$ 881,384.00	$ 766,804.08

FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 1YR - GovUS	RN-TAP-75KEPS-BD-1Y-US	$ 944,340.00	$ 821,575.80
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 1YR - GovUS	RN-TAP-80KEPS-BD-1Y-US	$ 1,007,296.00	$ 876,347.52
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 2YR - GovUS	RN-TAP-1KEPS-BD-2Y-US	$ 220,900.00	$ 192,183.00
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 2YR - GovUS	RN-TAP-2.5KEPS-BD-2Y-US	$ 237,976.00	$ 207,039.12
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 2YR - GovUS	RN-TAP-5KEPS-BD-2Y-US	$ 242,416.00	$ 210,901.92
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 2YR - GovUS	RN-TAP-10KEPS-BD-2Y-US	$ 296,264.00	$ 257,749.68
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 2YR - GovUS	RN-TAP-15KEPS-BD-2Y-US	$ 444,396.00	$ 386,624.52
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 2YR - GovUS	RN-TAP-20KEPS-BD-2Y-US	$ 530,156.00	$ 461,235.72
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 2YR - GovUS	RN-TAP-25KEPS-BD-2Y-US	$ 629,560.00	$ 547,717.20
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 2YR - GovUS	RN-TAP-30KEPS-BD-2Y-US	$ 755,472.00	$ 657,260.64
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 2YR - GovUS	RN-TAP-35KEPS-BD-2Y-US	$ 881,384.00	$ 766,804.08
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 2YR - GovUS	RN-TAP-40KEPS-BD-2Y-US	$ 1,007,296.00	$ 876,347.52
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 2YR - GovUS	RN-TAP-45KEPS-BD-2Y-US	$ 1,133,208.00	$ 985,890.96
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 2YR - GovUS	RN-TAP-50KEPS-BD-2Y-US	$ 1,259,120.00	$ 1,095,434.40
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 2YR - GovUS	RN-TAP-55KEPS-BD-2Y-US	$ 1,385,032.00	$ 1,204,977.84
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 2YR - GovUS	RN-TAP-60KEPS-BD-2Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 2YR - GovUS	RN-TAP-65KEPS-BD-2Y-US	$ 1,636,856.00	$ 1,424,064.72
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 2YR - GovUS	RN-TAP-70KEPS-BD-2Y-US	$ 1,762,768.00	$ 1,533,608.16
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 2YR - GovUS	RN-TAP-75KEPS-BD-2Y-US	$ 1,888,680.00	$ 1,643,151.60
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 2YR - GovUS	RN-TAP-80KEPS-BD-2Y-US	$ 2,014,592.00	$ 1,752,695.04
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 3YR - GovUS	RN-TAP-1KEPS-BD-3Y-US	$ 331,350.00	$ 288,274.50
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 3YR - GovUS	RN-TAP-2.5KEPS-BD-3Y-US	$ 356,964.00	$ 310,558.68
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 3YR - GovUS	RN-TAP-5KEPS-BD-3Y-US	$ 363,624.00	$ 316,352.88
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 3YR - GovUS	RN-TAP-10KEPS-BD-3Y-US	$ 444,396.00	$ 386,624.52
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 3YR - GovUS	RN-TAP-15KEPS-BD-3Y-US	$ 666,594.00	$ 579,936.78
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 3YR - GovUS	RN-TAP-20KEPS-BD-3Y-US	$ 795,234.00	$ 691,853.58
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 3YR - GovUS	RN-TAP-25KEPS-BD-3Y-US	$ 944,340.00	$ 821,575.80
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 3YR - GovUS	RN-TAP-30KEPS-BD-3Y-US	$ 1,133,208.00	$ 985,890.96
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 3YR - GovUS	RN-TAP-35KEPS-BD-3Y-US	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 3YR - GovUS	RN-TAP-40KEPS-BD-3Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 3YR - GovUS	RN-TAP-45KEPS-BD-3Y-US	$ 1,699,812.00	$ 1,478,836.44
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 3YR - GovUS	RN-TAP-50KEPS-BD-3Y-US	$ 1,888,680.00	$ 1,643,151.60
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 3YR - GovUS	RN-TAP-55KEPS-BD-3Y-US	$ 2,077,548.00	$ 1,807,466.76
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 3YR - GovUS	RN-TAP-60KEPS-BD-3Y-US	$ 2,266,416.00	$ 1,971,781.92
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 3YR - GovUS	RN-TAP-65KEPS-BD-3Y-US	$ 2,455,284.00	$ 2,136,097.08
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 3YR - GovUS	RN-TAP-70KEPS-BD-3Y-US	$ 2,644,152.00	$ 2,300,412.24
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 3YR - GovUS	RN-TAP-75KEPS-BD-3Y-US	$ 2,833,020.00	$ 2,464,727.40
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 3YR - GovUS	RN-TAP-80KEPS-BD-3Y-US	$ 3,021,888.00	$ 2,629,042.56
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 4YR - GovUS	RN-TAP-1KEPS-BD-4Y-US	$ 441,800.00	$ 384,366.00
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 4YR - GovUS	RN-TAP-2.5KEPS-BD-4Y-US	$ 475,952.00	$ 414,078.24
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 4YR - GovUS	RN-TAP-5KEPS-BD-4Y-US	$ 484,832.00	$ 421,803.84
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 4YR - GovUS	RN-TAP-10KEPS-BD-4Y-US	$ 592,528.00	$ 515,499.36
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 4YR - GovUS	RN-TAP-15KEPS-BD-4Y-US	$ 888,792.00	$ 773,249.04
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 4YR - GovUS	RN-TAP-20KEPS-BD-4Y-US	$ 1,060,312.00	$ 922,471.44
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 4YR - GovUS	RN-TAP-25KEPS-BD-4Y-US	$ 1,259,120.00	$ 1,095,434.40
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 4YR - GovUS	RN-TAP-30KEPS-BD-4Y-US	$ 1,510,944.00	$ 1,314,521.28
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 4YR - GovUS	RN-TAP-35KEPS-BD-4Y-US	$ 1,762,768.00	$ 1,533,608.16
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 4YR - GovUS	RN-TAP-40KEPS-BD-4Y-US	$ 2,014,592.00	$ 1,752,695.04
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 4YR - GovUS	RN-TAP-45KEPS-BD-4Y-US	$ 2,266,416.00	$ 1,971,781.92

FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 4YR - GovUS	RN-TAP-50KEPS-BD-4Y-US	$ 2,518,240.00	$ 2,190,868.80
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 4YR - GovUS	RN-TAP-55KEPS-BD-4Y-US	$ 2,770,064.00	$ 2,409,955.68
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 4YR - GovUS	RN-TAP-60KEPS-BD-4Y-US	$ 3,021,888.00	$ 2,629,042.56
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 4YR - GovUS	RN-TAP-65KEPS-BD-4Y-US	$ 3,273,712.00	$ 2,848,129.44
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 4YR - GovUS	RN-TAP-70KEPS-BD-4Y-US	$ 3,525,536.00	$ 3,067,216.32
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 4YR - GovUS	RN-TAP-75KEPS-BD-4Y-US	$ 3,777,360.00	$ 3,286,303.20
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 4YR - GovUS	RN-TAP-80KEPS-BD-4Y-US	$ 4,029,184.00	$ 3,505,390.08
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-BD-1Y-USPP	$ 115,973.00	$ 100,896.51
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-BD-1Y-USPP	$ 124,937.00	$ 108,695.19
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-BD-1Y-USPP	$ 127,268.00	$ 110,723.16
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-BD-1Y-USPP	$ 155,539.00	$ 135,318.93
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-BD-1Y-USPP	$ 233,308.00	$ 202,977.96
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-BD-1Y-USPP	$ 278,332.00	$ 242,148.84
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-BD-1Y-USPP	$ 330,519.00	$ 287,551.53
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-BD-1Y-USPP	$ 396,623.00	$ 345,062.01
FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-BD-1Y-USPP	$ 462,727.00	$ 402,572.49
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-BD-1Y-USPP	$ 528,830.00	$ 460,082.10
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - GovUS Prio Plus	TAP-45KEPS-BD-1Y-USPP	$ 594,934.00	$ 517,592.58
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - GovUS Prio Plus	TAP-50KEPS-BD-1Y-USPP	$ 661,038.00	$ 575,103.06
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - GovUS Prio Plus	TAP-55KEPS-BD-1Y-USPP	$ 727,142.00	$ 632,613.54
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - GovUS Prio Plus	TAP-60KEPS-BD-1Y-USPP	$ 793,246.00	$ 690,124.02
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - GovUS Prio Plus	TAP-65KEPS-BD-1Y-USPP	$ 859,349.00	$ 747,633.63
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - GovUS Prio Plus	TAP-70KEPS-BD-1Y-USPP	$ 925,453.00	$ 805,144.11
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - GovUS Prio Plus	TAP-75KEPS-BD-1Y-USPP	$ 991,557.00	$ 862,654.59
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - GovUS Prio Plus	TAP-80KEPS-BD-1Y-USPP	$ 1,057,661.00	$ 920,165.07
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-BD-2Y-USPP	$ 231,946.00	$ 201,793.02
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-BD-2Y-USPP	$ 249,874.00	$ 217,390.38
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-BD-2Y-USPP	$ 254,536.00	$ 221,446.32
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-BD-2Y-USPP	$ 311,078.00	$ 270,637.86
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-BD-2Y-USPP	$ 466,616.00	$ 405,955.92
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-BD-2Y-USPP	$ 556,664.00	$ 484,297.68
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-BD-2Y-USPP	$ 661,038.00	$ 575,103.06
FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-BD-2Y-USPP	$ 793,246.00	$ 690,124.02
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-BD-2Y-USPP	$ 925,454.00	$ 805,144.98
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-BD-2Y-USPP	$ 1,057,660.00	$ 920,164.20
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - GovUS Prio Plus	TAP-45KEPS-BD-2Y-USPP	$ 1,189,868.00	$ 1,035,185.16
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - GovUS Prio Plus	TAP-50KEPS-BD-2Y-USPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - GovUS Prio Plus	TAP-55KEPS-BD-2Y-USPP	$ 1,454,284.00	$ 1,265,227.08
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - GovUS Prio Plus	TAP-60KEPS-BD-2Y-USPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - GovUS Prio Plus	TAP-65KEPS-BD-2Y-USPP	$ 1,718,698.00	$ 1,495,267.26
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - GovUS Prio Plus	TAP-70KEPS-BD-2Y-USPP	$ 1,850,906.00	$ 1,610,288.22
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - GovUS Prio Plus	TAP-75KEPS-BD-2Y-USPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - GovUS Prio Plus	TAP-80KEPS-BD-2Y-USPP	$ 2,115,322.00	$ 1,840,330.14
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-BD-3Y-USPP	$ 347,919.00	$ 302,689.53
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-BD-3Y-USPP	$ 374,811.00	$ 326,085.57
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-BD-3Y-USPP	$ 381,804.00	$ 332,169.48
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-BD-3Y-USPP	$ 466,617.00	$ 405,956.79
FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-BD-3Y-USPP	$ 699,924.00	$ 608,933.88
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-BD-3Y-USPP	$ 834,996.00	$ 726,446.52

FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-BD-3Y-USPP	$ 991,557.00	$ 862,654.59
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-BD-3Y-USPP	$ 1,189,869.00	$ 1,035,186.03
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-BD-3Y-USPP	$ 1,388,181.00	$ 1,207,717.47
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-BD-3Y-USPP	$ 1,586,490.00	$ 1,380,246.30
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - GovUS Prio Plus	TAP-45KEPS-BD-3Y-USPP	$ 1,784,802.00	$ 1,552,777.74
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - GovUS Prio Plus	TAP-50KEPS-BD-3Y-USPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - GovUS Prio Plus	TAP-55KEPS-BD-3Y-USPP	$ 2,181,426.00	$ 1,897,840.62
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - GovUS Prio Plus	TAP-60KEPS-BD-3Y-USPP	$ 2,379,738.00	$ 2,070,372.06
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - GovUS Prio Plus	TAP-65KEPS-BD-3Y-USPP	$ 2,578,047.00	$ 2,242,900.89
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - GovUS Prio Plus	TAP-70KEPS-BD-3Y-USPP	$ 2,776,359.00	$ 2,415,432.33
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - GovUS Prio Plus	TAP-75KEPS-BD-3Y-USPP	$ 2,974,671.00	$ 2,587,963.77
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - GovUS Prio Plus	TAP-80KEPS-BD-3Y-USPP	$ 3,172,983.00	$ 2,760,495.21
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-BD-4Y-USPP	$ 463,892.00	$ 403,586.04
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-BD-4Y-USPP	$ 499,748.00	$ 434,780.76
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-BD-4Y-USPP	$ 509,072.00	$ 442,892.64
FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-BD-4Y-USPP	$ 622,156.00	$ 541,275.72
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-BD-4Y-USPP	$ 933,232.00	$ 811,911.84
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-BD-4Y-USPP	$ 1,113,328.00	$ 968,595.36
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-BD-4Y-USPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-BD-4Y-USPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-BD-4Y-USPP	$ 1,850,908.00	$ 1,610,289.96
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-BD-4Y-USPP	$ 2,115,320.00	$ 1,840,328.40
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - GovUS Prio Plus	TAP-45KEPS-BD-4Y-USPP	$ 2,379,736.00	$ 2,070,370.32
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - GovUS Prio Plus	TAP-50KEPS-BD-4Y-USPP	$ 2,644,152.00	$ 2,300,412.24
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - GovUS Prio Plus	TAP-55KEPS-BD-4Y-USPP	$ 2,908,568.00	$ 2,530,454.16
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - GovUS Prio Plus	TAP-60KEPS-BD-4Y-USPP	$ 3,172,984.00	$ 2,760,496.08
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - GovUS Prio Plus	TAP-65KEPS-BD-4Y-USPP	$ 3,437,396.00	$ 2,990,534.52
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - GovUS Prio Plus	TAP-70KEPS-BD-4Y-USPP	$ 3,701,812.00	$ 3,220,576.44
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - GovUS Prio Plus	TAP-75KEPS-BD-4Y-USPP	$ 3,966,228.00	$ 3,450,618.36
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - GovUS Prio Plus	TAP-80KEPS-BD-4Y-USPP	$ 4,230,644.00	$ 3,680,660.28
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-BD-5Y-USPP	$ 579,865.00	$ 504,482.55
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-BD-5Y-USPP	$ 624,685.00	$ 543,475.95
FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-BD-5Y-USPP	$ 636,340.00	$ 553,615.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-BD-5Y-USPP	$ 777,695.00	$ 676,594.65
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-BD-5Y-USPP	$ 1,166,540.00	$ 1,014,889.80
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-BD-5Y-USPP	$ 1,391,660.00	$ 1,210,744.20
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-BD-5Y-USPP	$ 1,652,595.00	$ 1,437,757.65
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-BD-5Y-USPP	$ 1,983,115.00	$ 1,725,310.05
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-BD-5Y-USPP	$ 2,313,635.00	$ 2,012,862.45
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-BD-5Y-USPP	$ 2,644,150.00	$ 2,300,410.50
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - GovUS Prio Plus	TAP-45KEPS-BD-5Y-USPP	$ 2,974,670.00	$ 2,587,962.90
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - GovUS Prio Plus	TAP-50KEPS-BD-5Y-USPP	$ 3,305,190.00	$ 2,875,515.30
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - GovUS Prio Plus	TAP-55KEPS-BD-5Y-USPP	$ 3,635,710.00	$ 3,163,067.70
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - GovUS Prio Plus	TAP-60KEPS-BD-5Y-USPP	$ 3,966,230.00	$ 3,450,620.10
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - GovUS Prio Plus	TAP-65KEPS-BD-5Y-USPP	$ 4,296,745.00	$ 3,738,168.15
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - GovUS Prio Plus	TAP-70KEPS-BD-5Y-USPP	$ 4,627,265.00	$ 4,025,720.55
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - GovUS Prio Plus	TAP-75KEPS-BD-5Y-USPP	$ 4,957,785.00	$ 4,313,272.95
FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - GovUS Prio Plus	TAP-80KEPS-BD-5Y-USPP	$ 5,288,305.00	$ 4,600,825.35
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 1YR - GovUS Prio Plus	RN-TAP-1KEPS-BD-1Y-USPP	$ 115,973.00	$ 100,896.51

FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 1YR - GovUS Prio Plus	RN-TAP-2.5KEPS-BD-1Y-USPP	$ 124,937.00	$ 108,695.19
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 1YR - GovUS Prio Plus	RN-TAP-5KEPS-BD-1Y-USPP	$ 127,268.00	$ 110,723.16
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 1YR - GovUS Prio Plus	RN-TAP-10KEPS-BD-1Y-USPP	$ 155,539.00	$ 135,318.93
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 1YR - GovUS Prio Plus	RN-TAP-15KEPS-BD-1Y-USPP	$ 233,308.00	$ 202,977.96
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 1YR - GovUS Prio Plus	RN-TAP-20KEPS-BD-1Y-USPP	$ 278,332.00	$ 242,148.84
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 1YR - GovUS Prio Plus	RN-TAP-25KEPS-BD-1Y-USPP	$ 330,519.00	$ 287,551.53
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 1YR - GovUS Prio Plus	RN-TAP-30KEPS-BD-1Y-USPP	$ 396,623.00	$ 345,062.01
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 1YR - GovUS Prio Plus	RN-TAP-35KEPS-BD-1Y-USPP	$ 462,727.00	$ 402,572.49
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 1YR - GovUS Prio Plus	RN-TAP-40KEPS-BD-1Y-USPP	$ 528,830.00	$ 460,082.10
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 1YR - GovUS Prio Plus	RN-TAP-45KEPS-BD-1Y-USPP	$ 594,934.00	$ 517,592.58
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 1YR - GovUS Prio Plus	RN-TAP-50KEPS-BD-1Y-USPP	$ 661,038.00	$ 575,103.06
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 1YR - GovUS Prio Plus	RN-TAP-55KEPS-BD-1Y-USPP	$ 727,142.00	$ 632,613.54
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 1YR - GovUS Prio Plus	RN-TAP-60KEPS-BD-1Y-USPP	$ 793,246.00	$ 690,124.02
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 1YR - GovUS Prio Plus	RN-TAP-65KEPS-BD-1Y-USPP	$ 859,349.00	$ 747,633.63
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 1YR - GovUS Prio Plus	RN-TAP-70KEPS-BD-1Y-USPP	$ 925,453.00	$ 805,144.11
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 1YR - GovUS Prio Plus	RN-TAP-75KEPS-BD-1Y-USPP	$ 991,557.00	$ 862,654.59
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 1YR - GovUS Prio Plus	RN-TAP-80KEPS-BD-1Y-USPP	$ 1,057,661.00	$ 920,165.07
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 2YR - GovUS Prio Plus	RN-TAP-1KEPS-BD-2Y-USPP	$ 231,946.00	$ 201,793.02
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 2YR - GovUS Prio Plus	RN-TAP-2.5KEPS-BD-2Y-USPP	$ 249,874.00	$ 217,390.38
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 2YR - GovUS Prio Plus	RN-TAP-5KEPS-BD-2Y-USPP	$ 254,536.00	$ 221,446.32
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 2YR - GovUS Prio Plus	RN-TAP-10KEPS-BD-2Y-USPP	$ 311,078.00	$ 270,637.86
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 2YR - GovUS Prio Plus	RN-TAP-15KEPS-BD-2Y-USPP	$ 466,616.00	$ 405,955.92
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 2YR - GovUS Prio Plus	RN-TAP-20KEPS-BD-2Y-USPP	$ 556,664.00	$ 484,297.68
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 2YR - GovUS Prio Plus	RN-TAP-25KEPS-BD-2Y-USPP	$ 661,038.00	$ 575,103.06
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 2YR - GovUS Prio Plus	RN-TAP-30KEPS-BD-2Y-USPP	$ 793,246.00	$ 690,124.02
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 2YR - GovUS Prio Plus	RN-TAP-35KEPS-BD-2Y-USPP	$ 925,454.00	$ 805,144.98
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 2YR - GovUS Prio Plus	RN-TAP-40KEPS-BD-2Y-USPP	$ 1,057,660.00	$ 920,164.20
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 2YR - GovUS Prio Plus	RN-TAP-45KEPS-BD-2Y-USPP	$ 1,189,868.00	$ 1,035,185.16
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 2YR - GovUS Prio Plus	RN-TAP-50KEPS-BD-2Y-USPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 2YR - GovUS Prio Plus	RN-TAP-55KEPS-BD-2Y-USPP	$ 1,454,284.00	$ 1,265,227.08
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 2YR - GovUS Prio Plus	RN-TAP-60KEPS-BD-2Y-USPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 2YR - GovUS Prio Plus	RN-TAP-65KEPS-BD-2Y-USPP	$ 1,718,698.00	$ 1,495,267.26
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 2YR - GovUS Prio Plus	RN-TAP-70KEPS-BD-2Y-USPP	$ 1,850,906.00	$ 1,610,288.22
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 2YR - GovUS Prio Plus	RN-TAP-75KEPS-BD-2Y-USPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 2YR - GovUS Prio Plus	RN-TAP-80KEPS-BD-2Y-USPP	$ 2,115,322.00	$ 1,840,330.14
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 3YR - GovUS Prio Plus	RN-TAP-1KEPS-BD-3Y-USPP	$ 347,919.00	$ 302,689.53
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 3YR - GovUS Prio Plus	RN-TAP-2.5KEPS-BD-3Y-USPP	$ 374,811.00	$ 326,085.57
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 3YR - GovUS Prio Plus	RN-TAP-5KEPS-BD-3Y-USPP	$ 381,804.00	$ 332,169.48
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 3YR - GovUS Prio Plus	RN-TAP-10KEPS-BD-3Y-USPP	$ 466,617.00	$ 405,956.79
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 3YR - GovUS Prio Plus	RN-TAP-15KEPS-BD-3Y-USPP	$ 699,924.00	$ 608,933.88
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 3YR - GovUS Prio Plus	RN-TAP-20KEPS-BD-3Y-USPP	$ 834,996.00	$ 726,446.52
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 3YR - GovUS Prio Plus	RN-TAP-25KEPS-BD-3Y-USPP	$ 991,557.00	$ 862,654.59
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 3YR - GovUS Prio Plus	RN-TAP-30KEPS-BD-3Y-USPP	$ 1,189,869.00	$ 1,035,186.03
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 3YR - GovUS Prio Plus	RN-TAP-35KEPS-BD-3Y-USPP	$ 1,388,181.00	$ 1,207,717.47
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 3YR - GovUS Prio Plus	RN-TAP-40KEPS-BD-3Y-USPP	$ 1,586,490.00	$ 1,380,246.30
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 3YR - GovUS Prio Plus	RN-TAP-45KEPS-BD-3Y-USPP	$ 1,784,802.00	$ 1,552,777.74
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 3YR - GovUS Prio Plus	RN-TAP-50KEPS-BD-3Y-USPP	$ 1,983,114.00	$ 1,725,309.18
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 3YR - GovUS Prio Plus	RN-TAP-55KEPS-BD-3Y-USPP	$ 2,181,426.00	$ 1,897,840.62
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 3YR - GovUS Prio Plus	RN-TAP-60KEPS-BD-3Y-USPP	$ 2,379,738.00	$ 2,070,372.06

FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 3YR - GovUS Prio Plus	RN-TAP-65KEPS-BD-3Y-USPP	$ 2,578,047.00	$ 2,242,900.89
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 3YR - GovUS Prio Plus	RN-TAP-70KEPS-BD-3Y-USPP	$ 2,776,359.00	$ 2,415,432.33
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 3YR - GovUS Prio Plus	RN-TAP-75KEPS-BD-3Y-USPP	$ 2,974,671.00	$ 2,587,963.77
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 3YR - GovUS Prio Plus	RN-TAP-80KEPS-BD-3Y-USPP	$ 3,172,983.00	$ 2,760,495.21
FireEye	Renewal-Threat Analytics Platform Base Detect 1K events/sec 4YR - GovUS Prio Plus	RN-TAP-1KEPS-BD-4Y-USPP	$ 463,892.00	$ 403,586.04
FireEye	Renewal-Threat Analytics Platform Base Detect 2.5K events/sec 4YR - GovUS Prio Plus	RN-TAP-2.5KEPS-BD-4Y-USPP	$ 499,748.00	$ 434,780.76
FireEye	Renewal-Threat Analytics Platform Base Detect 5K events/sec 4YR - GovUS Prio Plus	RN-TAP-5KEPS-BD-4Y-USPP	$ 509,072.00	$ 442,892.64
FireEye	Renewal-Threat Analytics Platform Base Detect 10K events/sec 4YR - GovUS Prio Plus	RN-TAP-10KEPS-BD-4Y-USPP	$ 622,156.00	$ 541,275.72
FireEye	Renewal-Threat Analytics Platform Base Detect 15K events/sec 4YR - GovUS Prio Plus	RN-TAP-15KEPS-BD-4Y-USPP	$ 933,232.00	$ 811,911.84
FireEye	Renewal-Threat Analytics Platform Base Detect 20K events/sec 4YR - GovUS Prio Plus	RN-TAP-20KEPS-BD-4Y-USPP	$ 1,113,328.00	$ 968,595.36
FireEye	Renewal-Threat Analytics Platform Base Detect 25K events/sec 4YR - GovUS Prio Plus	RN-TAP-25KEPS-BD-4Y-USPP	$ 1,322,076.00	$ 1,150,206.12
FireEye	Renewal-Threat Analytics Platform Base Detect 30K events/sec 4YR - GovUS Prio Plus	RN-TAP-30KEPS-BD-4Y-USPP	$ 1,586,492.00	$ 1,380,248.04
FireEye	Renewal-Threat Analytics Platform Base Detect 35K events/sec 4YR - GovUS Prio Plus	RN-TAP-35KEPS-BD-4Y-USPP	$ 1,850,908.00	$ 1,610,289.96
FireEye	Renewal-Threat Analytics Platform Base Detect 40K events/sec 4YR - GovUS Prio Plus	RN-TAP-40KEPS-BD-4Y-USPP	$ 2,115,320.00	$ 1,840,328.40
FireEye	Renewal-Threat Analytics Platform Base Detect 45K events/sec 4YR - GovUS Prio Plus	RN-TAP-45KEPS-BD-4Y-USPP	$ 2,379,736.00	$ 2,070,370.32
FireEye	Renewal-Threat Analytics Platform Base Detect 50K events/sec 4YR - GovUS Prio Plus	RN-TAP-50KEPS-BD-4Y-USPP	$ 2,644,152.00	$ 2,300,412.24
FireEye	Renewal-Threat Analytics Platform Base Detect 55K events/sec 4YR - GovUS Prio Plus	RN-TAP-55KEPS-BD-4Y-USPP	$ 2,908,568.00	$ 2,530,454.16
FireEye	Renewal-Threat Analytics Platform Base Detect 60K events/sec 4YR - GovUS Prio Plus	RN-TAP-60KEPS-BD-4Y-USPP	$ 3,172,984.00	$ 2,760,496.08
FireEye	Renewal-Threat Analytics Platform Base Detect 65K events/sec 4YR - GovUS Prio Plus	RN-TAP-65KEPS-BD-4Y-USPP	$ 3,437,396.00	$ 2,990,534.52
FireEye	Renewal-Threat Analytics Platform Base Detect 70K events/sec 4YR - GovUS Prio Plus	RN-TAP-70KEPS-BD-4Y-USPP	$ 3,701,812.00	$ 3,220,576.44
FireEye	Renewal-Threat Analytics Platform Base Detect 75K events/sec 4YR - GovUS Prio Plus	RN-TAP-75KEPS-BD-4Y-USPP	$ 3,966,228.00	$ 3,450,618.36
FireEye	Renewal-Threat Analytics Platform Base Detect 80K events/sec 4YR - GovUS Prio Plus	RN-TAP-80KEPS-BD-4Y-USPP	$ 4,230,644.00	$ 3,680,660.28
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - GovUS	TAP-1KEPS-SS-1Y-US	$ 232,635.00	$ 202,392.45
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-SS-1Y-US	$ 276,258.00	$ 240,344.46
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - GovUS	TAP-5KEPS-SS-1Y-US	$ 314,613.00	$ 273,713.31
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - GovUS	TAP-10KEPS-SS-1Y-US	$ 475,966.00	$ 414,090.42
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - GovUS	TAP-15KEPS-SS-1Y-US	$ 713,949.00	$ 621,135.63
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - GovUS	TAP-20KEPS-SS-1Y-US	$ 951,932.00	$ 828,180.84
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - GovUS	TAP-25KEPS-SS-1Y-US	$ 1,189,915.00	$ 1,035,226.05
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - GovUS	TAP-30KEPS-SS-1Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - GovUS	TAP-35KEPS-SS-1Y-US	$ 1,665,881.00	$ 1,449,316.47
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - GovUS	TAP-40KEPS-SS-1Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - GovUS	TAP-45KEPS-SS-1Y-US	$ 2,141,847.00	$ 1,863,406.89
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - GovUS	TAP-50KEPS-SS-1Y-US	$ 2,379,830.00	$ 2,070,452.10
FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - GovUS	TAP-55KEPS-SS-1Y-US	$ 2,617,813.00	$ 2,277,497.31
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - GovUS	TAP-60KEPS-SS-1Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - GovUS	TAP-65KEPS-SS-1Y-US	$ 3,093,779.00	$ 2,691,587.73
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - GovUS	TAP-70KEPS-SS-1Y-US	$ 3,331,762.00	$ 2,898,632.94
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - GovUS	TAP-75KEPS-SS-1Y-US	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - GovUS	TAP-80KEPS-SS-1Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - GovUS	TAP-1KEPS-SS-2Y-US	$ 465,270.00	$ 404,784.90
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-SS-2Y-US	$ 552,516.00	$ 480,688.92
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - GovUS	TAP-5KEPS-SS-2Y-US	$ 629,226.00	$ 547,426.62
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - GovUS	TAP-10KEPS-SS-2Y-US	$ 951,932.00	$ 828,180.84
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - GovUS	TAP-15KEPS-SS-2Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - GovUS	TAP-20KEPS-SS-2Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - GovUS	TAP-25KEPS-SS-2Y-US	$ 2,379,830.00	$ 2,070,452.10
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - GovUS	TAP-30KEPS-SS-2Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - GovUS	TAP-35KEPS-SS-2Y-US	$ 3,331,762.00	$ 2,898,632.94

FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - GovUS	TAP-40KEPS-SS-2Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - GovUS	TAP-45KEPS-SS-2Y-US	$ 4,283,694.00	$ 3,726,813.78
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - GovUS	TAP-50KEPS-SS-2Y-US	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - GovUS	TAP-55KEPS-SS-2Y-US	$ 5,235,626.00	$ 4,554,994.62
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - GovUS	TAP-60KEPS-SS-2Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - GovUS	TAP-65KEPS-SS-2Y-US	$ 6,187,558.00	$ 5,383,175.46
FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - GovUS	TAP-70KEPS-SS-2Y-US	$ 6,663,524.00	$ 5,797,265.88
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - GovUS	TAP-75KEPS-SS-2Y-US	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - GovUS	TAP-80KEPS-SS-2Y-US	$ 7,615,456.00	$ 6,625,446.72
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - GovUS	TAP-1KEPS-SS-3Y-US	$ 697,905.00	$ 607,177.35
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-SS-3Y-US	$ 828,774.00	$ 721,033.38
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - GovUS	TAP-5KEPS-SS-3Y-US	$ 943,839.00	$ 821,139.93
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - GovUS	TAP-10KEPS-SS-3Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - GovUS	TAP-15KEPS-SS-3Y-US	$ 2,141,847.00	$ 1,863,406.89
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - GovUS	TAP-20KEPS-SS-3Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - GovUS	TAP-25KEPS-SS-3Y-US	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - GovUS	TAP-30KEPS-SS-3Y-US	$ 4,283,694.00	$ 3,726,813.78
FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - GovUS	TAP-35KEPS-SS-3Y-US	$ 4,997,643.00	$ 4,347,949.41
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - GovUS	TAP-40KEPS-SS-3Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - GovUS	TAP-45KEPS-SS-3Y-US	$ 6,425,541.00	$ 5,590,220.67
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - GovUS	TAP-50KEPS-SS-3Y-US	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - GovUS	TAP-55KEPS-SS-3Y-US	$ 7,853,439.00	$ 6,832,491.93
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - GovUS	TAP-60KEPS-SS-3Y-US	$ 8,567,388.00	$ 7,453,627.56
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - GovUS	TAP-65KEPS-SS-3Y-US	$ 9,281,337.00	$ 8,074,763.19
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - GovUS	TAP-70KEPS-SS-3Y-US	$ 9,995,286.00	$ 8,695,898.82
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - GovUS	TAP-75KEPS-SS-3Y-US	##############	$ 9,317,034.45
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - GovUS	TAP-80KEPS-SS-3Y-US	##############	$ 9,938,170.08
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - GovUS	TAP-1KEPS-SS-4Y-US	$ 930,540.00	$ 809,569.80
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-SS-4Y-US	$ 1,105,032.00	$ 961,377.84
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - GovUS	TAP-5KEPS-SS-4Y-US	$ 1,258,452.00	$ 1,094,853.24
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - GovUS	TAP-10KEPS-SS-4Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - GovUS	TAP-15KEPS-SS-4Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - GovUS	TAP-20KEPS-SS-4Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - GovUS	TAP-25KEPS-SS-4Y-US	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - GovUS	TAP-30KEPS-SS-4Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - GovUS	TAP-35KEPS-SS-4Y-US	$ 6,663,524.00	$ 5,797,265.88
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - GovUS	TAP-40KEPS-SS-4Y-US	$ 7,615,456.00	$ 6,625,446.72
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - GovUS	TAP-45KEPS-SS-4Y-US	$ 8,567,388.00	$ 7,453,627.56
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - GovUS	TAP-50KEPS-SS-4Y-US	$ 9,519,320.00	$ 8,281,808.40
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - GovUS	TAP-55KEPS-SS-4Y-US	##############	$ 9,109,989.24
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - GovUS	TAP-60KEPS-SS-4Y-US	##############	$ 9,938,170.08
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - GovUS	TAP-65KEPS-SS-4Y-US	##############	##############
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - GovUS	TAP-70KEPS-SS-4Y-US	##############	##############
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - GovUS	TAP-75KEPS-SS-4Y-US	##############	##############
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - GovUS	TAP-80KEPS-SS-4Y-US	##############	##############
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - GovUS	TAP-1KEPS-SS-5Y-US	$ 1,163,175.00	$ 1,011,962.25
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-SS-5Y-US	$ 1,381,290.00	$ 1,201,722.30
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - GovUS	TAP-5KEPS-SS-5Y-US	$ 1,573,065.00	$ 1,368,566.55
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - GovUS	TAP-10KEPS-SS-5Y-US	$ 2,379,830.00	$ 2,070,452.10

FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - GovUS	TAP-15KEPS-SS-5Y-US	$ 3,569,745.00	$ 3,105,678.15
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - GovUS	TAP-20KEPS-SS-5Y-US	$ 4,759,660.00	$ 4,140,904.20
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - GovUS	TAP-25KEPS-SS-5Y-US	$ 5,949,575.00	$ 5,176,130.25
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - GovUS	TAP-30KEPS-SS-5Y-US	$ 7,139,490.00	$ 6,211,356.30
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - GovUS	TAP-35KEPS-SS-5Y-US	$ 8,329,405.00	$ 7,246,582.35
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - GovUS	TAP-40KEPS-SS-5Y-US	$ 9,519,320.00	$ 8,281,808.40
FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - GovUS	TAP-45KEPS-SS-5Y-US	############	$ 9,317,034.45
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - GovUS	TAP-50KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - GovUS	TAP-55KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - GovUS	TAP-60KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - GovUS	TAP-65KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - GovUS	TAP-70KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - GovUS	TAP-75KEPS-SS-5Y-US	############	############
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - GovUS	TAP-80KEPS-SS-5Y-US	############	############
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 1YR - GovUS	RN-TAP-1KEPS-SS-1Y-US	$ 232,635.00	$ 202,392.45
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 1YR - GovUS	RN-TAP-2.5KEPS-SS-1Y-US	$ 276,258.00	$ 240,344.46
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 1YR - GovUS	RN-TAP-5KEPS-SS-1Y-US	$ 314,613.00	$ 273,713.31
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 1YR - GovUS	RN-TAP-10KEPS-SS-1Y-US	$ 475,966.00	$ 414,090.42
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 1YR - GovUS	RN-TAP-15KEPS-SS-1Y-US	$ 713,949.00	$ 621,135.63
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 1YR - GovUS	RN-TAP-20KEPS-SS-1Y-US	$ 951,932.00	$ 828,180.84
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 1YR - GovUS	RN-TAP-25KEPS-SS-1Y-US	$ 1,189,915.00	$ 1,035,226.05
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 1YR - GovUS	RN-TAP-30KEPS-SS-1Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 1YR - GovUS	RN-TAP-35KEPS-SS-1Y-US	$ 1,665,881.00	$ 1,449,316.47
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 1YR - GovUS	RN-TAP-40KEPS-SS-1Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 1YR - GovUS	RN-TAP-45KEPS-SS-1Y-US	$ 2,141,847.00	$ 1,863,406.89
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 1YR - GovUS	RN-TAP-50KEPS-SS-1Y-US	$ 2,379,830.00	$ 2,070,452.10
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 1YR - GovUS	RN-TAP-55KEPS-SS-1Y-US	$ 2,617,813.00	$ 2,277,497.31
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 1YR - GovUS	RN-TAP-60KEPS-SS-1Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 1YR - GovUS	RN-TAP-65KEPS-SS-1Y-US	$ 3,093,779.00	$ 2,691,587.73
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 1YR - GovUS	RN-TAP-70KEPS-SS-1Y-US	$ 3,331,762.00	$ 2,898,632.94
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 1YR - GovUS	RN-TAP-75KEPS-SS-1Y-US	$ 3,569,745.00	$ 3,105,678.15
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 1YR - GovUS	RN-TAP-80KEPS-SS-1Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 2YR - GovUS	RN-TAP-1KEPS-SS-2Y-US	$ 465,270.00	$ 404,784.90
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 2YR - GovUS	RN-TAP-2.5KEPS-SS-2Y-US	$ 552,516.00	$ 480,688.92
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 2YR - GovUS	RN-TAP-5KEPS-SS-2Y-US	$ 629,226.00	$ 547,426.62
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 2YR - GovUS	RN-TAP-10KEPS-SS-2Y-US	$ 951,932.00	$ 828,180.84
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 2YR - GovUS	RN-TAP-15KEPS-SS-2Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 2YR - GovUS	RN-TAP-20KEPS-SS-2Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 2YR - GovUS	RN-TAP-25KEPS-SS-2Y-US	$ 2,379,830.00	$ 2,070,452.10
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 2YR - GovUS	RN-TAP-30KEPS-SS-2Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 2YR - GovUS	RN-TAP-35KEPS-SS-2Y-US	$ 3,331,762.00	$ 2,898,632.94
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 2YR - GovUS	RN-TAP-40KEPS-SS-2Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 2YR - GovUS	RN-TAP-45KEPS-SS-2Y-US	$ 4,283,694.00	$ 3,726,813.78
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 2YR - GovUS	RN-TAP-50KEPS-SS-2Y-US	$ 4,759,660.00	$ 4,140,904.20
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 2YR - GovUS	RN-TAP-55KEPS-SS-2Y-US	$ 5,235,626.00	$ 4,554,994.62
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 2YR - GovUS	RN-TAP-60KEPS-SS-2Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 2YR - GovUS	RN-TAP-65KEPS-SS-2Y-US	$ 6,187,558.00	$ 5,383,175.46
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 2YR - GovUS	RN-TAP-70KEPS-SS-2Y-US	$ 6,663,524.00	$ 5,797,265.88
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 2YR - GovUS	RN-TAP-75KEPS-SS-2Y-US	$ 7,139,490.00	$ 6,211,356.30

FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 2YR - GovUS	RN-TAP-80KEPS-SS-2Y-US	$ 7,615,456.00	$ 6,625,446.72
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 3YR - GovUS	RN-TAP-1KEPS-SS-3Y-US	$ 697,905.00	$ 607,177.35
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 3YR - GovUS	RN-TAP-2.5KEPS-SS-3Y-US	$ 828,774.00	$ 721,033.38
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 3YR - GovUS	RN-TAP-5KEPS-SS-3Y-US	$ 943,839.00	$ 821,139.93
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 3YR - GovUS	RN-TAP-10KEPS-SS-3Y-US	$ 1,427,898.00	$ 1,242,271.26
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 3YR - GovUS	RN-TAP-15KEPS-SS-3Y-US	$ 2,141,847.00	$ 1,863,406.89
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 3YR - GovUS	RN-TAP-20KEPS-SS-3Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 3YR - GovUS	RN-TAP-25KEPS-SS-3Y-US	$ 3,569,745.00	$ 3,105,678.15
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 3YR - GovUS	RN-TAP-30KEPS-SS-3Y-US	$ 4,283,694.00	$ 3,726,813.78
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 3YR - GovUS	RN-TAP-35KEPS-SS-3Y-US	$ 4,997,643.00	$ 4,347,949.41
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 3YR - GovUS	RN-TAP-40KEPS-SS-3Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 3YR - GovUS	RN-TAP-45KEPS-SS-3Y-US	$ 6,425,541.00	$ 5,590,220.67
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 3YR - GovUS	RN-TAP-50KEPS-SS-3Y-US	$ 7,139,490.00	$ 6,211,356.30
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 3YR - GovUS	RN-TAP-55KEPS-SS-3Y-US	$ 7,853,439.00	$ 6,832,491.93
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 3YR - GovUS	RN-TAP-60KEPS-SS-3Y-US	$ 8,567,388.00	$ 7,453,627.56
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 3YR - GovUS	RN-TAP-65KEPS-SS-3Y-US	$ 9,281,337.00	$ 8,074,763.19
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 3YR - GovUS	RN-TAP-70KEPS-SS-3Y-US	$ 9,995,286.00	$ 8,695,898.82
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 3YR - GovUS	RN-TAP-75KEPS-SS-3Y-US	##############	$ 9,317,034.45
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 3YR - GovUS	RN-TAP-80KEPS-SS-3Y-US	##############	$ 9,938,170.08
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 4YR - GovUS	RN-TAP-1KEPS-SS-4Y-US	$ 930,540.00	$ 809,569.80
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 4YR - GovUS	RN-TAP-2.5KEPS-SS-4Y-US	$ 1,105,032.00	$ 961,377.84
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 4YR - GovUS	RN-TAP-5KEPS-SS-4Y-US	$ 1,258,452.00	$ 1,094,853.24
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 4YR - GovUS	RN-TAP-10KEPS-SS-4Y-US	$ 1,903,864.00	$ 1,656,361.68
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 4YR - GovUS	RN-TAP-15KEPS-SS-4Y-US	$ 2,855,796.00	$ 2,484,542.52
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 4YR - GovUS	RN-TAP-20KEPS-SS-4Y-US	$ 3,807,728.00	$ 3,312,723.36
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 4YR - GovUS	RN-TAP-25KEPS-SS-4Y-US	$ 4,759,660.00	$ 4,140,904.20
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 4YR - GovUS	RN-TAP-30KEPS-SS-4Y-US	$ 5,711,592.00	$ 4,969,085.04
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 4YR - GovUS	RN-TAP-35KEPS-SS-4Y-US	$ 6,663,524.00	$ 5,797,265.88
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 4YR - GovUS	RN-TAP-40KEPS-SS-4Y-US	$ 7,615,456.00	$ 6,625,446.72
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 4YR - GovUS	RN-TAP-45KEPS-SS-4Y-US	$ 8,567,388.00	$ 7,453,627.56
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 4YR - GovUS	RN-TAP-50KEPS-SS-4Y-US	$ 9,519,320.00	$ 8,281,808.40
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 4YR - GovUS	RN-TAP-55KEPS-SS-4Y-US	##############	$ 9,109,989.24
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 4YR - GovUS	RN-TAP-60KEPS-SS-4Y-US	##############	$ 9,938,170.08
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 4YR - GovUS	RN-TAP-65KEPS-SS-4Y-US	##############	##############
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 4YR - GovUS	RN-TAP-70KEPS-SS-4Y-US	##############	##############
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 4YR - GovUS	RN-TAP-75KEPS-SS-4Y-US	##############	##############
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 4YR - GovUS	RN-TAP-80KEPS-SS-4Y-US	##############	##############
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-SS-1Y-USPP	$ 244,267.00	$ 212,512.29
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-SS-1Y-USPP	$ 290,071.00	$ 252,361.77
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-SS-1Y-USPP	$ 330,344.00	$ 287,399.28
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-SS-1Y-USPP	$ 499,764.00	$ 434,794.68
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-SS-1Y-USPP	$ 749,646.00	$ 652,192.02
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-SS-1Y-USPP	$ 999,529.00	$ 869,590.23
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-SS-1Y-USPP	$ 1,249,411.00	$ 1,086,987.57
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-SS-1Y-USPP	$ 1,499,293.00	$ 1,304,384.91
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-SS-1Y-USPP	$ 1,749,175.00	$ 1,521,782.25
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-SS-1Y-USPP	$ 1,999,057.00	$ 1,739,179.59
FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - GovUS Prio Plus	TAP-45KEPS-SS-1Y-USPP	$ 2,248,939.00	$ 1,956,576.93
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - GovUS Prio Plus	TAP-50KEPS-SS-1Y-USPP	$ 2,498,822.00	$ 2,173,975.14

FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - GovUS Prio Plus	TAP-55KEPS-SS-1Y-USPP	$ 2,748,704.00	$ 2,391,372.48
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - GovUS Prio Plus	TAP-60KEPS-SS-1Y-USPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - GovUS Prio Plus	TAP-65KEPS-SS-1Y-USPP	$ 3,248,468.00	$ 2,826,167.16
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - GovUS Prio Plus	TAP-70KEPS-SS-1Y-USPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - GovUS Prio Plus	TAP-75KEPS-SS-1Y-USPP	$ 3,748,232.00	$ 3,260,961.84
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - GovUS Prio Plus	TAP-80KEPS-SS-1Y-USPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-SS-2Y-USPP	$ 488,534.00	$ 425,024.58
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-SS-2Y-USPP	$ 580,142.00	$ 504,723.54
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-SS-2Y-USPP	$ 660,688.00	$ 574,798.56
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-SS-2Y-USPP	$ 999,528.00	$ 869,589.36
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-SS-2Y-USPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-SS-2Y-USPP	$ 1,999,058.00	$ 1,739,180.46
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-SS-2Y-USPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-SS-2Y-USPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-SS-2Y-USPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-SS-2Y-USPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - GovUS Prio Plus	TAP-45KEPS-SS-2Y-USPP	$ 4,497,878.00	$ 3,913,153.86
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - GovUS Prio Plus	TAP-50KEPS-SS-2Y-USPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - GovUS Prio Plus	TAP-55KEPS-SS-2Y-USPP	$ 5,497,408.00	$ 4,782,744.96
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - GovUS Prio Plus	TAP-60KEPS-SS-2Y-USPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - GovUS Prio Plus	TAP-65KEPS-SS-2Y-USPP	$ 6,496,936.00	$ 5,652,334.32
FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - GovUS Prio Plus	TAP-70KEPS-SS-2Y-USPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - GovUS Prio Plus	TAP-75KEPS-SS-2Y-USPP	$ 7,496,464.00	$ 6,521,923.68
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - GovUS Prio Plus	TAP-80KEPS-SS-2Y-USPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-SS-3Y-USPP	$ 732,801.00	$ 637,536.87
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-SS-3Y-USPP	$ 870,213.00	$ 757,085.31
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-SS-3Y-USPP	$ 991,032.00	$ 862,197.84
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-SS-3Y-USPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-SS-3Y-USPP	$ 2,248,938.00	$ 1,956,576.06
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-SS-3Y-USPP	$ 2,998,587.00	$ 2,608,770.69
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-SS-3Y-USPP	$ 3,748,233.00	$ 3,260,962.71
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-SS-3Y-USPP	$ 4,497,879.00	$ 3,913,154.73
FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-SS-3Y-USPP	$ 5,247,525.00	$ 4,565,346.75
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-SS-3Y-USPP	$ 5,997,171.00	$ 5,217,538.77
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - GovUS Prio Plus	TAP-45KEPS-SS-3Y-USPP	$ 6,746,817.00	$ 5,869,730.79
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - GovUS Prio Plus	TAP-50KEPS-SS-3Y-USPP	$ 7,496,466.00	$ 6,521,925.42
FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - GovUS Prio Plus	TAP-55KEPS-SS-3Y-USPP	$ 8,246,112.00	$ 7,174,117.44
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - GovUS Prio Plus	TAP-60KEPS-SS-3Y-USPP	$ 8,995,758.00	$ 7,826,309.46
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - GovUS Prio Plus	TAP-65KEPS-SS-3Y-USPP	$ 9,745,404.00	$ 8,478,501.48
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - GovUS Prio Plus	TAP-70KEPS-SS-3Y-USPP	##############	$ 9,130,693.50
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - GovUS Prio Plus	TAP-75KEPS-SS-3Y-USPP	##############	$ 9,782,885.52
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - GovUS Prio Plus	TAP-80KEPS-SS-3Y-USPP	##############	##############
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-SS-4Y-USPP	$ 977,068.00	$ 850,049.16
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-SS-4Y-USPP	$ 1,160,284.00	$ 1,009,447.08
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-SS-4Y-USPP	$ 1,321,376.00	$ 1,149,597.12
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-SS-4Y-USPP	$ 1,999,056.00	$ 1,739,178.72
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-SS-4Y-USPP	$ 2,998,584.00	$ 2,608,768.08
FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-SS-4Y-USPP	$ 3,998,116.00	$ 3,478,360.92
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-SS-4Y-USPP	$ 4,997,644.00	$ 4,347,950.28

FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-SS-4Y-USPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-SS-4Y-USPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-SS-4Y-USPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - GovUS Prio Plus	TAP-45KEPS-SS-4Y-USPP	$ 8,995,756.00	$ 7,826,307.72
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - GovUS Prio Plus	TAP-50KEPS-SS-4Y-USPP	$ 9,995,288.00	$ 8,695,900.56
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - GovUS Prio Plus	TAP-55KEPS-SS-4Y-USPP	##########	$ 9,565,489.92
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - GovUS Prio Plus	TAP-60KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - GovUS Prio Plus	TAP-65KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - GovUS Prio Plus	TAP-70KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - GovUS Prio Plus	TAP-75KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - GovUS Prio Plus	TAP-80KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-SS-5Y-USPP	$ 1,221,335.00	$ 1,062,561.45
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-SS-5Y-USPP	$ 1,450,355.00	$ 1,261,808.85
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-SS-5Y-USPP	$ 1,651,720.00	$ 1,436,996.40
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-SS-5Y-USPP	$ 2,498,820.00	$ 2,173,973.40
FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-SS-5Y-USPP	$ 3,748,230.00	$ 3,260,960.10
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-SS-5Y-USPP	$ 4,997,645.00	$ 4,347,951.15
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-SS-5Y-USPP	$ 6,247,055.00	$ 5,434,937.85
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-SS-5Y-USPP	$ 7,496,465.00	$ 6,521,924.55
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-SS-5Y-USPP	$ 8,745,875.00	$ 7,608,911.25
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-SS-5Y-USPP	$ 9,995,285.00	$ 8,695,897.95
FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - GovUS Prio Plus	TAP-45KEPS-SS-5Y-USPP	##########	$ 9,782,884.65
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - GovUS Prio Plus	TAP-50KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - GovUS Prio Plus	TAP-55KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - GovUS Prio Plus	TAP-60KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - GovUS Prio Plus	TAP-65KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - GovUS Prio Plus	TAP-70KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - GovUS Prio Plus	TAP-75KEPS-SS-5Y-USPP	##########	##########
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - GovUS Prio Plus	TAP-80KEPS-SS-5Y-USPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 1YR - GovUS Prio Plus	RN-TAP-1KEPS-SS-1Y-USPP	$ 244,267.00	$ 212,512.29
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 1YR - GovUS Prio Plus	RN-TAP-2.5KEPS-SS-1Y-USPP	$ 290,071.00	$ 252,361.77
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 1YR - GovUS Prio Plus	RN-TAP-5KEPS-SS-1Y-USPP	$ 330,344.00	$ 287,399.28
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 1YR - GovUS Prio Plus	RN-TAP-10KEPS-SS-1Y-USPP	$ 499,764.00	$ 434,794.68
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 1YR - GovUS Prio Plus	RN-TAP-15KEPS-SS-1Y-USPP	$ 749,646.00	$ 652,192.02
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 1YR - GovUS Prio Plus	RN-TAP-20KEPS-SS-1Y-USPP	$ 999,529.00	$ 869,590.23
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 1YR - GovUS Prio Plus	RN-TAP-25KEPS-SS-1Y-USPP	$ 1,249,411.00	$ 1,086,987.57
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 1YR - GovUS Prio Plus	RN-TAP-30KEPS-SS-1Y-USPP	$ 1,499,293.00	$ 1,304,384.91
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 1YR - GovUS Prio Plus	RN-TAP-35KEPS-SS-1Y-USPP	$ 1,749,175.00	$ 1,521,782.25
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 1YR - GovUS Prio Plus	RN-TAP-40KEPS-SS-1Y-USPP	$ 1,999,057.00	$ 1,739,179.59
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 1YR - GovUS Prio Plus	RN-TAP-45KEPS-SS-1Y-USPP	$ 2,248,939.00	$ 1,956,576.93
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 1YR - GovUS Prio Plus	RN-TAP-50KEPS-SS-1Y-USPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 1YR - GovUS Prio Plus	RN-TAP-55KEPS-SS-1Y-USPP	$ 2,748,704.00	$ 2,391,372.48
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 1YR - GovUS Prio Plus	RN-TAP-60KEPS-SS-1Y-USPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 1YR - GovUS Prio Plus	RN-TAP-65KEPS-SS-1Y-USPP	$ 3,248,468.00	$ 2,826,167.16
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 1YR - GovUS Prio Plus	RN-TAP-70KEPS-SS-1Y-USPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 1YR - GovUS Prio Plus	RN-TAP-75KEPS-SS-1Y-USPP	$ 3,748,232.00	$ 3,260,961.84
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 1YR - GovUS Prio Plus	RN-TAP-80KEPS-SS-1Y-USPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 2YR - GovUS Prio Plus	RN-TAP-1KEPS-SS-2Y-USPP	$ 488,534.00	$ 425,024.58
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 2YR - GovUS Prio Plus	RN-TAP-2.5KEPS-SS-2Y-USPP	$ 580,142.00	$ 504,723.54

FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 2YR - GovUS Prio Plus	RN-TAP-5KEPS-SS-2Y-USPP	$ 660,688.00	$ 574,798.56
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 2YR - GovUS Prio Plus	RN-TAP-10KEPS-SS-2Y-USPP	$ 999,528.00	$ 869,589.36
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 2YR - GovUS Prio Plus	RN-TAP-15KEPS-SS-2Y-USPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 2YR - GovUS Prio Plus	RN-TAP-20KEPS-SS-2Y-USPP	$ 1,999,058.00	$ 1,739,180.46
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 2YR - GovUS Prio Plus	RN-TAP-25KEPS-SS-2Y-USPP	$ 2,498,822.00	$ 2,173,975.14
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 2YR - GovUS Prio Plus	RN-TAP-30KEPS-SS-2Y-USPP	$ 2,998,586.00	$ 2,608,769.82
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 2YR - GovUS Prio Plus	RN-TAP-35KEPS-SS-2Y-USPP	$ 3,498,350.00	$ 3,043,564.50
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 2YR - GovUS Prio Plus	RN-TAP-40KEPS-SS-2Y-USPP	$ 3,998,114.00	$ 3,478,359.18
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 2YR - GovUS Prio Plus	RN-TAP-45KEPS-SS-2Y-USPP	$ 4,497,878.00	$ 3,913,153.86
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 2YR - GovUS Prio Plus	RN-TAP-50KEPS-SS-2Y-USPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 2YR - GovUS Prio Plus	RN-TAP-55KEPS-SS-2Y-USPP	$ 5,497,408.00	$ 4,782,744.96
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 2YR - GovUS Prio Plus	RN-TAP-60KEPS-SS-2Y-USPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 2YR - GovUS Prio Plus	RN-TAP-65KEPS-SS-2Y-USPP	$ 6,496,936.00	$ 5,652,334.32
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 2YR - GovUS Prio Plus	RN-TAP-70KEPS-SS-2Y-USPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 2YR - GovUS Prio Plus	RN-TAP-75KEPS-SS-2Y-USPP	$ 7,496,464.00	$ 6,521,923.68
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 2YR - GovUS Prio Plus	RN-TAP-80KEPS-SS-2Y-USPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 3YR - GovUS Prio Plus	RN-TAP-1KEPS-SS-3Y-USPP	$ 732,801.00	$ 637,536.87
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 3YR - GovUS Prio Plus	RN-TAP-2.5KEPS-SS-3Y-USPP	$ 870,213.00	$ 757,085.31
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 3YR - GovUS Prio Plus	RN-TAP-5KEPS-SS-3Y-USPP	$ 991,032.00	$ 862,197.84
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 3YR - GovUS Prio Plus	RN-TAP-10KEPS-SS-3Y-USPP	$ 1,499,292.00	$ 1,304,384.04
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 3YR - GovUS Prio Plus	RN-TAP-15KEPS-SS-3Y-USPP	$ 2,248,938.00	$ 1,956,576.06
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 3YR - GovUS Prio Plus	RN-TAP-20KEPS-SS-3Y-USPP	$ 2,998,587.00	$ 2,608,770.69
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 3YR - GovUS Prio Plus	RN-TAP-25KEPS-SS-3Y-USPP	$ 3,748,233.00	$ 3,260,962.71
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 3YR - GovUS Prio Plus	RN-TAP-30KEPS-SS-3Y-USPP	$ 4,497,879.00	$ 3,913,154.73
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 3YR - GovUS Prio Plus	RN-TAP-35KEPS-SS-3Y-USPP	$ 5,247,525.00	$ 4,565,346.75
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 3YR - GovUS Prio Plus	RN-TAP-40KEPS-SS-3Y-USPP	$ 5,997,171.00	$ 5,217,538.77
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 3YR - GovUS Prio Plus	RN-TAP-45KEPS-SS-3Y-USPP	$ 6,746,817.00	$ 5,869,730.79
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 3YR - GovUS Prio Plus	RN-TAP-50KEPS-SS-3Y-USPP	$ 7,496,466.00	$ 6,521,925.42
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 3YR - GovUS Prio Plus	RN-TAP-55KEPS-SS-3Y-USPP	$ 8,246,112.00	$ 7,174,117.44
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 3YR - GovUS Prio Plus	RN-TAP-60KEPS-SS-3Y-USPP	$ 8,995,758.00	$ 7,826,309.46
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 3YR - GovUS Prio Plus	RN-TAP-65KEPS-SS-3Y-USPP	$ 9,745,404.00	$ 8,478,501.48
FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 3YR - GovUS Prio Plus	RN-TAP-70KEPS-SS-3Y-USPP	##############	$ 9,130,693.50
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 3YR - GovUS Prio Plus	RN-TAP-75KEPS-SS-3Y-USPP	##############	$ 9,782,885.52
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 3YR - GovUS Prio Plus	RN-TAP-80KEPS-SS-3Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Short Search 1K events/sec 4YR - GovUS Prio Plus	RN-TAP-1KEPS-SS-4Y-USPP	$ 977,068.00	$ 850,049.16
FireEye	Renewal-Threat Analytics Platform Short Search 2.5K events/sec 4YR - GovUS Prio Plus	RN-TAP-2.5KEPS-SS-4Y-USPP	$ 1,160,284.00	$ 1,009,447.08
FireEye	Renewal-Threat Analytics Platform Short Search 5K events/sec 4YR - GovUS Prio Plus	RN-TAP-5KEPS-SS-4Y-USPP	$ 1,321,376.00	$ 1,149,597.12
FireEye	Renewal-Threat Analytics Platform Short Search 10K events/sec 4YR - GovUS Prio Plus	RN-TAP-10KEPS-SS-4Y-USPP	$ 1,999,056.00	$ 1,739,178.72
FireEye	Renewal-Threat Analytics Platform Short Search 15K events/sec 4YR - GovUS Prio Plus	RN-TAP-15KEPS-SS-4Y-USPP	$ 2,998,584.00	$ 2,608,768.08
FireEye	Renewal-Threat Analytics Platform Short Search 20K events/sec 4YR - GovUS Prio Plus	RN-TAP-20KEPS-SS-4Y-USPP	$ 3,998,116.00	$ 3,478,360.92
FireEye	Renewal-Threat Analytics Platform Short Search 25K events/sec 4YR - GovUS Prio Plus	RN-TAP-25KEPS-SS-4Y-USPP	$ 4,997,644.00	$ 4,347,950.28
FireEye	Renewal-Threat Analytics Platform Short Search 30K events/sec 4YR - GovUS Prio Plus	RN-TAP-30KEPS-SS-4Y-USPP	$ 5,997,172.00	$ 5,217,539.64
FireEye	Renewal-Threat Analytics Platform Short Search 35K events/sec 4YR - GovUS Prio Plus	RN-TAP-35KEPS-SS-4Y-USPP	$ 6,996,700.00	$ 6,087,129.00
FireEye	Renewal-Threat Analytics Platform Short Search 40K events/sec 4YR - GovUS Prio Plus	RN-TAP-40KEPS-SS-4Y-USPP	$ 7,996,228.00	$ 6,956,718.36
FireEye	Renewal-Threat Analytics Platform Short Search 45K events/sec 4YR - GovUS Prio Plus	RN-TAP-45KEPS-SS-4Y-USPP	$ 8,995,756.00	$ 7,826,307.72
FireEye	Renewal-Threat Analytics Platform Short Search 50K events/sec 4YR - GovUS Prio Plus	RN-TAP-50KEPS-SS-4Y-USPP	$ 9,995,288.00	$ 8,695,900.56
FireEye	Renewal-Threat Analytics Platform Short Search 55K events/sec 4YR - GovUS Prio Plus	RN-TAP-55KEPS-SS-4Y-USPP	##############	$ 9,565,489.92
FireEye	Renewal-Threat Analytics Platform Short Search 60K events/sec 4YR - GovUS Prio Plus	RN-TAP-60KEPS-SS-4Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Short Search 65K events/sec 4YR - GovUS Prio Plus	RN-TAP-65KEPS-SS-4Y-USPP	##############	##############

FireEye	Renewal-Threat Analytics Platform Short Search 70K events/sec 4YR - GovUS Prio Plus	RN-TAP-70KEPS-SS-4Y-USPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 75K events/sec 4YR - GovUS Prio Plus	RN-TAP-75KEPS-SS-4Y-USPP	##########	##########
FireEye	Renewal-Threat Analytics Platform Short Search 80K events/sec 4YR - GovUS Prio Plus	RN-TAP-80KEPS-SS-4Y-USPP	##########	##########
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - GovUS	TAP-1KEPS-LS-1Y-US	$ 492,411.00	$ 428,397.57
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-LS-1Y-US	$ 600,978.00	$ 522,850.86
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - GovUS	TAP-5KEPS-LS-1Y-US	$ 704,277.00	$ 612,720.99
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - GovUS	TAP-10KEPS-LS-1Y-US	$ 1,125,406.00	$ 979,103.22
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - GovUS	TAP-15KEPS-LS-1Y-US	$ 1,688,109.00	$ 1,468,654.83
FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - GovUS	TAP-20KEPS-LS-1Y-US	$ 2,250,812.00	$ 1,958,206.44
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - GovUS	TAP-25KEPS-LS-1Y-US	$ 2,813,515.00	$ 2,447,758.05
FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - GovUS	TAP-30KEPS-LS-1Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - GovUS	TAP-35KEPS-LS-1Y-US	$ 3,938,921.00	$ 3,426,861.27
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - GovUS	TAP-40KEPS-LS-1Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - GovUS	TAP-1KEPS-LS-2Y-US	$ 984,822.00	$ 856,795.14
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-LS-2Y-US	$ 1,201,956.00	$ 1,045,701.72
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - GovUS	TAP-5KEPS-LS-2Y-US	$ 1,408,554.00	$ 1,225,441.98
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - GovUS	TAP-10KEPS-LS-2Y-US	$ 2,250,812.00	$ 1,958,206.44
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - GovUS	TAP-15KEPS-LS-2Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - GovUS	TAP-20KEPS-LS-2Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - GovUS	TAP-25KEPS-LS-2Y-US	$ 5,627,030.00	$ 4,895,516.10
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - GovUS	TAP-30KEPS-LS-2Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - GovUS	TAP-35KEPS-LS-2Y-US	$ 7,877,842.00	$ 6,853,722.54
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - GovUS	TAP-40KEPS-LS-2Y-US	$ 9,003,248.00	$ 7,832,825.76
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - GovUS	TAP-1KEPS-LS-3Y-US	$ 1,477,233.00	$ 1,285,192.71
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-LS-3Y-US	$ 1,802,934.00	$ 1,568,552.58
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - GovUS	TAP-5KEPS-LS-3Y-US	$ 2,112,831.00	$ 1,838,162.97
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - GovUS	TAP-10KEPS-LS-3Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - GovUS	TAP-15KEPS-LS-3Y-US	$ 5,064,327.00	$ 4,405,964.49
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - GovUS	TAP-20KEPS-LS-3Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - GovUS	TAP-25KEPS-LS-3Y-US	$ 8,440,545.00	$ 7,343,274.15
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - GovUS	TAP-30KEPS-LS-3Y-US	##########	$ 8,811,928.98
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - GovUS	TAP-35KEPS-LS-3Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - GovUS	TAP-40KEPS-LS-3Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - GovUS	TAP-1KEPS-LS-4Y-US	$ 1,969,644.00	$ 1,713,590.28
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-LS-4Y-US	$ 2,403,912.00	$ 2,091,403.44
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - GovUS	TAP-5KEPS-LS-4Y-US	$ 2,817,108.00	$ 2,450,883.96
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - GovUS	TAP-10KEPS-LS-4Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - GovUS	TAP-15KEPS-LS-4Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - GovUS	TAP-20KEPS-LS-4Y-US	$ 9,003,248.00	$ 7,832,825.76
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - GovUS	TAP-25KEPS-LS-4Y-US	##########	$ 9,791,032.20
FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - GovUS	TAP-30KEPS-LS-4Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - GovUS	TAP-35KEPS-LS-4Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - GovUS	TAP-40KEPS-LS-4Y-US	##########	##########
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - GovUS	TAP-1KEPS-LS-5Y-US	$ 2,462,055.00	$ 2,141,987.85
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-LS-5Y-US	$ 3,004,890.00	$ 2,614,254.30
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - GovUS	TAP-5KEPS-LS-5Y-US	$ 3,521,385.00	$ 3,063,604.95
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - GovUS	TAP-10KEPS-LS-5Y-US	$ 5,627,030.00	$ 4,895,516.10
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - GovUS	TAP-15KEPS-LS-5Y-US	$ 8,440,545.00	$ 7,343,274.15
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - GovUS	TAP-20KEPS-LS-5Y-US	##########	$ 9,791,032.20

FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - GovUS	TAP-25KEPS-LS-5Y-US	############	############
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - GovUS	TAP-30KEPS-LS-5Y-US	############	############
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - GovUS	TAP-35KEPS-LS-5Y-US	############	############
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - GovUS	TAP-40KEPS-LS-5Y-US	############	############
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 1YR - GovUS	RN-TAP-1KEPS-LS-1Y-US	$ 492,411.00	$ 428,397.57
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 1YR - GovUS	RN-TAP-2.5KEPS-LS-1Y-US	$ 600,978.00	$ 522,850.86
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 1YR - GovUS	RN-TAP-5KEPS-LS-1Y-US	$ 704,277.00	$ 612,720.99
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 1YR - GovUS	RN-TAP-10KEPS-LS-1Y-US	$ 1,125,406.00	$ 979,103.22
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 1YR - GovUS	RN-TAP-15KEPS-LS-1Y-US	$ 1,688,109.00	$ 1,468,654.83
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 1YR - GovUS	RN-TAP-20KEPS-LS-1Y-US	$ 2,250,812.00	$ 1,958,206.44
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 1YR - GovUS	RN-TAP-25KEPS-LS-1Y-US	$ 2,813,515.00	$ 2,447,758.05
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 1YR - GovUS	RN-TAP-30KEPS-LS-1Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 1YR - GovUS	RN-TAP-35KEPS-LS-1Y-US	$ 3,938,921.00	$ 3,426,861.27
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 1YR - GovUS	RN-TAP-40KEPS-LS-1Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 2YR - GovUS	RN-TAP-1KEPS-LS-2Y-US	$ 984,822.00	$ 856,795.14
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 2YR - GovUS	RN-TAP-2.5KEPS-LS-2Y-US	$ 1,201,956.00	$ 1,045,701.72
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 2YR - GovUS	RN-TAP-5KEPS-LS-2Y-US	$ 1,408,554.00	$ 1,225,441.98
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 2YR - GovUS	RN-TAP-10KEPS-LS-2Y-US	$ 2,250,812.00	$ 1,958,206.44
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 2YR - GovUS	RN-TAP-15KEPS-LS-2Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 2YR - GovUS	RN-TAP-20KEPS-LS-2Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 2YR - GovUS	RN-TAP-25KEPS-LS-2Y-US	$ 5,627,030.00	$ 4,895,516.10
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 2YR - GovUS	RN-TAP-30KEPS-LS-2Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 2YR - GovUS	RN-TAP-35KEPS-LS-2Y-US	$ 7,877,842.00	$ 6,853,722.54
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 2YR - GovUS	RN-TAP-40KEPS-LS-2Y-US	$ 9,003,248.00	$ 7,832,825.76
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 3YR - GovUS	RN-TAP-1KEPS-LS-3Y-US	$ 1,477,233.00	$ 1,285,192.71
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 3YR - GovUS	RN-TAP-2.5KEPS-LS-3Y-US	$ 1,802,934.00	$ 1,568,552.58
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 3YR - GovUS	RN-TAP-5KEPS-LS-3Y-US	$ 2,112,831.00	$ 1,838,162.97
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 3YR - GovUS	RN-TAP-10KEPS-LS-3Y-US	$ 3,376,218.00	$ 2,937,309.66
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 3YR - GovUS	RN-TAP-15KEPS-LS-3Y-US	$ 5,064,327.00	$ 4,405,964.49
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 3YR - GovUS	RN-TAP-20KEPS-LS-3Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 3YR - GovUS	RN-TAP-25KEPS-LS-3Y-US	$ 8,440,545.00	$ 7,343,274.15
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 3YR - GovUS	RN-TAP-30KEPS-LS-3Y-US	############	$ 8,811,928.98
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 3YR - GovUS	RN-TAP-35KEPS-LS-3Y-US	############	############
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 3YR - GovUS	RN-TAP-40KEPS-LS-3Y-US	############	############
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 4YR - GovUS	RN-TAP-1KEPS-LS-4Y-US	$ 1,969,644.00	$ 1,713,590.28
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 4YR - GovUS	RN-TAP-2.5KEPS-LS-4Y-US	$ 2,403,912.00	$ 2,091,403.44
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 4YR - GovUS	RN-TAP-5KEPS-LS-4Y-US	$ 2,817,108.00	$ 2,450,883.96
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 4YR - GovUS	RN-TAP-10KEPS-LS-4Y-US	$ 4,501,624.00	$ 3,916,412.88
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 4YR - GovUS	RN-TAP-15KEPS-LS-4Y-US	$ 6,752,436.00	$ 5,874,619.32
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 4YR - GovUS	RN-TAP-20KEPS-LS-4Y-US	$ 9,003,248.00	$ 7,832,825.76
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 4YR - GovUS	RN-TAP-25KEPS-LS-4Y-US	############	$ 9,791,032.20
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 4YR - GovUS	RN-TAP-30KEPS-LS-4Y-US	############	############
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 4YR - GovUS	RN-TAP-35KEPS-LS-4Y-US	############	############
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 4YR - GovUS	RN-TAP-40KEPS-LS-4Y-US	############	############
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-LS-1Y-USPP	$ 517,032.00	$ 449,817.84
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-LS-1Y-USPP	$ 631,027.00	$ 548,993.49
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-LS-1Y-USPP	$ 739,491.00	$ 643,357.17
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-LS-1Y-USPP	$ 1,181,676.00	$ 1,028,058.12
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-LS-1Y-USPP	$ 1,772,514.00	$ 1,542,087.18

FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-LS-1Y-USPP	$ 2,363,353.00	$ 2,056,117.11
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-LS-1Y-USPP	$ 2,954,191.00	$ 2,570,146.17
FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-LS-1Y-USPP	$ 3,545,029.00	$ 3,084,175.23
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-LS-1Y-USPP	$ 4,135,867.00	$ 3,598,204.29
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-LS-1Y-USPP	$ 4,726,705.00	$ 4,112,233.35
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-LS-2Y-USPP	$ 1,034,064.00	$ 899,635.68
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-LS-2Y-USPP	$ 1,262,054.00	$ 1,097,986.98
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-LS-2Y-USPP	$ 1,478,982.00	$ 1,286,714.34
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-LS-2Y-USPP	$ 2,363,352.00	$ 2,056,116.24
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-LS-2Y-USPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-LS-2Y-USPP	$ 4,726,706.00	$ 4,112,234.22
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-LS-2Y-USPP	$ 5,908,382.00	$ 5,140,292.34
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-LS-2Y-USPP	$ 7,090,058.00	$ 6,168,350.46
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-LS-2Y-USPP	$ 8,271,734.00	$ 7,196,408.58
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-LS-2Y-USPP	$ 9,453,410.00	$ 8,224,466.70
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-LS-3Y-USPP	$ 1,551,096.00	$ 1,349,453.52
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-LS-3Y-USPP	$ 1,893,081.00	$ 1,646,980.47
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-LS-3Y-USPP	$ 2,218,473.00	$ 1,930,071.51
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-LS-3Y-USPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-LS-3Y-USPP	$ 5,317,542.00	$ 4,626,261.54
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-LS-3Y-USPP	$ 7,090,059.00	$ 6,168,351.33
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-LS-3Y-USPP	$ 8,862,573.00	$ 7,710,438.51
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-LS-3Y-USPP	##############	$ 9,252,525.69
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-LS-3Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-LS-3Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-LS-4Y-USPP	$ 2,068,128.00	$ 1,799,271.36
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-LS-4Y-USPP	$ 2,524,108.00	$ 2,195,973.96
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-LS-4Y-USPP	$ 2,957,964.00	$ 2,573,428.68
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-LS-4Y-USPP	$ 4,726,704.00	$ 4,112,232.48
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-LS-4Y-USPP	$ 7,090,056.00	$ 6,168,348.72
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-LS-4Y-USPP	$ 9,453,412.00	$ 8,224,468.44
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-LS-4Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-LS-4Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-LS-4Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-LS-4Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-LS-5Y-USPP	$ 2,585,160.00	$ 2,249,089.20
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-LS-5Y-USPP	$ 3,155,135.00	$ 2,744,967.45
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-LS-5Y-USPP	$ 3,697,455.00	$ 3,216,785.85
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-LS-5Y-USPP	$ 5,908,380.00	$ 5,140,290.60
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-LS-5Y-USPP	$ 8,862,570.00	$ 7,710,435.90
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-LS-5Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-LS-5Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-LS-5Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-LS-5Y-USPP	##############	##############
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-LS-5Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 1YR - GovUS Prio Plus	RN-TAP-1KEPS-LS-1Y-USPP	$ 517,032.00	$ 449,817.84
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 1YR - GovUS Prio Plus	RN-TAP-2.5KEPS-LS-1Y-USPP	$ 631,027.00	$ 548,993.49
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 1YR - GovUS Prio Plus	RN-TAP-5KEPS-LS-1Y-USPP	$ 739,491.00	$ 643,357.17
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 1YR - GovUS Prio Plus	RN-TAP-10KEPS-LS-1Y-USPP	$ 1,181,676.00	$ 1,028,058.12

FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 1YR - GovUS Prio Plus	RN-TAP-15KEPS-LS-1Y-USPP	$ 1,772,514.00	$ 1,542,087.18
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 1YR - GovUS Prio Plus	RN-TAP-20KEPS-LS-1Y-USPP	$ 2,363,353.00	$ 2,056,117.11
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 1YR - GovUS Prio Plus	RN-TAP-25KEPS-LS-1Y-USPP	$ 2,954,191.00	$ 2,570,146.17
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 1YR - GovUS Prio Plus	RN-TAP-30KEPS-LS-1Y-USPP	$ 3,545,029.00	$ 3,084,175.23
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 1YR - GovUS Prio Plus	RN-TAP-35KEPS-LS-1Y-USPP	$ 4,135,867.00	$ 3,598,204.29
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 1YR - GovUS Prio Plus	RN-TAP-40KEPS-LS-1Y-USPP	$ 4,726,705.00	$ 4,112,233.35
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 2YR - GovUS Prio Plus	RN-TAP-1KEPS-LS-2Y-USPP	$ 1,034,064.00	$ 899,635.68
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 2YR - GovUS Prio Plus	RN-TAP-2.5KEPS-LS-2Y-USPP	$ 1,262,054.00	$ 1,097,986.98
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 2YR - GovUS Prio Plus	RN-TAP-5KEPS-LS-2Y-USPP	$ 1,478,982.00	$ 1,286,714.34
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 2YR - GovUS Prio Plus	RN-TAP-10KEPS-LS-2Y-USPP	$ 2,363,352.00	$ 2,056,116.24
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 2YR - GovUS Prio Plus	RN-TAP-15KEPS-LS-2Y-USPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 2YR - GovUS Prio Plus	RN-TAP-20KEPS-LS-2Y-USPP	$ 4,726,706.00	$ 4,112,234.22
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 2YR - GovUS Prio Plus	RN-TAP-25KEPS-LS-2Y-USPP	$ 5,908,382.00	$ 5,140,292.34
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 2YR - GovUS Prio Plus	RN-TAP-30KEPS-LS-2Y-USPP	$ 7,090,058.00	$ 6,168,350.46
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 2YR - GovUS Prio Plus	RN-TAP-35KEPS-LS-2Y-USPP	$ 8,271,734.00	$ 7,196,408.58
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 2YR - GovUS Prio Plus	RN-TAP-40KEPS-LS-2Y-USPP	$ 9,453,410.00	$ 8,224,466.70
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 3YR - GovUS Prio Plus	RN-TAP-1KEPS-LS-3Y-USPP	$ 1,551,096.00	$ 1,349,453.52
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 3YR - GovUS Prio Plus	RN-TAP-2.5KEPS-LS-3Y-USPP	$ 1,893,081.00	$ 1,646,980.47
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 3YR - GovUS Prio Plus	RN-TAP-5KEPS-LS-3Y-USPP	$ 2,218,473.00	$ 1,930,071.51
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 3YR - GovUS Prio Plus	RN-TAP-10KEPS-LS-3Y-USPP	$ 3,545,028.00	$ 3,084,174.36
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 3YR - GovUS Prio Plus	RN-TAP-15KEPS-LS-3Y-USPP	$ 5,317,542.00	$ 4,626,261.54
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 3YR - GovUS Prio Plus	RN-TAP-20KEPS-LS-3Y-USPP	$ 7,090,059.00	$ 6,168,351.33
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 3YR - GovUS Prio Plus	RN-TAP-25KEPS-LS-3Y-USPP	$ 8,862,573.00	$ 7,710,438.51
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 3YR - GovUS Prio Plus	RN-TAP-30KEPS-LS-3Y-USPP	##############	$ 9,252,525.69
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 3YR - GovUS Prio Plus	RN-TAP-35KEPS-LS-3Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 3YR - GovUS Prio Plus	RN-TAP-40KEPS-LS-3Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 1K events/sec 4YR - GovUS Prio Plus	RN-TAP-1KEPS-LS-4Y-USPP	$ 2,068,128.00	$ 1,799,271.36
FireEye	Renewal-Threat Analytics Platform Long Search 2.5K events/sec 4YR - GovUS Prio Plus	RN-TAP-2.5KEPS-LS-4Y-USPP	$ 2,524,108.00	$ 2,195,973.96
FireEye	Renewal-Threat Analytics Platform Long Search 5K events/sec 4YR - GovUS Prio Plus	RN-TAP-5KEPS-LS-4Y-USPP	$ 2,957,964.00	$ 2,573,428.68
FireEye	Renewal-Threat Analytics Platform Long Search 10K events/sec 4YR - GovUS Prio Plus	RN-TAP-10KEPS-LS-4Y-USPP	$ 4,726,704.00	$ 4,112,232.48
FireEye	Renewal-Threat Analytics Platform Long Search 15K events/sec 4YR - GovUS Prio Plus	RN-TAP-15KEPS-LS-4Y-USPP	$ 7,090,056.00	$ 6,168,348.72
FireEye	Renewal-Threat Analytics Platform Long Search 20K events/sec 4YR - GovUS Prio Plus	RN-TAP-20KEPS-LS-4Y-USPP	$ 9,453,412.00	$ 8,224,468.44
FireEye	Renewal-Threat Analytics Platform Long Search 25K events/sec 4YR - GovUS Prio Plus	RN-TAP-25KEPS-LS-4Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 30K events/sec 4YR - GovUS Prio Plus	RN-TAP-30KEPS-LS-4Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 35K events/sec 4YR - GovUS Prio Plus	RN-TAP-35KEPS-LS-4Y-USPP	##############	##############
FireEye	Renewal-Threat Analytics Platform Long Search 40K events/sec 4YR - GovUS Prio Plus	RN-TAP-40KEPS-LS-4Y-USPP	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 1YR - GovUS	TAP-1KEPS-DT2SS-1Y-US-A	$ 122,185.00	$ 106,300.95
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-DT2SS-1Y-US-A	$ 157,270.00	$ 136,824.90
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 1YR - GovUS	TAP-5KEPS-DT2SS-1Y-US-A	$ 193,405.00	$ 168,262.35
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 1YR - GovUS	TAP-10KEPS-DT2SS-1Y-US-A	$ 327,834.00	$ 285,215.58
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 1YR - GovUS	TAP-15KEPS-DT2SS-1Y-US-A	$ 491,751.00	$ 427,823.37
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 1YR - GovUS	TAP-20KEPS-DT2SS-1Y-US-A	$ 686,854.00	$ 597,562.98
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 1YR - GovUS	TAP-25KEPS-DT2SS-1Y-US-A	$ 875,135.00	$ 761,367.45
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 1YR - GovUS	TAP-30KEPS-DT2SS-1Y-US-A	$ 1,050,162.00	$ 913,640.94
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 1YR - GovUS	TAP-35KEPS-DT2SS-1Y-US-A	$ 1,225,189.00	$ 1,065,914.43
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 1YR - GovUS	TAP-40KEPS-DT2SS-1Y-US-A	$ 1,400,216.00	$ 1,218,187.92
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 1YR - GovUS	TAP-45KEPS-DT2SS-1Y-US-A	$ 1,575,243.00	$ 1,370,461.41
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 1YR - GovUS	TAP-50KEPS-DT2SS-1Y-US-A	$ 1,750,270.00	$ 1,522,734.90
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 1YR - GovUS	TAP-55KEPS-DT2SS-1Y-US-A	$ 1,925,297.00	$ 1,675,008.39

FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 1YR - GovUS	TAP-60KEPS-DT2SS-1Y-US-A	$ 2,100,324.00	$ 1,827,281.88
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 1YR - GovUS	TAP-65KEPS-DT2SS-1Y-US-A	$ 2,275,351.00	$ 1,979,555.37
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 1YR - GovUS	TAP-70KEPS-DT2SS-1Y-US-A	$ 2,450,378.00	$ 2,131,828.86
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 1YR - GovUS	TAP-75KEPS-DT2SS-1Y-US-A	$ 2,625,405.00	$ 2,284,102.35
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 1YR - GovUS	TAP-80KEPS-DT2SS-1Y-US-A	$ 2,800,432.00	$ 2,436,375.84
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 2YR - GovUS	TAP-1KEPS-DT2SS-2Y-US-A	$ 244,370.00	$ 212,601.90
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-DT2SS-2Y-US-A	$ 314,540.00	$ 273,649.80
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 2YR - GovUS	TAP-5KEPS-DT2SS-2Y-US-A	$ 386,810.00	$ 336,524.70
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 2YR - GovUS	TAP-10KEPS-DT2SS-2Y-US-A	$ 655,668.00	$ 570,431.16
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 2YR - GovUS	TAP-15KEPS-DT2SS-2Y-US-A	$ 983,502.00	$ 855,646.74
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 2YR - GovUS	TAP-20KEPS-DT2SS-2Y-US-A	$ 1,373,708.00	$ 1,195,125.96
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 2YR - GovUS	TAP-25KEPS-DT2SS-2Y-US-A	$ 1,750,270.00	$ 1,522,734.90
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 2YR - GovUS	TAP-30KEPS-DT2SS-2Y-US-A	$ 2,100,324.00	$ 1,827,281.88
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 2YR - GovUS	TAP-35KEPS-DT2SS-2Y-US-A	$ 2,450,378.00	$ 2,131,828.86
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 2YR - GovUS	TAP-40KEPS-DT2SS-2Y-US-A	$ 2,800,432.00	$ 2,436,375.84
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 2YR - GovUS	TAP-45KEPS-DT2SS-2Y-US-A	$ 3,150,486.00	$ 2,740,922.82
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 2YR - GovUS	TAP-50KEPS-DT2SS-2Y-US-A	$ 3,500,540.00	$ 3,045,469.80
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 2YR - GovUS	TAP-55KEPS-DT2SS-2Y-US-A	$ 3,850,594.00	$ 3,350,016.78
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 2YR - GovUS	TAP-60KEPS-DT2SS-2Y-US-A	$ 4,200,648.00	$ 3,654,563.76
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 2YR - GovUS	TAP-65KEPS-DT2SS-2Y-US-A	$ 4,550,702.00	$ 3,959,110.74
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 2YR - GovUS	TAP-70KEPS-DT2SS-2Y-US-A	$ 4,900,756.00	$ 4,263,657.72
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 2YR - GovUS	TAP-75KEPS-DT2SS-2Y-US-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 2YR - GovUS	TAP-80KEPS-DT2SS-2Y-US-A	$ 5,600,864.00	$ 4,872,751.68
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 3YR - GovUS	TAP-1KEPS-DT2SS-3Y-US-A	$ 366,555.00	$ 318,902.85
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-DT2SS-3Y-US-A	$ 471,810.00	$ 410,474.70
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 3YR - GovUS	TAP-5KEPS-DT2SS-3Y-US-A	$ 580,215.00	$ 504,787.05
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 3YR - GovUS	TAP-10KEPS-DT2SS-3Y-US-A	$ 983,502.00	$ 855,646.74
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 3YR - GovUS	TAP-15KEPS-DT2SS-3Y-US-A	$ 1,475,253.00	$ 1,283,470.11
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 3YR - GovUS	TAP-20KEPS-DT2SS-3Y-US-A	$ 2,060,562.00	$ 1,792,688.94
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 3YR - GovUS	TAP-25KEPS-DT2SS-3Y-US-A	$ 2,625,405.00	$ 2,284,102.35
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 3YR - GovUS	TAP-30KEPS-DT2SS-3Y-US-A	$ 3,150,486.00	$ 2,740,922.82
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 3YR - GovUS	TAP-35KEPS-DT2SS-3Y-US-A	$ 3,675,567.00	$ 3,197,743.29
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 3YR - GovUS	TAP-40KEPS-DT2SS-3Y-US-A	$ 4,200,648.00	$ 3,654,563.76
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 3YR - GovUS	TAP-45KEPS-DT2SS-3Y-US-A	$ 4,725,729.00	$ 4,111,384.23
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 3YR - GovUS	TAP-50KEPS-DT2SS-3Y-US-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 3YR - GovUS	TAP-55KEPS-DT2SS-3Y-US-A	$ 5,775,891.00	$ 5,025,025.17
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 3YR - GovUS	TAP-60KEPS-DT2SS-3Y-US-A	$ 6,300,972.00	$ 5,481,845.64
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 3YR - GovUS	TAP-65KEPS-DT2SS-3Y-US-A	$ 6,826,053.00	$ 5,938,666.11
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 3YR - GovUS	TAP-70KEPS-DT2SS-3Y-US-A	$ 7,351,134.00	$ 6,395,486.58
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 3YR - GovUS	TAP-75KEPS-DT2SS-3Y-US-A	$ 7,876,215.00	$ 6,852,307.05
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 3YR - GovUS	TAP-80KEPS-DT2SS-3Y-US-A	$ 8,401,296.00	$ 7,309,127.52
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 4YR - GovUS	TAP-1KEPS-DT2SS-4Y-US-A	$ 488,740.00	$ 425,203.80
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-DT2SS-4Y-US-A	$ 629,080.00	$ 547,299.60
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 4YR - GovUS	TAP-5KEPS-DT2SS-4Y-US-A	$ 773,620.00	$ 673,049.40
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 4YR - GovUS	TAP-10KEPS-DT2SS-4Y-US-A	$ 1,311,336.00	$ 1,140,862.32
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 4YR - GovUS	TAP-15KEPS-DT2SS-4Y-US-A	$ 1,967,004.00	$ 1,711,293.48
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 4YR - GovUS	TAP-20KEPS-DT2SS-4Y-US-A	$ 2,747,416.00	$ 2,390,251.92
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 4YR - GovUS	TAP-25KEPS-DT2SS-4Y-US-A	$ 3,500,540.00	$ 3,045,469.80
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 4YR - GovUS	TAP-30KEPS-DT2SS-4Y-US-A	$ 4,200,648.00	$ 3,654,563.76

FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 4YR - GovUS	TAP-35KEPS-DT2SS-4Y-US-A	$ 4,900,756.00	$ 4,263,657.72
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 4YR - GovUS	TAP-40KEPS-DT2SS-4Y-US-A	$ 5,600,864.00	$ 4,872,751.68
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 4YR - GovUS	TAP-45KEPS-DT2SS-4Y-US-A	$ 6,300,972.00	$ 5,481,845.64
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 4YR - GovUS	TAP-50KEPS-DT2SS-4Y-US-A	$ 7,001,080.00	$ 6,090,939.60
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 4YR - GovUS	TAP-55KEPS-DT2SS-4Y-US-A	$ 7,701,188.00	$ 6,700,033.56
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 4YR - GovUS	TAP-60KEPS-DT2SS-4Y-US-A	$ 8,401,296.00	$ 7,309,127.52
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 4YR - GovUS	TAP-65KEPS-DT2SS-4Y-US-A	$ 9,101,404.00	$ 7,918,221.48
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 4YR - GovUS	TAP-70KEPS-DT2SS-4Y-US-A	$ 9,801,512.00	$ 8,527,315.44
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 4YR - GovUS	TAP-75KEPS-DT2SS-4Y-US-A	##############	$ 9,136,409.40
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 4YR - GovUS	TAP-80KEPS-DT2SS-4Y-US-A	##############	$ 9,745,503.36
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 5YR - GovUS	TAP-1KEPS-DT2SS-5Y-US-A	$ 610,925.00	$ 531,504.75
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-DT2SS-5Y-US-A	$ 786,350.00	$ 684,124.50
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 5YR - GovUS	TAP-5KEPS-DT2SS-5Y-US-A	$ 967,025.00	$ 841,311.75
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 5YR - GovUS	TAP-10KEPS-DT2SS-5Y-US-A	$ 1,639,170.00	$ 1,426,077.90
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 5YR - GovUS	TAP-15KEPS-DT2SS-5Y-US-A	$ 2,458,755.00	$ 2,139,116.85
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 5YR - GovUS	TAP-20KEPS-DT2SS-5Y-US-A	$ 3,434,270.00	$ 2,987,814.90
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 5YR - GovUS	TAP-25KEPS-DT2SS-5Y-US-A	$ 4,375,675.00	$ 3,806,837.25
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 5YR - GovUS	TAP-30KEPS-DT2SS-5Y-US-A	$ 5,250,810.00	$ 4,568,204.70
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 5YR - GovUS	TAP-35KEPS-DT2SS-5Y-US-A	$ 6,125,945.00	$ 5,329,572.15
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 5YR - GovUS	TAP-40KEPS-DT2SS-5Y-US-A	$ 7,001,080.00	$ 6,090,939.60
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 5YR - GovUS	TAP-45KEPS-DT2SS-5Y-US-A	$ 7,876,215.00	$ 6,852,307.05
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 5YR - GovUS	TAP-50KEPS-DT2SS-5Y-US-A	$ 8,751,350.00	$ 7,613,674.50
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 5YR - GovUS	TAP-55KEPS-DT2SS-5Y-US-A	$ 9,626,485.00	$ 8,375,041.95
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 5YR - GovUS	TAP-60KEPS-DT2SS-5Y-US-A	##############	$ 9,136,409.40
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 5YR - GovUS	TAP-65KEPS-DT2SS-5Y-US-A	##############	$ 9,897,776.85
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 5YR - GovUS	TAP-70KEPS-DT2SS-5Y-US-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 5YR - GovUS	TAP-75KEPS-DT2SS-5Y-US-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 5YR - GovUS	TAP-80KEPS-DT2SS-5Y-US-A	##############	##############
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-DT2SS-1Y-USPP-A	$ 128,294.00	$ 111,615.78
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-DT2SS-1Y-USPP	$ 165,134.00	$ 143,666.58
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-DT2SS-1Y-USPP-A	$ 203,076.00	$ 176,676.12
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-DT2SS-1Y-USPP-	$ 344,225.00	$ 299,475.75
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-DT2SS-1Y-USPP-	$ 516,338.00	$ 449,214.06
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-DT2SS-1Y-USPP-	$ 721,197.00	$ 627,441.39
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-DT2SS-1Y-USPP-	$ 918,892.00	$ 799,436.04
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-DT2SS-1Y-USPP-	$ 1,102,670.00	$ 959,322.90
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-DT2SS-1Y-USPP-	$ 1,286,448.00	$ 1,119,209.76
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-DT2SS-1Y-USPP-	$ 1,470,227.00	$ 1,279,097.49
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 1YR - GovUS Prio Plus	TAP-45KEPS-DT2SS-1Y-USPP-	$ 1,654,005.00	$ 1,438,984.35
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 1YR - GovUS Prio Plus	TAP-50KEPS-DT2SS-1Y-USPP-	$ 1,837,784.00	$ 1,598,872.08
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 1YR - GovUS Prio Plus	TAP-55KEPS-DT2SS-1Y-USPP-	$ 2,021,562.00	$ 1,758,758.94
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 1YR - GovUS Prio Plus	TAP-60KEPS-DT2SS-1Y-USPP-	$ 2,205,340.00	$ 1,918,645.80
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 1YR - GovUS Prio Plus	TAP-65KEPS-DT2SS-1Y-USPP-	$ 2,389,119.00	$ 2,078,533.53
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 1YR - GovUS Prio Plus	TAP-70KEPS-DT2SS-1Y-USPP-	$ 2,572,897.00	$ 2,238,420.39
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 1YR - GovUS Prio Plus	TAP-75KEPS-DT2SS-1Y-USPP-	$ 2,756,675.00	$ 2,398,307.25
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 1YR - GovUS Prio Plus	TAP-80KEPS-DT2SS-1Y-USPP-	$ 2,940,453.00	$ 2,558,194.11
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-DT2SS-2Y-USPP-A	$ 256,588.00	$ 223,231.56
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-DT2SS-2Y-USPP	$ 330,268.00	$ 287,333.16
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-DT2SS-2Y-USPP-A	$ 406,152.00	$ 353,352.24

FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-DT2SS-2Y-USPP-	$ 688,450.00	$ 598,951.50
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-DT2SS-2Y-USPP-	$ 1,032,676.00	$ 898,428.12
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-DT2SS-2Y-USPP-	$ 1,442,394.00	$ 1,254,882.78
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-DT2SS-2Y-USPP-	$ 1,837,784.00	$ 1,598,872.08
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-DT2SS-2Y-USPP-	$ 2,205,340.00	$ 1,918,645.80
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-DT2SS-2Y-USPP-	$ 2,572,896.00	$ 2,238,419.52
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-DT2SS-2Y-USPP-	$ 2,940,454.00	$ 2,558,194.98
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 2YR - GovUS Prio Plus	TAP-45KEPS-DT2SS-2Y-USPP-	$ 3,308,010.00	$ 2,877,968.70
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 2YR - GovUS Prio Plus	TAP-50KEPS-DT2SS-2Y-USPP-	$ 3,675,568.00	$ 3,197,744.16
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 2YR - GovUS Prio Plus	TAP-55KEPS-DT2SS-2Y-USPP-	$ 4,043,124.00	$ 3,517,517.88
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 2YR - GovUS Prio Plus	TAP-60KEPS-DT2SS-2Y-USPP-	$ 4,410,680.00	$ 3,837,291.60
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 2YR - GovUS Prio Plus	TAP-65KEPS-DT2SS-2Y-USPP-	$ 4,778,238.00	$ 4,157,067.06
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 2YR - GovUS Prio Plus	TAP-70KEPS-DT2SS-2Y-USPP-	$ 5,145,794.00	$ 4,476,840.78
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 2YR - GovUS Prio Plus	TAP-75KEPS-DT2SS-2Y-USPP-	$ 5,513,350.00	$ 4,796,614.50
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 2YR - GovUS Prio Plus	TAP-80KEPS-DT2SS-2Y-USPP-	$ 5,880,906.00	$ 5,116,388.22
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-DT2SS-3Y-USPP-A	$ 384,882.00	$ 334,847.34
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-DT2SS-3Y-USPP	$ 495,402.00	$ 430,999.74
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-DT2SS-3Y-USPP-A	$ 609,228.00	$ 530,028.36
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-DT2SS-3Y-USPP-	$ 1,032,675.00	$ 898,427.25
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-DT2SS-3Y-USPP-	$ 1,549,014.00	$ 1,347,642.18
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-DT2SS-3Y-USPP-	$ 2,163,591.00	$ 1,882,324.17
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-DT2SS-3Y-USPP-	$ 2,756,676.00	$ 2,398,308.12
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-DT2SS-3Y-USPP-	$ 3,308,010.00	$ 2,877,968.70
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-DT2SS-3Y-USPP-	$ 3,859,344.00	$ 3,357,629.28
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-DT2SS-3Y-USPP-	$ 4,410,681.00	$ 3,837,292.47
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 3YR - GovUS Prio Plus	TAP-45KEPS-DT2SS-3Y-USPP-	$ 4,962,015.00	$ 4,316,953.05
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 3YR - GovUS Prio Plus	TAP-50KEPS-DT2SS-3Y-USPP-	$ 5,513,352.00	$ 4,796,616.24
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 3YR - GovUS Prio Plus	TAP-55KEPS-DT2SS-3Y-USPP-	$ 6,064,686.00	$ 5,276,276.82
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 3YR - GovUS Prio Plus	TAP-60KEPS-DT2SS-3Y-USPP-	$ 6,616,020.00	$ 5,755,937.40
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 3YR - GovUS Prio Plus	TAP-65KEPS-DT2SS-3Y-USPP-	$ 7,167,357.00	$ 6,235,600.59
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 3YR - GovUS Prio Plus	TAP-70KEPS-DT2SS-3Y-USPP-	$ 7,718,691.00	$ 6,715,261.17
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 3YR - GovUS Prio Plus	TAP-75KEPS-DT2SS-3Y-USPP-	$ 8,270,025.00	$ 7,194,921.75
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 3YR - GovUS Prio Plus	TAP-80KEPS-DT2SS-3Y-USPP-	$ 8,821,359.00	$ 7,674,582.33
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-DT2SS-4Y-USPP-A	$ 513,176.00	$ 446,463.12
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-DT2SS-4Y-USPP	$ 660,536.00	$ 574,666.32
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-DT2SS-4Y-USPP-A	$ 812,304.00	$ 706,704.48
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-DT2SS-4Y-USPP-	$ 1,376,900.00	$ 1,197,903.00
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-DT2SS-4Y-USPP-	$ 2,065,352.00	$ 1,796,856.24
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-DT2SS-4Y-USPP-	$ 2,884,788.00	$ 2,509,765.56
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-DT2SS-4Y-USPP-	$ 3,675,568.00	$ 3,197,744.16
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-DT2SS-4Y-USPP-	$ 4,410,680.00	$ 3,837,291.60
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-DT2SS-4Y-USPP-	$ 5,145,792.00	$ 4,476,839.04
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-DT2SS-4Y-USPP-	$ 5,880,908.00	$ 5,116,389.96
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 4YR - GovUS Prio Plus	TAP-45KEPS-DT2SS-4Y-USPP-	$ 6,616,020.00	$ 5,755,937.40
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 4YR - GovUS Prio Plus	TAP-50KEPS-DT2SS-4Y-USPP-	$ 7,351,136.00	$ 6,395,488.32
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 4YR - GovUS Prio Plus	TAP-55KEPS-DT2SS-4Y-USPP-	$ 8,086,248.00	$ 7,035,035.76
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 4YR - GovUS Prio Plus	TAP-60KEPS-DT2SS-4Y-USPP-	$ 8,821,360.00	$ 7,674,583.20
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 4YR - GovUS Prio Plus	TAP-65KEPS-DT2SS-4Y-USPP-	$ 9,556,476.00	$ 8,314,134.12
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 4YR - GovUS Prio Plus	TAP-70KEPS-DT2SS-4Y-USPP-	############	$ 8,953,681.56

FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 4YR - GovUS Prio Plus	TAP-75KEPS-DT2SS-4Y-USPP-	##########	$ 9,593,229.00
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 4YR - GovUS Prio Plus	TAP-80KEPS-DT2SS-4Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Short Search 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-DT2SS-5Y-USPP-A	$ 641,470.00	$ 558,078.90
FireEye	Threat Analytics Platform Detect to Short Search 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-DT2SS-5Y-USPP	$ 825,670.00	$ 718,332.90
FireEye	Threat Analytics Platform Detect to Short Search 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-DT2SS-5Y-USPP-A	$ 1,015,380.00	$ 883,380.60
FireEye	Threat Analytics Platform Detect to Short Search 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-DT2SS-5Y-USPP-	$ 1,721,125.00	$ 1,497,378.75
FireEye	Threat Analytics Platform Detect to Short Search 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-DT2SS-5Y-USPP-	$ 2,581,690.00	$ 2,246,070.30
FireEye	Threat Analytics Platform Detect to Short Search 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-DT2SS-5Y-USPP-	$ 3,605,985.00	$ 3,137,206.95
FireEye	Threat Analytics Platform Detect to Short Search 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-DT2SS-5Y-USPP-	$ 4,594,460.00	$ 3,997,180.20
FireEye	Threat Analytics Platform Detect to Short Search 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-DT2SS-5Y-USPP-	$ 5,513,350.00	$ 4,796,614.50
FireEye	Threat Analytics Platform Detect to Short Search 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-DT2SS-5Y-USPP-	$ 6,432,240.00	$ 5,596,048.80
FireEye	Threat Analytics Platform Detect to Short Search 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-DT2SS-5Y-USPP-	$ 7,351,135.00	$ 6,395,487.45
FireEye	Threat Analytics Platform Detect to Short Search 45K events/sec 5YR - GovUS Prio Plus	TAP-45KEPS-DT2SS-5Y-USPP-	$ 8,270,025.00	$ 7,194,921.75
FireEye	Threat Analytics Platform Detect to Short Search 50K events/sec 5YR - GovUS Prio Plus	TAP-50KEPS-DT2SS-5Y-USPP-	$ 9,188,920.00	$ 7,994,360.40
FireEye	Threat Analytics Platform Detect to Short Search 55K events/sec 5YR - GovUS Prio Plus	TAP-55KEPS-DT2SS-5Y-USPP-	##########	$ 8,793,794.70
FireEye	Threat Analytics Platform Detect to Short Search 60K events/sec 5YR - GovUS Prio Plus	TAP-60KEPS-DT2SS-5Y-USPP-	##########	$ 9,593,229.00
FireEye	Threat Analytics Platform Detect to Short Search 65K events/sec 5YR - GovUS Prio Plus	TAP-65KEPS-DT2SS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Short Search 70K events/sec 5YR - GovUS Prio Plus	TAP-70KEPS-DT2SS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Short Search 75K events/sec 5YR - GovUS Prio Plus	TAP-75KEPS-DT2SS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Short Search 80K events/sec 5YR - GovUS Prio Plus	TAP-80KEPS-DT2SS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 1YR - GovUS	TAP-1KEPS-DT2LS-1Y-US-A	$ 381,961.00	$ 332,306.07
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-DT2LS-1Y-US-A	$ 481,990.00	$ 419,331.30
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 1YR - GovUS	TAP-5KEPS-DT2LS-1Y-US-A	$ 583,069.00	$ 507,270.03
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 1YR - GovUS	TAP-10KEPS-DT2LS-1Y-US-A	$ 977,274.00	$ 850,228.38
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 1YR - GovUS	TAP-15KEPS-DT2LS-1Y-US-A	$ 1,465,911.00	$ 1,275,342.57
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 1YR - GovUS	TAP-20KEPS-DT2LS-1Y-US-A	$ 1,985,734.00	$ 1,727,588.58
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 1YR - GovUS	TAP-25KEPS-DT2LS-1Y-US-A	$ 2,498,735.00	$ 2,173,899.45
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 1YR - GovUS	TAP-30KEPS-DT2LS-1Y-US-A	$ 2,998,482.00	$ 2,608,679.34
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 1YR - GovUS	TAP-35KEPS-DT2LS-1Y-US-A	$ 3,498,229.00	$ 3,043,459.23
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 1YR - GovUS	TAP-40KEPS-DT2LS-1Y-US-A	$ 3,997,976.00	$ 3,478,239.12
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 2YR - GovUS	TAP-1KEPS-DT2LS-2Y-US-A	$ 763,922.00	$ 664,612.14
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-DT2LS-2Y-US-A	$ 963,980.00	$ 838,662.60
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 2YR - GovUS	TAP-5KEPS-DT2LS-2Y-US-A	$ 1,166,138.00	$ 1,014,540.06
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 2YR - GovUS	TAP-10KEPS-DT2LS-2Y-US-A	$ 1,954,548.00	$ 1,700,456.76
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 2YR - GovUS	TAP-15KEPS-DT2LS-2Y-US-A	$ 2,931,822.00	$ 2,550,685.14
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 2YR - GovUS	TAP-20KEPS-DT2LS-2Y-US-A	$ 3,971,468.00	$ 3,455,177.16
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 2YR - GovUS	TAP-25KEPS-DT2LS-2Y-US-A	$ 4,997,470.00	$ 4,347,798.90
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 2YR - GovUS	TAP-30KEPS-DT2LS-2Y-US-A	$ 5,996,964.00	$ 5,217,358.68
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 2YR - GovUS	TAP-35KEPS-DT2LS-2Y-US-A	$ 6,996,458.00	$ 6,086,918.46
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 2YR - GovUS	TAP-40KEPS-DT2LS-2Y-US-A	$ 7,995,952.00	$ 6,956,478.24
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 3YR - GovUS	TAP-1KEPS-DT2LS-3Y-US-A	$ 1,145,883.00	$ 996,918.21
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-DT2LS-3Y-US-A	$ 1,445,970.00	$ 1,257,993.90
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 3YR - GovUS	TAP-5KEPS-DT2LS-3Y-US-A	$ 1,749,207.00	$ 1,521,810.09
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 3YR - GovUS	TAP-10KEPS-DT2LS-3Y-US-A	$ 2,931,822.00	$ 2,550,685.14
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 3YR - GovUS	TAP-15KEPS-DT2LS-3Y-US-A	$ 4,397,733.00	$ 3,826,027.71
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 3YR - GovUS	TAP-20KEPS-DT2LS-3Y-US-A	$ 5,957,202.00	$ 5,182,765.74
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 3YR - GovUS	TAP-25KEPS-DT2LS-3Y-US-A	$ 7,496,205.00	$ 6,521,698.35
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 3YR - GovUS	TAP-30KEPS-DT2LS-3Y-US-A	$ 8,995,446.00	$ 7,826,038.02
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 3YR - GovUS	TAP-35KEPS-DT2LS-3Y-US-A	##########	$ 9,130,377.69

FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 3YR - GovUS	TAP-40KEPS-DT2LS-3Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 4YR - GovUS	TAP-1KEPS-DT2LS-4Y-US-A	$ 1,527,844.00	$ 1,329,224.28
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-DT2LS-4Y-US-A	$ 1,927,960.00	$ 1,677,325.20
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 4YR - GovUS	TAP-5KEPS-DT2LS-4Y-US-A	$ 2,332,276.00	$ 2,029,080.12
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 4YR - GovUS	TAP-10KEPS-DT2LS-4Y-US-A	$ 3,909,096.00	$ 3,400,913.52
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 4YR - GovUS	TAP-15KEPS-DT2LS-4Y-US-A	$ 5,863,644.00	$ 5,101,370.28
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 4YR - GovUS	TAP-20KEPS-DT2LS-4Y-US-A	$ 7,942,936.00	$ 6,910,354.32
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 4YR - GovUS	TAP-25KEPS-DT2LS-4Y-US-A	$ 9,994,940.00	$ 8,695,597.80
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 4YR - GovUS	TAP-30KEPS-DT2LS-4Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 4YR - GovUS	TAP-35KEPS-DT2LS-4Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 4YR - GovUS	TAP-40KEPS-DT2LS-4Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 5YR - GovUS	TAP-1KEPS-DT2LS-5Y-US-A	$ 1,909,805.00	$ 1,661,530.35
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-DT2LS-5Y-US-A	$ 2,409,950.00	$ 2,096,656.50
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 5YR - GovUS	TAP-5KEPS-DT2LS-5Y-US-A	$ 2,915,345.00	$ 2,536,350.15
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 5YR - GovUS	TAP-10KEPS-DT2LS-5Y-US-A	$ 4,886,370.00	$ 4,251,141.90
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 5YR - GovUS	TAP-15KEPS-DT2LS-5Y-US-A	$ 7,329,555.00	$ 6,376,712.85
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 5YR - GovUS	TAP-20KEPS-DT2LS-5Y-US-A	$ 9,928,670.00	$ 8,637,942.90
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 5YR - GovUS	TAP-25KEPS-DT2LS-5Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 5YR - GovUS	TAP-30KEPS-DT2LS-5Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 5YR - GovUS	TAP-35KEPS-DT2LS-5Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 5YR - GovUS	TAP-40KEPS-DT2LS-5Y-US-A	############	############
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-DT2LS-1Y-USPP-A	$ 401,059.00	$ 348,921.33
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-DT2LS-1Y-USPP	$ 506,090.00	$ 440,298.30
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-DT2LS-1Y-USPP-A	$ 612,223.00	$ 532,634.01
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-DT2LS-1Y-USPP-	$ 1,026,137.00	$ 892,739.19
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-DT2LS-1Y-USPP-	$ 1,539,206.00	$ 1,339,109.22
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-DT2LS-1Y-USPP-	$ 2,085,021.00	$ 1,813,968.27
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-DT2LS-1Y-USPP-	$ 2,623,672.00	$ 2,282,594.64
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-DT2LS-1Y-USPP-	$ 3,148,406.00	$ 2,739,113.22
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-DT2LS-1Y-USPP-	$ 3,673,140.00	$ 3,195,631.80
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-DT2LS-1Y-USPP-	$ 4,197,875.00	$ 3,652,151.25
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-DT2LS-2Y-USPP-A	$ 802,118.00	$ 697,842.66
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-DT2LS-2Y-USPP	$ 1,012,180.00	$ 880,596.60
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-DT2LS-2Y-USPP-A	$ 1,224,446.00	$ 1,065,268.02
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-DT2LS-2Y-USPP-	$ 2,052,274.00	$ 1,785,478.38
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-DT2LS-2Y-USPP-	$ 3,078,412.00	$ 2,678,218.44
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-DT2LS-2Y-USPP-	$ 4,170,042.00	$ 3,627,936.54
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-DT2LS-2Y-USPP-	$ 5,247,344.00	$ 4,565,189.28
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-DT2LS-2Y-USPP-	$ 6,296,812.00	$ 5,478,226.44
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-DT2LS-2Y-USPP-	$ 7,346,280.00	$ 6,391,263.60
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-DT2LS-2Y-USPP-	$ 8,395,750.00	$ 7,304,302.50
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-DT2LS-3Y-USPP-A	$ 1,203,177.00	$ 1,046,763.99
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-DT2LS-3Y-USPP	$ 1,518,270.00	$ 1,320,894.90
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-DT2LS-3Y-USPP-A	$ 1,836,669.00	$ 1,597,902.03
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-DT2LS-3Y-USPP-	$ 3,078,411.00	$ 2,678,217.57
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-DT2LS-3Y-USPP-	$ 4,617,618.00	$ 4,017,327.66
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-DT2LS-3Y-USPP-	$ 6,255,063.00	$ 5,441,904.81
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-DT2LS-3Y-USPP-	$ 7,871,016.00	$ 6,847,783.92
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-DT2LS-3Y-USPP-	$ 9,445,218.00	$ 8,217,339.66

FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-DT2LS-3Y-USPP-	##########	$ 9,586,895.40
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-DT2LS-3Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-DT2LS-4Y-USPP-A	$ 1,604,236.00	$ 1,395,685.32
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-DT2LS-4Y-USPP	$ 2,024,360.00	$ 1,761,193.20
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-DT2LS-4Y-USPP-A	$ 2,448,892.00	$ 2,130,536.04
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-DT2LS-4Y-USPP-	$ 4,104,548.00	$ 3,570,956.76
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-DT2LS-4Y-USPP-	$ 6,156,824.00	$ 5,356,436.88
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-DT2LS-4Y-USPP-	$ 8,340,084.00	$ 7,255,873.08
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-DT2LS-4Y-USPP-	##########	$ 9,130,378.56
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-DT2LS-4Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-DT2LS-4Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-DT2LS-4Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-DT2LS-5Y-USPP-A	$ 2,005,295.00	$ 1,744,606.65
FireEye	Threat Analytics Platform Detect to Long Search 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-DT2LS-5Y-USPP	$ 2,530,450.00	$ 2,201,491.50
FireEye	Threat Analytics Platform Detect to Long Search 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-DT2LS-5Y-USPP-A	$ 3,061,115.00	$ 2,663,170.05
FireEye	Threat Analytics Platform Detect to Long Search 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-DT2LS-5Y-USPP-	$ 5,130,685.00	$ 4,463,695.95
FireEye	Threat Analytics Platform Detect to Long Search 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-DT2LS-5Y-USPP-	$ 7,696,030.00	$ 6,695,546.10
FireEye	Threat Analytics Platform Detect to Long Search 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-DT2LS-5Y-USPP-	##########	$ 9,069,841.35
FireEye	Threat Analytics Platform Detect to Long Search 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-DT2LS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-DT2LS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-DT2LS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Detect to Long Search 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-DT2LS-5Y-USPP-	##########	##########
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 1YR - GovUS	TAP-1KEPS-SS2LS-1Y-US-A	$ 259,776.00	$ 226,005.12
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 1YR - GovUS	TAP-2.5KEPS-SS2LS-1Y-US-A	$ 324,720.00	$ 282,506.40
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 1YR - GovUS	TAP-5KEPS-SS2LS-1Y-US-A	$ 389,664.00	$ 339,007.68
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 1YR - GovUS	TAP-10KEPS-SS2LS-1Y-US-A	$ 649,440.00	$ 565,012.80
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 1YR - GovUS	TAP-15KEPS-SS2LS-1Y-US-A	$ 974,160.00	$ 847,519.20
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 1YR - GovUS	TAP-20KEPS-SS2LS-1Y-US-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 1YR - GovUS	TAP-25KEPS-SS2LS-1Y-US-A	$ 1,623,600.00	$ 1,412,532.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 1YR - GovUS	TAP-30KEPS-SS2LS-1Y-US-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 1YR - GovUS	TAP-35KEPS-SS2LS-1Y-US-A	$ 2,273,040.00	$ 1,977,544.80
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 1YR - GovUS	TAP-40KEPS-SS2LS-1Y-US-A	$ 2,597,760.00	$ 2,260,051.20
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 2YR - GovUS	TAP-1KEPS-SS2LS-2Y-US-A	$ 519,552.00	$ 452,010.24
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 2YR - GovUS	TAP-2.5KEPS-SS2LS-2Y-US-A	$ 649,440.00	$ 565,012.80
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 2YR - GovUS	TAP-5KEPS-SS2LS-2Y-US-A	$ 779,328.00	$ 678,015.36
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 2YR - GovUS	TAP-10KEPS-SS2LS-2Y-US-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 2YR - GovUS	TAP-15KEPS-SS2LS-2Y-US-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 2YR - GovUS	TAP-20KEPS-SS2LS-2Y-US-A	$ 2,597,760.00	$ 2,260,051.20
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 2YR - GovUS	TAP-25KEPS-SS2LS-2Y-US-A	$ 3,247,200.00	$ 2,825,064.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 2YR - GovUS	TAP-30KEPS-SS2LS-2Y-US-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 2YR - GovUS	TAP-35KEPS-SS2LS-2Y-US-A	$ 4,546,080.00	$ 3,955,089.60
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 2YR - GovUS	TAP-40KEPS-SS2LS-2Y-US-A	$ 5,195,520.00	$ 4,520,102.40
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 3YR - GovUS	TAP-1KEPS-SS2LS-3Y-US-A	$ 779,328.00	$ 678,015.36
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 3YR - GovUS	TAP-2.5KEPS-SS2LS-3Y-US-A	$ 974,160.00	$ 847,519.20
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 3YR - GovUS	TAP-5KEPS-SS2LS-3Y-US-A	$ 1,168,992.00	$ 1,017,023.04
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 3YR - GovUS	TAP-10KEPS-SS2LS-3Y-US-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 3YR - GovUS	TAP-15KEPS-SS2LS-3Y-US-A	$ 2,922,480.00	$ 2,542,557.60
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 3YR - GovUS	TAP-20KEPS-SS2LS-3Y-US-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 3YR - GovUS	TAP-25KEPS-SS2LS-3Y-US-A	$ 4,870,800.00	$ 4,237,596.00

FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 3YR - GovUS	TAP-30KEPS-SS2LS-3Y-US-A	$ 5,844,960.00	$ 5,085,115.20
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 3YR - GovUS	TAP-35KEPS-SS2LS-3Y-US-A	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 3YR - GovUS	TAP-40KEPS-SS2LS-3Y-US-A	$ 7,793,280.00	$ 6,780,153.60
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 4YR - GovUS	TAP-1KEPS-SS2LS-4Y-US-A	$ 1,039,104.00	$ 904,020.48
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 4YR - GovUS	TAP-2.5KEPS-SS2LS-4Y-US-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 4YR - GovUS	TAP-5KEPS-SS2LS-4Y-US-A	$ 1,558,656.00	$ 1,356,030.72
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 4YR - GovUS	TAP-10KEPS-SS2LS-4Y-US-A	$ 2,597,760.00	$ 2,260,051.20
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 4YR - GovUS	TAP-15KEPS-SS2LS-4Y-US-A	$ 3,896,640.00	$ 3,390,076.80
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 4YR - GovUS	TAP-20KEPS-SS2LS-4Y-US-A	$ 5,195,520.00	$ 4,520,102.40
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 4YR - GovUS	TAP-25KEPS-SS2LS-4Y-US-A	$ 6,494,400.00	$ 5,650,128.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 4YR - GovUS	TAP-30KEPS-SS2LS-4Y-US-A	$ 7,793,280.00	$ 6,780,153.60
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 4YR - GovUS	TAP-35KEPS-SS2LS-4Y-US-A	$ 9,092,160.00	$ 7,910,179.20
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 4YR - GovUS	TAP-40KEPS-SS2LS-4Y-US-A	##############	$ 9,040,204.80
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 5YR - GovUS	TAP-1KEPS-SS2LS-5Y-US-A	$ 1,298,880.00	$ 1,130,025.60
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 5YR - GovUS	TAP-2.5KEPS-SS2LS-5Y-US-A	$ 1,623,600.00	$ 1,412,532.00
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 5YR - GovUS	TAP-5KEPS-SS2LS-5Y-US-A	$ 1,948,320.00	$ 1,695,038.40
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 5YR - GovUS	TAP-10KEPS-SS2LS-5Y-US-A	$ 3,247,200.00	$ 2,825,064.00
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 5YR - GovUS	TAP-15KEPS-SS2LS-5Y-US-A	$ 4,870,800.00	$ 4,237,596.00
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 5YR - GovUS	TAP-20KEPS-SS2LS-5Y-US-A	$ 6,494,400.00	$ 5,650,128.00
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 5YR - GovUS	TAP-25KEPS-SS2LS-5Y-US-A	$ 8,118,000.00	$ 7,062,660.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 5YR - GovUS	TAP-30KEPS-SS2LS-5Y-US-A	$ 9,741,600.00	$ 8,475,192.00
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 5YR - GovUS	TAP-35KEPS-SS2LS-5Y-US-A	##############	$ 9,887,724.00
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 5YR - GovUS	TAP-40KEPS-SS2LS-5Y-US-A	##############	##############
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 1YR - GovUS Prio Plus	TAP-1KEPS-SS2LS-1Y-USPP-A	$ 272,765.00	$ 237,305.55
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 1YR - GovUS Prio Plus	TAP-2.5KEPS-SS2LS-1Y-USPP-	$ 340,956.00	$ 296,631.72
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 1YR - GovUS Prio Plus	TAP-5KEPS-SS2LS-1Y-USPP-A	$ 409,147.00	$ 355,957.89
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 1YR - GovUS Prio Plus	TAP-10KEPS-SS2LS-1Y-USPP-	$ 681,912.00	$ 593,263.44
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 1YR - GovUS Prio Plus	TAP-15KEPS-SS2LS-1Y-USPP-	$ 1,022,868.00	$ 889,895.16
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 1YR - GovUS Prio Plus	TAP-20KEPS-SS2LS-1Y-USPP-	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 1YR - GovUS Prio Plus	TAP-25KEPS-SS2LS-1Y-USPP-	$ 1,704,780.00	$ 1,483,158.60
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 1YR - GovUS Prio Plus	TAP-30KEPS-SS2LS-1Y-USPP-	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 1YR - GovUS Prio Plus	TAP-35KEPS-SS2LS-1Y-USPP-	$ 2,386,692.00	$ 2,076,422.04
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 1YR - GovUS Prio Plus	TAP-40KEPS-SS2LS-1Y-USPP-	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 2YR - GovUS Prio Plus	TAP-1KEPS-SS2LS-2Y-USPP-A	$ 545,530.00	$ 474,611.10
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 2YR - GovUS Prio Plus	TAP-2.5KEPS-SS2LS-2Y-USPP-	$ 681,912.00	$ 593,263.44
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 2YR - GovUS Prio Plus	TAP-5KEPS-SS2LS-2Y-USPP-A	$ 818,294.00	$ 711,915.78
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 2YR - GovUS Prio Plus	TAP-10KEPS-SS2LS-2Y-USPP-	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 2YR - GovUS Prio Plus	TAP-15KEPS-SS2LS-2Y-USPP-	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 2YR - GovUS Prio Plus	TAP-20KEPS-SS2LS-2Y-USPP-	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 2YR - GovUS Prio Plus	TAP-25KEPS-SS2LS-2Y-USPP-	$ 3,409,560.00	$ 2,966,317.20
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 2YR - GovUS Prio Plus	TAP-30KEPS-SS2LS-2Y-USPP-	$ 4,091,472.00	$ 3,559,580.64
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 2YR - GovUS Prio Plus	TAP-35KEPS-SS2LS-2Y-USPP-	$ 4,773,384.00	$ 4,152,844.08
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 2YR - GovUS Prio Plus	TAP-40KEPS-SS2LS-2Y-USPP-	$ 5,455,296.00	$ 4,746,107.52
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 3YR - GovUS Prio Plus	TAP-1KEPS-SS2LS-3Y-USPP-A	$ 818,295.00	$ 711,916.65
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 3YR - GovUS Prio Plus	TAP-2.5KEPS-SS2LS-3Y-USPP-	$ 1,022,868.00	$ 889,895.16
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 3YR - GovUS Prio Plus	TAP-5KEPS-SS2LS-3Y-USPP-A	$ 1,227,441.00	$ 1,067,873.67
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 3YR - GovUS Prio Plus	TAP-10KEPS-SS2LS-3Y-USPP-	$ 2,045,736.00	$ 1,779,790.32
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 3YR - GovUS Prio Plus	TAP-15KEPS-SS2LS-3Y-USPP-	$ 3,068,604.00	$ 2,669,685.48
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 3YR - GovUS Prio Plus	TAP-20KEPS-SS2LS-3Y-USPP-	$ 4,091,472.00	$ 3,559,580.64

FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 3YR - GovUS Prio Plus	TAP-25KEPS-SS2LS-3Y-USPP-	$ 5,114,340.00	$ 4,449,475.80
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 3YR - GovUS Prio Plus	TAP-30KEPS-SS2LS-3Y-USPP-	$ 6,137,208.00	$ 5,339,370.96
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 3YR - GovUS Prio Plus	TAP-35KEPS-SS2LS-3Y-USPP-	$ 7,160,076.00	$ 6,229,266.12
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 3YR - GovUS Prio Plus	TAP-40KEPS-SS2LS-3Y-USPP-	$ 8,182,944.00	$ 7,119,161.28
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 4YR - GovUS Prio Plus	TAP-1KEPS-SS2LS-4Y-USPP-A	$ 1,091,060.00	$ 949,222.20
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 4YR - GovUS Prio Plus	TAP-2.5KEPS-SS2LS-4Y-USPP-	$ 1,363,824.00	$ 1,186,526.88
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 4YR - GovUS Prio Plus	TAP-5KEPS-SS2LS-4Y-USPP-A	$ 1,636,588.00	$ 1,423,831.56
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 4YR - GovUS Prio Plus	TAP-10KEPS-SS2LS-4Y-USPP-	$ 2,727,648.00	$ 2,373,053.76
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 4YR - GovUS Prio Plus	TAP-15KEPS-SS2LS-4Y-USPP-	$ 4,091,472.00	$ 3,559,580.64
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 4YR - GovUS Prio Plus	TAP-20KEPS-SS2LS-4Y-USPP-	$ 5,455,296.00	$ 4,746,107.52
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 4YR - GovUS Prio Plus	TAP-25KEPS-SS2LS-4Y-USPP-	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 4YR - GovUS Prio Plus	TAP-30KEPS-SS2LS-4Y-USPP-	$ 8,182,944.00	$ 7,119,161.28
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 4YR - GovUS Prio Plus	TAP-35KEPS-SS2LS-4Y-USPP-	$ 9,546,768.00	$ 8,305,688.16
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 4YR - GovUS Prio Plus	TAP-40KEPS-SS2LS-4Y-USPP-	##############	$ 9,492,215.04
FireEye	Threat Analytics Platform Short Search to Long Search 1K events/sec 5YR - GovUS Prio Plus	TAP-1KEPS-SS2LS-5Y-USPP-A	$ 1,363,825.00	$ 1,186,527.75
FireEye	Threat Analytics Platform Short Search to Long Search 2.5K events/sec 5YR - GovUS Prio Plus	TAP-2.5KEPS-SS2LS-5Y-USPP-	$ 1,704,780.00	$ 1,483,158.60
FireEye	Threat Analytics Platform Short Search to Long Search 5K events/sec 5YR - GovUS Prio Plus	TAP-5KEPS-SS2LS-5Y-USPP-A	$ 2,045,735.00	$ 1,779,789.45
FireEye	Threat Analytics Platform Short Search to Long Search 10K events/sec 5YR - GovUS Prio Plus	TAP-10KEPS-SS2LS-5Y-USPP-	$ 3,409,560.00	$ 2,966,317.20
FireEye	Threat Analytics Platform Short Search to Long Search 15K events/sec 5YR - GovUS Prio Plus	TAP-15KEPS-SS2LS-5Y-USPP-	$ 5,114,340.00	$ 4,449,475.80
FireEye	Threat Analytics Platform Short Search to Long Search 20K events/sec 5YR - GovUS Prio Plus	TAP-20KEPS-SS2LS-5Y-USPP-	$ 6,819,120.00	$ 5,932,634.40
FireEye	Threat Analytics Platform Short Search to Long Search 25K events/sec 5YR - GovUS Prio Plus	TAP-25KEPS-SS2LS-5Y-USPP-	$ 8,523,900.00	$ 7,415,793.00
FireEye	Threat Analytics Platform Short Search to Long Search 30K events/sec 5YR - GovUS Prio Plus	TAP-30KEPS-SS2LS-5Y-USPP-	##############	$ 8,898,951.60
FireEye	Threat Analytics Platform Short Search to Long Search 35K events/sec 5YR - GovUS Prio Plus	TAP-35KEPS-SS2LS-5Y-USPP-	##############	##############
FireEye	Threat Analytics Platform Short Search to Long Search 40K events/sec 5YR - GovUS Prio Plus	TAP-40KEPS-SS2LS-5Y-USPP-	##############	##############
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-BD-1Y-PT2PP	$ 5,523.00	$ 4,805.01
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-BD-1Y-PT2P	$ 5,949.00	$ 5,175.63
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-BD-1Y-PT2PP	$ 6,060.00	$ 5,272.20
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-BD-1Y-PT2P	$ 7,407.00	$ 6,444.09
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-BD-1Y-PT2P	$ 11,110.00	$ 9,665.70
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-BD-1Y-PT2P	$ 13,254.00	$ 11,530.98
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-BD-1Y-PT2P	$ 15,739.00	$ 13,692.93
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-BD-1Y-PT2P	$ 18,887.00	$ 16,431.69
FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-BD-1Y-PT2P	$ 22,035.00	$ 19,170.45
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-BD-1Y-PT2P	$ 25,182.00	$ 21,908.34
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-BD-1Y-PT2P	$ 28,330.00	$ 24,647.10
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-BD-1Y-PT2P	$ 31,478.00	$ 27,385.86
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-BD-1Y-PT2P	$ 34,626.00	$ 30,124.62
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-BD-1Y-PT2P	$ 37,774.00	$ 32,863.38
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-BD-1Y-PT2P	$ 40,921.00	$ 35,601.27
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-BD-1Y-PT2P	$ 44,069.00	$ 38,340.03
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-BD-1Y-PT2P	$ 47,217.00	$ 41,078.79
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-BD-1Y-PT2P	$ 50,365.00	$ 43,817.55
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-BD-2Y-PT2PP	$ 11,046.00	$ 9,610.02
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-BD-2Y-PT2P	$ 11,898.00	$ 10,351.26
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-BD-2Y-PT2PP	$ 12,120.00	$ 10,544.40
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-BD-2Y-PT2P	$ 14,814.00	$ 12,888.18
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-BD-2Y-PT2P	$ 22,220.00	$ 19,331.40
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-BD-2Y-PT2P	$ 26,508.00	$ 23,061.96
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-BD-2Y-PT2P	$ 31,478.00	$ 27,385.86

FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-BD-2Y-PT2P	$ 37,774.00	$ 32,863.38
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-BD-2Y-PT2P	$ 44,070.00	$ 38,340.90
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-BD-2Y-PT2P	$ 50,364.00	$ 43,816.68
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-BD-2Y-PT2P	$ 56,660.00	$ 49,294.20
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-BD-2Y-PT2P	$ 62,956.00	$ 54,771.72
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-BD-2Y-PT2P	$ 69,252.00	$ 60,249.24
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-BD-2Y-PT2P	$ 75,548.00	$ 65,726.76
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-BD-2Y-PT2P	$ 81,842.00	$ 71,202.54
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-BD-2Y-PT2P	$ 88,138.00	$ 76,680.06
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-BD-2Y-PT2P	$ 94,434.00	$ 82,157.58
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-BD-2Y-PT2P	$ 100,730.00	$ 87,635.10
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-BD-3Y-PT2PP	$ 16,569.00	$ 14,415.03
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-BD-3Y-PT2P	$ 17,847.00	$ 15,526.89
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-BD-3Y-PT2PP	$ 18,180.00	$ 15,816.60
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-BD-3Y-PT2P	$ 22,221.00	$ 19,332.27
FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-BD-3Y-PT2P	$ 33,330.00	$ 28,997.10
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-BD-3Y-PT2P	$ 39,762.00	$ 34,592.94
FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-BD-3Y-PT2P	$ 47,217.00	$ 41,078.79
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-BD-3Y-PT2P	$ 56,661.00	$ 49,295.07
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-BD-3Y-PT2P	$ 66,105.00	$ 57,511.35
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-BD-3Y-PT2P	$ 75,546.00	$ 65,725.02
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-BD-3Y-PT2P	$ 84,990.00	$ 73,941.30
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-BD-3Y-PT2P	$ 94,434.00	$ 82,157.58
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-BD-3Y-PT2P	$ 103,878.00	$ 90,373.86
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-BD-3Y-PT2P	$ 113,322.00	$ 98,590.14
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-BD-3Y-PT2P	$ 122,763.00	$ 106,803.81
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-BD-3Y-PT2P	$ 132,207.00	$ 115,020.09
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-BD-3Y-PT2P	$ 141,651.00	$ 123,236.37
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-BD-3Y-PT2P	$ 151,095.00	$ 131,452.65
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-BD-4Y-PT2PP	$ 22,092.00	$ 19,220.04
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-BD-4Y-PT2P	$ 23,796.00	$ 20,702.52
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-BD-4Y-PT2PP	$ 24,240.00	$ 21,088.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-BD-4Y-PT2P	$ 29,628.00	$ 25,776.36
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-BD-4Y-PT2P	$ 44,440.00	$ 38,662.80
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-BD-4Y-PT2P	$ 53,016.00	$ 46,123.92
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-BD-4Y-PT2P	$ 62,956.00	$ 54,771.72
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-BD-4Y-PT2P	$ 75,548.00	$ 65,726.76
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-BD-4Y-PT2P	$ 88,140.00	$ 76,681.80
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-BD-4Y-PT2P	$ 100,728.00	$ 87,633.36
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-BD-4Y-PT2P	$ 113,320.00	$ 98,588.40
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-BD-4Y-PT2P	$ 125,912.00	$ 109,543.44
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-BD-4Y-PT2P	$ 138,504.00	$ 120,498.48
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-BD-4Y-PT2P	$ 151,096.00	$ 131,453.52
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-BD-4Y-PT2P	$ 163,684.00	$ 142,405.08
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-BD-4Y-PT2P	$ 176,276.00	$ 153,360.12
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-BD-4Y-PT2P	$ 188,868.00	$ 164,315.16
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-BD-4Y-PT2P	$ 201,460.00	$ 175,270.20
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-BD-5Y-PT2PP	$ 27,615.00	$ 24,025.05
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-BD-5Y-PT2P	$ 29,745.00	$ 25,878.15

FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-BD-5Y-PT2PP	$ 30,300.00	$ 26,361.00
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-BD-5Y-PT2P	$ 37,035.00	$ 32,220.45
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-BD-5Y-PT2P	$ 55,550.00	$ 48,328.50
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-BD-5Y-PT2P	$ 66,270.00	$ 57,654.90
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-BD-5Y-PT2P	$ 78,695.00	$ 68,464.65
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-BD-5Y-PT2P	$ 94,435.00	$ 82,158.45
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-BD-5Y-PT2P	$ 110,175.00	$ 95,852.25
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-BD-5Y-PT2P	$ 125,910.00	$ 109,541.70
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-BD-5Y-PT2P	$ 141,650.00	$ 123,235.50
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-BD-5Y-PT2P	$ 157,390.00	$ 136,929.30
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-BD-5Y-PT2P	$ 173,130.00	$ 150,623.10
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-BD-5Y-PT2P	$ 188,870.00	$ 164,316.90
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-BD-5Y-PT2P	$ 204,605.00	$ 178,006.35
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-BD-5Y-PT2P	$ 220,345.00	$ 191,700.15
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-BD-5Y-PT2P	$ 236,085.00	$ 205,393.95
FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-BD-5Y-PT2P	$ 251,825.00	$ 219,087.75
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-SS-1Y-PT2PPP	$ 11,632.00	$ 10,119.84
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-SS-1Y-PT2P	$ 13,813.00	$ 12,017.31
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-SS-1Y-PT2PPP	$ 15,731.00	$ 13,685.97
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-SS-1Y-PT2PP	$ 23,798.00	$ 20,704.26
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-SS-1Y-PT2PP	$ 35,697.00	$ 31,056.39
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-SS-1Y-PT2PP	$ 47,597.00	$ 41,409.39
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-SS-1Y-PT2PP	$ 59,496.00	$ 51,761.52
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-SS-1Y-PT2PP	$ 71,395.00	$ 62,113.65
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-SS-1Y-PT2PP	$ 83,294.00	$ 72,465.78
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-SS-1Y-PT2PP	$ 95,193.00	$ 82,817.91
FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-SS-1Y-PT2PP	$ 107,092.00	$ 93,170.04
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-SS-1Y-PT2PP	$ 118,992.00	$ 103,523.04
FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-SS-1Y-PT2PP	$ 130,891.00	$ 113,875.17
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-SS-1Y-PT2PP	$ 142,790.00	$ 124,227.30
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-SS-1Y-PT2PP	$ 154,689.00	$ 134,579.43
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-SS-1Y-PT2PP	$ 166,588.00	$ 144,931.56
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-SS-1Y-PT2PP	$ 178,487.00	$ 155,283.69
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-SS-1Y-PT2PP	$ 190,386.00	$ 165,635.82
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-SS-2Y-PT2PPP	$ 23,264.00	$ 20,239.68
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-SS-2Y-PT2P	$ 27,626.00	$ 24,034.62
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-SS-2Y-PT2PPP	$ 31,462.00	$ 27,371.94
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-SS-2Y-PT2PP	$ 47,596.00	$ 41,408.52
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-SS-2Y-PT2PP	$ 71,394.00	$ 62,112.78
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-SS-2Y-PT2PP	$ 95,194.00	$ 82,818.78
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-SS-2Y-PT2PP	$ 118,992.00	$ 103,523.04
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-SS-2Y-PT2PP	$ 142,790.00	$ 124,227.30
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-SS-2Y-PT2PP	$ 166,588.00	$ 144,931.56
FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-SS-2Y-PT2PP	$ 190,386.00	$ 165,635.82
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-SS-2Y-PT2PP	$ 214,184.00	$ 186,340.08
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-SS-2Y-PT2PP	$ 237,984.00	$ 207,046.08
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-SS-2Y-PT2PP	$ 261,782.00	$ 227,750.34
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-SS-2Y-PT2PP	$ 285,580.00	$ 248,454.60
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-SS-2Y-PT2PP	$ 309,378.00	$ 269,158.86

FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-SS-2Y-PT2PP	$ 333,176.00	$ 289,863.12
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-SS-2Y-PT2PP	$ 356,974.00	$ 310,567.38
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-SS-2Y-PT2PP	$ 380,772.00	$ 331,271.64
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-SS-3Y-PT2PPP	$ 34,896.00	$ 30,359.52
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-SS-3Y-PT2P	$ 41,439.00	$ 36,051.93
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-SS-3Y-PT2PPP	$ 47,193.00	$ 41,057.91
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-SS-3Y-PT2PP	$ 71,394.00	$ 62,112.78
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-SS-3Y-PT2PP	$ 107,091.00	$ 93,169.17
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-SS-3Y-PT2PP	$ 142,791.00	$ 124,228.17
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-SS-3Y-PT2PP	$ 178,488.00	$ 155,284.56
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-SS-3Y-PT2PP	$ 214,185.00	$ 186,340.95
FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-SS-3Y-PT2PP	$ 249,882.00	$ 217,397.34
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-SS-3Y-PT2PP	$ 285,579.00	$ 248,453.73
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-SS-3Y-PT2PP	$ 321,276.00	$ 279,510.12
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-SS-3Y-PT2PP	$ 356,976.00	$ 310,569.12
FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-SS-3Y-PT2PP	$ 392,673.00	$ 341,625.51
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-SS-3Y-PT2PP	$ 428,370.00	$ 372,681.90
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-SS-3Y-PT2PP	$ 464,067.00	$ 403,738.29
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-SS-3Y-PT2PP	$ 499,764.00	$ 434,794.68
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-SS-3Y-PT2PP	$ 535,461.00	$ 465,851.07
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-SS-3Y-PT2PP	$ 571,158.00	$ 496,907.46
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-SS-4Y-PT2PPP	$ 46,528.00	$ 40,479.36
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-SS-4Y-PT2P	$ 55,252.00	$ 48,069.24
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-SS-4Y-PT2PPP	$ 62,924.00	$ 54,743.88
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-SS-4Y-PT2PP	$ 95,192.00	$ 82,817.04
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-SS-4Y-PT2PP	$ 142,788.00	$ 124,225.56
FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-SS-4Y-PT2PP	$ 190,388.00	$ 165,637.56
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-SS-4Y-PT2PP	$ 237,984.00	$ 207,046.08
FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-SS-4Y-PT2PP	$ 285,580.00	$ 248,454.60
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-SS-4Y-PT2PP	$ 333,176.00	$ 289,863.12
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-SS-4Y-PT2PP	$ 380,772.00	$ 331,271.64
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-SS-4Y-PT2PP	$ 428,368.00	$ 372,680.16
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-SS-4Y-PT2PP	$ 475,968.00	$ 414,092.16
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-SS-4Y-PT2PP	$ 523,564.00	$ 455,500.68
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-SS-4Y-PT2PP	$ 571,160.00	$ 496,909.20
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-SS-4Y-PT2PP	$ 618,756.00	$ 538,317.72
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-SS-4Y-PT2PP	$ 666,352.00	$ 579,726.24
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-SS-4Y-PT2PP	$ 713,948.00	$ 621,134.76
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-SS-4Y-PT2PP	$ 761,544.00	$ 662,543.28
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-SS-5Y-PT2PPP	$ 58,160.00	$ 50,599.20
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-SS-5Y-PT2P	$ 69,065.00	$ 60,086.55
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-SS-5Y-PT2PPP	$ 78,655.00	$ 68,429.85
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-SS-5Y-PT2PP	$ 118,990.00	$ 103,521.30
FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-SS-5Y-PT2PP	$ 178,485.00	$ 155,281.95
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-SS-5Y-PT2PP	$ 237,985.00	$ 207,046.95
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-SS-5Y-PT2PP	$ 297,480.00	$ 258,807.60
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-SS-5Y-PT2PP	$ 356,975.00	$ 310,568.25
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-SS-5Y-PT2PP	$ 416,470.00	$ 362,328.90
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-SS-5Y-PT2PP	$ 475,965.00	$ 414,089.55

FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-45KEPS-SS-5Y-PT2PP	$ 535,460.00	$ 465,850.20
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-50KEPS-SS-5Y-PT2PP	$ 594,960.00	$ 517,615.20
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-55KEPS-SS-5Y-PT2PP	$ 654,455.00	$ 569,375.85
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-60KEPS-SS-5Y-PT2PP	$ 713,950.00	$ 621,136.50
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-65KEPS-SS-5Y-PT2PP	$ 773,445.00	$ 672,897.15
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-70KEPS-SS-5Y-PT2PP	$ 832,940.00	$ 724,657.80
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-75KEPS-SS-5Y-PT2PP	$ 892,435.00	$ 776,418.45
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-80KEPS-SS-5Y-PT2PP	$ 951,930.00	$ 828,179.10
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-LS-1Y-PT2PPP	$ 24,621.00	$ 21,420.27
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-LS-1Y-PT2P	$ 30,049.00	$ 26,142.63
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-LS-1Y-PT2PPP	$ 35,214.00	$ 30,636.18
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-LS-1Y-PT2PP	$ 56,270.00	$ 48,954.90
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-LS-1Y-PT2PP	$ 84,405.00	$ 73,432.35
FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-LS-1Y-PT2PP	$ 112,541.00	$ 97,910.67
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-LS-1Y-PT2PP	$ 140,676.00	$ 122,388.12
FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-LS-1Y-PT2PP	$ 168,811.00	$ 146,865.57
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-LS-1Y-PT2PP	$ 196,946.00	$ 171,343.02
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-LS-1Y-PT2PP	$ 225,081.00	$ 195,820.47
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-LS-2Y-PT2PPP	$ 49,242.00	$ 42,840.54
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-LS-2Y-PT2P	$ 60,098.00	$ 52,285.26
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-LS-2Y-PT2PPP	$ 70,428.00	$ 61,272.36
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-LS-2Y-PT2PP	$ 112,540.00	$ 97,909.80
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-LS-2Y-PT2PP	$ 168,810.00	$ 146,864.70
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-LS-2Y-PT2PP	$ 225,082.00	$ 195,821.34
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-LS-2Y-PT2PP	$ 281,352.00	$ 244,776.24
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-LS-2Y-PT2PP	$ 337,622.00	$ 293,731.14
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-LS-2Y-PT2PP	$ 393,892.00	$ 342,686.04
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-LS-2Y-PT2PP	$ 450,162.00	$ 391,640.94
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-LS-3Y-PT2PPP	$ 73,863.00	$ 64,260.81
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-LS-3Y-PT2P	$ 90,147.00	$ 78,427.89
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-LS-3Y-PT2PPP	$ 105,642.00	$ 91,908.54
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-LS-3Y-PT2PP	$ 168,810.00	$ 146,864.70
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-LS-3Y-PT2PP	$ 253,215.00	$ 220,297.05
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-LS-3Y-PT2PP	$ 337,623.00	$ 293,732.01
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-LS-3Y-PT2PP	$ 422,028.00	$ 367,164.36
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-LS-3Y-PT2PP	$ 506,433.00	$ 440,596.71
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-LS-3Y-PT2PP	$ 590,838.00	$ 514,029.06
FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-LS-3Y-PT2PP	$ 675,243.00	$ 587,461.41
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-LS-4Y-PT2PPP	$ 98,484.00	$ 85,681.08
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-LS-4Y-PT2P	$ 120,196.00	$ 104,570.52
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-LS-4Y-PT2PPP	$ 140,856.00	$ 122,544.72
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-LS-4Y-PT2PP	$ 225,080.00	$ 195,819.60
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-LS-4Y-PT2PP	$ 337,620.00	$ 293,729.40
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-LS-4Y-PT2PP	$ 450,164.00	$ 391,642.68
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-LS-4Y-PT2PP	$ 562,704.00	$ 489,552.48
FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-LS-4Y-PT2PP	$ 675,244.00	$ 587,462.28
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-LS-4Y-PT2PP	$ 787,784.00	$ 685,372.08
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-LS-4Y-PT2PP	$ 900,324.00	$ 783,281.88
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-1KEPS-LS-5Y-PT2PPP	$ 123,105.00	$ 107,101.35

FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-2.5KEPS-LS-5Y-PT2P	$ 150,245.00	$ 130,713.15
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-5KEPS-LS-5Y-PT2PPP	$ 176,070.00	$ 153,180.90
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-10KEPS-LS-5Y-PT2PP	$ 281,350.00	$ 244,774.50
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-15KEPS-LS-5Y-PT2PP	$ 422,025.00	$ 367,161.75
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-20KEPS-LS-5Y-PT2PP	$ 562,705.00	$ 489,553.35
FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-25KEPS-LS-5Y-PT2PP	$ 703,380.00	$ 611,940.60
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-30KEPS-LS-5Y-PT2PP	$ 844,055.00	$ 734,327.85
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-35KEPS-LS-5Y-PT2PP	$ 984,730.00	$ 856,715.10
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - Platinum to Plat Prio Plus	UP-TAP-40KEPS-LS-5Y-PT2PP	$ 1,125,405.00	$ 979,102.35
FireEye	Threat Analytics Platform Base Detect 1K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-BD-1Y-USG2U	$ 5,523.00	$ 4,805.01
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-BD-1Y-USG2	$ 5,949.00	$ 5,175.63
FireEye	Threat Analytics Platform Base Detect 5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-BD-1Y-USG2U	$ 6,060.00	$ 5,272.20
FireEye	Threat Analytics Platform Base Detect 10K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-BD-1Y-USG2	$ 7,407.00	$ 6,444.09
FireEye	Threat Analytics Platform Base Detect 15K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-BD-1Y-USG2	$ 11,110.00	$ 9,665.70
FireEye	Threat Analytics Platform Base Detect 20K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-BD-1Y-USG2	$ 13,254.00	$ 11,530.98
FireEye	Threat Analytics Platform Base Detect 25K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-BD-1Y-USG2	$ 15,739.00	$ 13,692.93
FireEye	Threat Analytics Platform Base Detect 30K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-BD-1Y-USG2	$ 18,887.00	$ 16,431.69
FireEye	Threat Analytics Platform Base Detect 35K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-BD-1Y-USG2	$ 22,035.00	$ 19,170.45
FireEye	Threat Analytics Platform Base Detect 40K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-BD-1Y-USG2	$ 25,182.00	$ 21,908.34
FireEye	Threat Analytics Platform Base Detect 45K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-BD-1Y-USG2	$ 28,330.00	$ 24,647.10
FireEye	Threat Analytics Platform Base Detect 50K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-BD-1Y-USG2	$ 31,478.00	$ 27,385.86
FireEye	Threat Analytics Platform Base Detect 55K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-BD-1Y-USG2	$ 34,626.00	$ 30,124.62
FireEye	Threat Analytics Platform Base Detect 60K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-BD-1Y-USG2	$ 37,774.00	$ 32,863.38
FireEye	Threat Analytics Platform Base Detect 65K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-BD-1Y-USG2	$ 40,921.00	$ 35,601.27
FireEye	Threat Analytics Platform Base Detect 70K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-BD-1Y-USG2	$ 44,069.00	$ 38,340.03
FireEye	Threat Analytics Platform Base Detect 75K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-BD-1Y-USG2	$ 47,217.00	$ 41,078.79
FireEye	Threat Analytics Platform Base Detect 80K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-BD-1Y-USG2	$ 50,365.00	$ 43,817.55
FireEye	Threat Analytics Platform Base Detect 1K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-BD-2Y-USG2U	$ 11,046.00	$ 9,610.02
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-BD-2Y-USG2	$ 11,898.00	$ 10,351.26
FireEye	Threat Analytics Platform Base Detect 5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-BD-2Y-USG2U	$ 12,120.00	$ 10,544.40
FireEye	Threat Analytics Platform Base Detect 10K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-BD-2Y-USG2	$ 14,814.00	$ 12,888.18
FireEye	Threat Analytics Platform Base Detect 15K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-BD-2Y-USG2	$ 22,220.00	$ 19,331.40
FireEye	Threat Analytics Platform Base Detect 20K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-BD-2Y-USG2	$ 26,508.00	$ 23,061.96
FireEye	Threat Analytics Platform Base Detect 25K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-BD-2Y-USG2	$ 31,478.00	$ 27,385.86
FireEye	Threat Analytics Platform Base Detect 30K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-BD-2Y-USG2	$ 37,774.00	$ 32,863.38
FireEye	Threat Analytics Platform Base Detect 35K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-BD-2Y-USG2	$ 44,070.00	$ 38,340.90
FireEye	Threat Analytics Platform Base Detect 40K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-BD-2Y-USG2	$ 50,364.00	$ 43,816.68
FireEye	Threat Analytics Platform Base Detect 45K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-BD-2Y-USG2	$ 56,660.00	$ 49,294.20
FireEye	Threat Analytics Platform Base Detect 50K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-BD-2Y-USG2	$ 62,956.00	$ 54,771.72
FireEye	Threat Analytics Platform Base Detect 55K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-BD-2Y-USG2	$ 69,252.00	$ 60,249.24
FireEye	Threat Analytics Platform Base Detect 60K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-BD-2Y-USG2	$ 75,548.00	$ 65,726.76
FireEye	Threat Analytics Platform Base Detect 65K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-BD-2Y-USG2	$ 81,842.00	$ 71,202.54
FireEye	Threat Analytics Platform Base Detect 70K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-BD-2Y-USG2	$ 88,138.00	$ 76,680.06
FireEye	Threat Analytics Platform Base Detect 75K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-BD-2Y-USG2	$ 94,434.00	$ 82,157.58
FireEye	Threat Analytics Platform Base Detect 80K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-BD-2Y-USG2	$ 100,730.00	$ 87,635.10
FireEye	Threat Analytics Platform Base Detect 1K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-BD-3Y-USG2U	$ 16,569.00	$ 14,415.03
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-BD-3Y-USG2	$ 17,847.00	$ 15,526.89
FireEye	Threat Analytics Platform Base Detect 5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-BD-3Y-USG2U	$ 18,180.00	$ 15,816.60
FireEye	Threat Analytics Platform Base Detect 10K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-BD-3Y-USG2	$ 22,221.00	$ 19,332.27

FireEye	Threat Analytics Platform Base Detect 15K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-BD-3Y-USG2	$ 33,330.00	$ 28,997.10
FireEye	Threat Analytics Platform Base Detect 20K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-BD-3Y-USG2	$ 39,762.00	$ 34,592.94
FireEye	Threat Analytics Platform Base Detect 25K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-BD-3Y-USG2	$ 47,217.00	$ 41,078.79
FireEye	Threat Analytics Platform Base Detect 30K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-BD-3Y-USG2	$ 56,661.00	$ 49,295.07
FireEye	Threat Analytics Platform Base Detect 35K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-BD-3Y-USG2	$ 66,105.00	$ 57,511.35
FireEye	Threat Analytics Platform Base Detect 40K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-BD-3Y-USG2	$ 75,546.00	$ 65,725.02
FireEye	Threat Analytics Platform Base Detect 45K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-BD-3Y-USG2	$ 84,990.00	$ 73,941.30
FireEye	Threat Analytics Platform Base Detect 50K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-BD-3Y-USG2	$ 94,434.00	$ 82,157.58
FireEye	Threat Analytics Platform Base Detect 55K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-BD-3Y-USG2	$ 103,878.00	$ 90,373.86
FireEye	Threat Analytics Platform Base Detect 60K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-BD-3Y-USG2	$ 113,322.00	$ 98,590.14
FireEye	Threat Analytics Platform Base Detect 65K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-BD-3Y-USG2	$ 122,763.00	$ 106,803.81
FireEye	Threat Analytics Platform Base Detect 70K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-BD-3Y-USG2	$ 132,207.00	$ 115,020.09
FireEye	Threat Analytics Platform Base Detect 75K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-BD-3Y-USG2	$ 141,651.00	$ 123,236.37
FireEye	Threat Analytics Platform Base Detect 80K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-BD-3Y-USG2	$ 151,095.00	$ 131,452.65
FireEye	Threat Analytics Platform Base Detect 1K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-BD-4Y-USG2U	$ 22,092.00	$ 19,220.04
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-BD-4Y-USG2	$ 23,796.00	$ 20,702.52
FireEye	Threat Analytics Platform Base Detect 5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-BD-4Y-USG2U	$ 24,240.00	$ 21,088.80
FireEye	Threat Analytics Platform Base Detect 10K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-BD-4Y-USG2	$ 29,628.00	$ 25,776.36
FireEye	Threat Analytics Platform Base Detect 15K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-BD-4Y-USG2	$ 44,440.00	$ 38,662.80
FireEye	Threat Analytics Platform Base Detect 20K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-BD-4Y-USG2	$ 53,016.00	$ 46,123.92
FireEye	Threat Analytics Platform Base Detect 25K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-BD-4Y-USG2	$ 62,956.00	$ 54,771.72
FireEye	Threat Analytics Platform Base Detect 30K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-BD-4Y-USG2	$ 75,548.00	$ 65,726.76
FireEye	Threat Analytics Platform Base Detect 35K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-BD-4Y-USG2	$ 88,140.00	$ 76,681.80
FireEye	Threat Analytics Platform Base Detect 40K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-BD-4Y-USG2	$ 100,728.00	$ 87,633.36
FireEye	Threat Analytics Platform Base Detect 45K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-BD-4Y-USG2	$ 113,320.00	$ 98,588.40
FireEye	Threat Analytics Platform Base Detect 50K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-BD-4Y-USG2	$ 125,912.00	$ 109,543.44
FireEye	Threat Analytics Platform Base Detect 55K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-BD-4Y-USG2	$ 138,504.00	$ 120,498.48
FireEye	Threat Analytics Platform Base Detect 60K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-BD-4Y-USG2	$ 151,096.00	$ 131,453.52
FireEye	Threat Analytics Platform Base Detect 65K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-BD-4Y-USG2	$ 163,684.00	$ 142,405.08
FireEye	Threat Analytics Platform Base Detect 70K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-BD-4Y-USG2	$ 176,276.00	$ 153,360.12
FireEye	Threat Analytics Platform Base Detect 75K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-BD-4Y-USG2	$ 188,868.00	$ 164,315.16
FireEye	Threat Analytics Platform Base Detect 80K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-BD-4Y-USG2	$ 201,460.00	$ 175,270.20
FireEye	Threat Analytics Platform Base Detect 1K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-BD-5Y-USG2U	$ 27,615.00	$ 24,025.05
FireEye	Threat Analytics Platform Base Detect 2.5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-BD-5Y-USG2	$ 29,745.00	$ 25,878.15
FireEye	Threat Analytics Platform Base Detect 5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-BD-5Y-USG2U	$ 30,300.00	$ 26,361.00
FireEye	Threat Analytics Platform Base Detect 10K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-BD-5Y-USG2	$ 37,035.00	$ 32,220.45
FireEye	Threat Analytics Platform Base Detect 15K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-BD-5Y-USG2	$ 55,550.00	$ 48,328.50
FireEye	Threat Analytics Platform Base Detect 20K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-BD-5Y-USG2	$ 66,270.00	$ 57,654.90
FireEye	Threat Analytics Platform Base Detect 25K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-BD-5Y-USG2	$ 78,695.00	$ 68,464.65
FireEye	Threat Analytics Platform Base Detect 30K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-BD-5Y-USG2	$ 94,435.00	$ 82,158.45
FireEye	Threat Analytics Platform Base Detect 35K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-BD-5Y-USG2	$ 110,175.00	$ 95,852.25
FireEye	Threat Analytics Platform Base Detect 40K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-BD-5Y-USG2	$ 125,910.00	$ 109,541.70
FireEye	Threat Analytics Platform Base Detect 45K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-BD-5Y-USG2	$ 141,650.00	$ 123,235.50
FireEye	Threat Analytics Platform Base Detect 50K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-BD-5Y-USG2	$ 157,390.00	$ 136,929.30
FireEye	Threat Analytics Platform Base Detect 55K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-BD-5Y-USG2	$ 173,130.00	$ 150,623.10
FireEye	Threat Analytics Platform Base Detect 60K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-BD-5Y-USG2	$ 188,870.00	$ 164,316.90
FireEye	Threat Analytics Platform Base Detect 65K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-BD-5Y-USG2	$ 204,605.00	$ 178,006.35
FireEye	Threat Analytics Platform Base Detect 70K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-BD-5Y-USG2	$ 220,345.00	$ 191,700.15
FireEye	Threat Analytics Platform Base Detect 75K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-BD-5Y-USG2	$ 236,085.00	$ 205,393.95

FireEye	Threat Analytics Platform Base Detect 80K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-BD-5Y-USG2	$ 251,825.00	$ 219,087.75
FireEye	Threat Analytics Platform Short Search 1K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-SS-1Y-USG2U	$ 11,632.00	$ 10,119.84
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-SS-1Y-USG2	$ 13,813.00	$ 12,017.31
FireEye	Threat Analytics Platform Short Search 5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-SS-1Y-USG2U	$ 15,731.00	$ 13,685.97
FireEye	Threat Analytics Platform Short Search 10K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-SS-1Y-USG2	$ 23,798.00	$ 20,704.26
FireEye	Threat Analytics Platform Short Search 15K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-SS-1Y-USG2	$ 35,697.00	$ 31,056.39
FireEye	Threat Analytics Platform Short Search 20K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-SS-1Y-USG2	$ 47,597.00	$ 41,409.39
FireEye	Threat Analytics Platform Short Search 25K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-SS-1Y-USG2	$ 59,496.00	$ 51,761.52
FireEye	Threat Analytics Platform Short Search 30K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-SS-1Y-USG2	$ 71,395.00	$ 62,113.65
FireEye	Threat Analytics Platform Short Search 35K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-SS-1Y-USG2	$ 83,294.00	$ 72,465.78
FireEye	Threat Analytics Platform Short Search 40K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-SS-1Y-USG2	$ 95,193.00	$ 82,817.91
FireEye	Threat Analytics Platform Short Search 45K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-SS-1Y-USG2	$ 107,092.00	$ 93,170.04
FireEye	Threat Analytics Platform Short Search 50K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-SS-1Y-USG2	$ 118,992.00	$ 103,523.04
FireEye	Threat Analytics Platform Short Search 55K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-SS-1Y-USG2	$ 130,891.00	$ 113,875.17
FireEye	Threat Analytics Platform Short Search 60K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-SS-1Y-USG2	$ 142,790.00	$ 124,227.30
FireEye	Threat Analytics Platform Short Search 65K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-SS-1Y-USG2	$ 154,689.00	$ 134,579.43
FireEye	Threat Analytics Platform Short Search 70K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-SS-1Y-USG2	$ 166,588.00	$ 144,931.56
FireEye	Threat Analytics Platform Short Search 75K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-SS-1Y-USG2	$ 178,487.00	$ 155,283.69
FireEye	Threat Analytics Platform Short Search 80K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-SS-1Y-USG2	$ 190,386.00	$ 165,635.82
FireEye	Threat Analytics Platform Short Search 1K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-SS-2Y-USG2U	$ 23,264.00	$ 20,239.68
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-SS-2Y-USG2	$ 27,626.00	$ 24,034.62
FireEye	Threat Analytics Platform Short Search 5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-SS-2Y-USG2U	$ 31,462.00	$ 27,371.94
FireEye	Threat Analytics Platform Short Search 10K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-SS-2Y-USG2	$ 47,596.00	$ 41,408.52
FireEye	Threat Analytics Platform Short Search 15K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-SS-2Y-USG2	$ 71,394.00	$ 62,112.78
FireEye	Threat Analytics Platform Short Search 20K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-SS-2Y-USG2	$ 95,194.00	$ 82,818.78
FireEye	Threat Analytics Platform Short Search 25K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-SS-2Y-USG2	$ 118,992.00	$ 103,523.04
FireEye	Threat Analytics Platform Short Search 30K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-SS-2Y-USG2	$ 142,790.00	$ 124,227.30
FireEye	Threat Analytics Platform Short Search 35K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-SS-2Y-USG2	$ 166,588.00	$ 144,931.56
FireEye	Threat Analytics Platform Short Search 40K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-SS-2Y-USG2	$ 190,386.00	$ 165,635.82
FireEye	Threat Analytics Platform Short Search 45K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-SS-2Y-USG2	$ 214,184.00	$ 186,340.08
FireEye	Threat Analytics Platform Short Search 50K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-SS-2Y-USG2	$ 237,984.00	$ 207,046.08
FireEye	Threat Analytics Platform Short Search 55K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-SS-2Y-USG2	$ 261,782.00	$ 227,750.34
FireEye	Threat Analytics Platform Short Search 60K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-SS-2Y-USG2	$ 285,580.00	$ 248,454.60
FireEye	Threat Analytics Platform Short Search 65K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-SS-2Y-USG2	$ 309,378.00	$ 269,158.86
FireEye	Threat Analytics Platform Short Search 70K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-SS-2Y-USG2	$ 333,176.00	$ 289,863.12
FireEye	Threat Analytics Platform Short Search 75K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-SS-2Y-USG2	$ 356,974.00	$ 310,567.38
FireEye	Threat Analytics Platform Short Search 80K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-SS-2Y-USG2	$ 380,772.00	$ 331,271.64
FireEye	Threat Analytics Platform Short Search 1K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-SS-3Y-USG2U	$ 34,896.00	$ 30,359.52
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-SS-3Y-USG2	$ 41,439.00	$ 36,051.93
FireEye	Threat Analytics Platform Short Search 5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-SS-3Y-USG2U	$ 47,193.00	$ 41,057.91
FireEye	Threat Analytics Platform Short Search 10K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-SS-3Y-USG2	$ 71,394.00	$ 62,112.78
FireEye	Threat Analytics Platform Short Search 15K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-SS-3Y-USG2	$ 107,091.00	$ 93,169.17
FireEye	Threat Analytics Platform Short Search 20K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-SS-3Y-USG2	$ 142,791.00	$ 124,228.17
FireEye	Threat Analytics Platform Short Search 25K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-SS-3Y-USG2	$ 178,488.00	$ 155,284.56
FireEye	Threat Analytics Platform Short Search 30K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-SS-3Y-USG2	$ 214,185.00	$ 186,340.95
FireEye	Threat Analytics Platform Short Search 35K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-SS-3Y-USG2	$ 249,882.00	$ 217,397.34
FireEye	Threat Analytics Platform Short Search 40K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-SS-3Y-USG2	$ 285,579.00	$ 248,453.73
FireEye	Threat Analytics Platform Short Search 45K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-SS-3Y-USG2	$ 321,276.00	$ 279,510.12
FireEye	Threat Analytics Platform Short Search 50K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-SS-3Y-USG2	$ 356,976.00	$ 310,569.12

FireEye	Threat Analytics Platform Short Search 55K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-SS-3Y-USG2	$ 392,673.00	$ 341,625.51
FireEye	Threat Analytics Platform Short Search 60K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-SS-3Y-USG2	$ 428,370.00	$ 372,681.90
FireEye	Threat Analytics Platform Short Search 65K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-SS-3Y-USG2	$ 464,067.00	$ 403,738.29
FireEye	Threat Analytics Platform Short Search 70K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-SS-3Y-USG2	$ 499,764.00	$ 434,794.68
FireEye	Threat Analytics Platform Short Search 75K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-SS-3Y-USG2	$ 535,461.00	$ 465,851.07
FireEye	Threat Analytics Platform Short Search 80K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-SS-3Y-USG2	$ 571,158.00	$ 496,907.46
FireEye	Threat Analytics Platform Short Search 1K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-SS-4Y-USG2U	$ 46,528.00	$ 40,479.36
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-SS-4Y-USG2	$ 55,252.00	$ 48,069.24
FireEye	Threat Analytics Platform Short Search 5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-SS-4Y-USG2U	$ 62,924.00	$ 54,743.88
FireEye	Threat Analytics Platform Short Search 10K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-SS-4Y-USG2	$ 95,192.00	$ 82,817.04
FireEye	Threat Analytics Platform Short Search 15K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-SS-4Y-USG2	$ 142,788.00	$ 124,225.56
FireEye	Threat Analytics Platform Short Search 20K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-SS-4Y-USG2	$ 190,388.00	$ 165,637.56
FireEye	Threat Analytics Platform Short Search 25K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-SS-4Y-USG2	$ 237,984.00	$ 207,046.08
FireEye	Threat Analytics Platform Short Search 30K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-SS-4Y-USG2	$ 285,580.00	$ 248,454.60
FireEye	Threat Analytics Platform Short Search 35K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-SS-4Y-USG2	$ 333,176.00	$ 289,863.12
FireEye	Threat Analytics Platform Short Search 40K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-SS-4Y-USG2	$ 380,772.00	$ 331,271.64
FireEye	Threat Analytics Platform Short Search 45K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-SS-4Y-USG2	$ 428,368.00	$ 372,680.16
FireEye	Threat Analytics Platform Short Search 50K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-SS-4Y-USG2	$ 475,968.00	$ 414,092.16
FireEye	Threat Analytics Platform Short Search 55K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-SS-4Y-USG2	$ 523,564.00	$ 455,500.68
FireEye	Threat Analytics Platform Short Search 60K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-SS-4Y-USG2	$ 571,160.00	$ 496,909.20
FireEye	Threat Analytics Platform Short Search 65K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-SS-4Y-USG2	$ 618,756.00	$ 538,317.72
FireEye	Threat Analytics Platform Short Search 70K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-SS-4Y-USG2	$ 666,352.00	$ 579,726.24
FireEye	Threat Analytics Platform Short Search 75K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-SS-4Y-USG2	$ 713,948.00	$ 621,134.76
FireEye	Threat Analytics Platform Short Search 80K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-SS-4Y-USG2	$ 761,544.00	$ 662,543.28
FireEye	Threat Analytics Platform Short Search 1K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-SS-5Y-USG2U	$ 58,160.00	$ 50,599.20
FireEye	Threat Analytics Platform Short Search 2.5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-SS-5Y-USG2	$ 69,065.00	$ 60,086.55
FireEye	Threat Analytics Platform Short Search 5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-SS-5Y-USG2U	$ 78,655.00	$ 68,429.85
FireEye	Threat Analytics Platform Short Search 10K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-SS-5Y-USG2	$ 118,990.00	$ 103,521.30
FireEye	Threat Analytics Platform Short Search 15K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-SS-5Y-USG2	$ 178,485.00	$ 155,281.95
FireEye	Threat Analytics Platform Short Search 20K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-SS-5Y-USG2	$ 237,985.00	$ 207,046.95
FireEye	Threat Analytics Platform Short Search 25K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-SS-5Y-USG2	$ 297,480.00	$ 258,807.60
FireEye	Threat Analytics Platform Short Search 30K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-SS-5Y-USG2	$ 356,975.00	$ 310,568.25
FireEye	Threat Analytics Platform Short Search 35K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-SS-5Y-USG2	$ 416,470.00	$ 362,328.90
FireEye	Threat Analytics Platform Short Search 40K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-SS-5Y-USG2	$ 475,965.00	$ 414,089.55
FireEye	Threat Analytics Platform Short Search 45K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-45KEPS-SS-5Y-USG2	$ 535,460.00	$ 465,850.20
FireEye	Threat Analytics Platform Short Search 50K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-50KEPS-SS-5Y-USG2	$ 594,960.00	$ 517,615.20
FireEye	Threat Analytics Platform Short Search 55K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-55KEPS-SS-5Y-USG2	$ 654,455.00	$ 569,375.85
FireEye	Threat Analytics Platform Short Search 60K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-60KEPS-SS-5Y-USG2	$ 713,950.00	$ 621,136.50
FireEye	Threat Analytics Platform Short Search 65K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-65KEPS-SS-5Y-USG2	$ 773,445.00	$ 672,897.15
FireEye	Threat Analytics Platform Short Search 70K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-70KEPS-SS-5Y-USG2	$ 832,940.00	$ 724,657.80
FireEye	Threat Analytics Platform Short Search 75K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-75KEPS-SS-5Y-USG2	$ 892,435.00	$ 776,418.45
FireEye	Threat Analytics Platform Short Search 80K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-80KEPS-SS-5Y-USG2	$ 951,930.00	$ 828,179.10
FireEye	Threat Analytics Platform Long Search 1K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-LS-1Y-USG2U	$ 24,621.00	$ 21,420.27
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-LS-1Y-USG2	$ 30,049.00	$ 26,142.63
FireEye	Threat Analytics Platform Long Search 5K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-LS-1Y-USG2U	$ 35,214.00	$ 30,636.18
FireEye	Threat Analytics Platform Long Search 10K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-LS-1Y-USG2	$ 56,270.00	$ 48,954.90
FireEye	Threat Analytics Platform Long Search 15K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-LS-1Y-USG2	$ 84,405.00	$ 73,432.35
FireEye	Threat Analytics Platform Long Search 20K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-LS-1Y-USG2	$ 112,541.00	$ 97,910.67
FireEye	Threat Analytics Platform Long Search 25K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-LS-1Y-USG2	$ 140,676.00	$ 122,388.12

FireEye	Threat Analytics Platform Long Search 30K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-LS-1Y-USG2U	$ 168,811.00	$ 146,865.57
FireEye	Threat Analytics Platform Long Search 35K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-LS-1Y-USG2U	$ 196,946.00	$ 171,343.02
FireEye	Threat Analytics Platform Long Search 40K events/sec 1YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-LS-1Y-USG2U	$ 225,081.00	$ 195,820.47
FireEye	Threat Analytics Platform Long Search 1K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-LS-2Y-USG2US	$ 49,242.00	$ 42,840.54
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-LS-2Y-USG2	$ 60,098.00	$ 52,285.26
FireEye	Threat Analytics Platform Long Search 5K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-LS-2Y-USG2US	$ 70,428.00	$ 61,272.36
FireEye	Threat Analytics Platform Long Search 10K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-LS-2Y-USG2U	$ 112,540.00	$ 97,909.80
FireEye	Threat Analytics Platform Long Search 15K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-LS-2Y-USG2U	$ 168,810.00	$ 146,864.70
FireEye	Threat Analytics Platform Long Search 20K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-LS-2Y-USG2U	$ 225,082.00	$ 195,821.34
FireEye	Threat Analytics Platform Long Search 25K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-LS-2Y-USG2U	$ 281,352.00	$ 244,776.24
FireEye	Threat Analytics Platform Long Search 30K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-LS-2Y-USG2U	$ 337,622.00	$ 293,731.14
FireEye	Threat Analytics Platform Long Search 35K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-LS-2Y-USG2U	$ 393,892.00	$ 342,686.04
FireEye	Threat Analytics Platform Long Search 40K events/sec 2YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-LS-2Y-USG2U	$ 450,162.00	$ 391,640.94
FireEye	Threat Analytics Platform Long Search 1K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-LS-3Y-USG2US	$ 73,863.00	$ 64,260.81
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-LS-3Y-USG2	$ 90,147.00	$ 78,427.89
FireEye	Threat Analytics Platform Long Search 5K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-LS-3Y-USG2US	$ 105,642.00	$ 91,908.54
FireEye	Threat Analytics Platform Long Search 10K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-LS-3Y-USG2U	$ 168,810.00	$ 146,864.70
FireEye	Threat Analytics Platform Long Search 15K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-LS-3Y-USG2U	$ 253,215.00	$ 220,297.05
FireEye	Threat Analytics Platform Long Search 20K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-LS-3Y-USG2U	$ 337,623.00	$ 293,732.01
FireEye	Threat Analytics Platform Long Search 25K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-LS-3Y-USG2U	$ 422,028.00	$ 367,164.36
FireEye	Threat Analytics Platform Long Search 30K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-LS-3Y-USG2U	$ 506,433.00	$ 440,596.71
FireEye	Threat Analytics Platform Long Search 35K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-LS-3Y-USG2U	$ 590,838.00	$ 514,029.06
FireEye	Threat Analytics Platform Long Search 40K events/sec 3YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-LS-3Y-USG2U	$ 675,243.00	$ 587,461.41
FireEye	Threat Analytics Platform Long Search 1K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-LS-4Y-USG2US	$ 98,484.00	$ 85,681.08
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-LS-4Y-USG2	$ 120,196.00	$ 104,570.52
FireEye	Threat Analytics Platform Long Search 5K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-LS-4Y-USG2US	$ 140,856.00	$ 122,544.72
FireEye	Threat Analytics Platform Long Search 10K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-LS-4Y-USG2U	$ 225,080.00	$ 195,819.60
FireEye	Threat Analytics Platform Long Search 15K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-LS-4Y-USG2U	$ 337,620.00	$ 293,729.40
FireEye	Threat Analytics Platform Long Search 20K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-LS-4Y-USG2U	$ 450,164.00	$ 391,642.68
FireEye	Threat Analytics Platform Long Search 25K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-LS-4Y-USG2U	$ 562,704.00	$ 489,552.48
FireEye	Threat Analytics Platform Long Search 30K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-LS-4Y-USG2U	$ 675,244.00	$ 587,462.28
FireEye	Threat Analytics Platform Long Search 35K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-LS-4Y-USG2U	$ 787,784.00	$ 685,372.08
FireEye	Threat Analytics Platform Long Search 40K events/sec 4YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-LS-4Y-USG2U	$ 900,324.00	$ 783,281.88
FireEye	Threat Analytics Platform Long Search 1K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-1KEPS-LS-5Y-USG2US	$ 123,105.00	$ 107,101.35
FireEye	Threat Analytics Platform Long Search 2.5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-2.5KEPS-LS-5Y-USG2	$ 150,245.00	$ 130,713.15
FireEye	Threat Analytics Platform Long Search 5K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-5KEPS-LS-5Y-USG2US	$ 176,070.00	$ 153,180.90
FireEye	Threat Analytics Platform Long Search 10K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-10KEPS-LS-5Y-USG2U	$ 281,350.00	$ 244,774.50
FireEye	Threat Analytics Platform Long Search 15K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-15KEPS-LS-5Y-USG2U	$ 422,025.00	$ 367,161.75
FireEye	Threat Analytics Platform Long Search 20K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-20KEPS-LS-5Y-USG2U	$ 562,705.00	$ 489,553.35
FireEye	Threat Analytics Platform Long Search 25K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-25KEPS-LS-5Y-USG2U	$ 703,380.00	$ 611,940.60
FireEye	Threat Analytics Platform Long Search 30K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-30KEPS-LS-5Y-USG2U	$ 844,055.00	$ 734,327.85
FireEye	Threat Analytics Platform Long Search 35K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-35KEPS-LS-5Y-USG2U	$ 984,730.00	$ 856,715.10
FireEye	Threat Analytics Platform Long Search 40K events/sec 5YR - GovUS to GovUS Prio Plus	UP-TAP-40KEPS-LS-5Y-USG2U	$ 1,125,405.00	$ 979,102.35
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 500-999	RN-MC-MSMC-000999-1Y	$ 52.00	$ 45.24
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 500-999	RN-MC-MSMC-000999-2Y	$ 104.00	$ 90.48
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 500-999	RN-MC-MSMC-000999-3Y	$ 140.40	$ 122.15
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 500-999	RN-MC-MSMC-000999-4Y	$ 187.20	$ 162.86
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 1000-1999	RN-MC-MSMC-001999-1Y	$ 43.00	$ 37.41
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 1000-1999	RN-MC-MSMC-001999-2Y	$ 86.00	$ 74.82

FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 1000-1999	RN-MC-MSMC-001999-3Y	$ 116.10	$ 101.01
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 1000-1999	RN-MC-MSMC-001999-4Y	$ 154.80	$ 134.68
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 2000-4999	RN-MC-MSMC-004999-1Y	$ 36.00	$ 31.32
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 2000-4999	RN-MC-MSMC-004999-2Y	$ 72.00	$ 62.64
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 2000-4999	RN-MC-MSMC-004999-3Y	$ 97.20	$ 84.56
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 2000-4999	RN-MC-MSMC-004999-4Y	$ 129.60	$ 112.75
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 5000-9999	RN-MC-MSMC-009999-1Y	$ 30.00	$ 26.10
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 5000-9999	RN-MC-MSMC-009999-2Y	$ 60.00	$ 52.20
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 5000-9999	RN-MC-MSMC-009999-3Y	$ 81.00	$ 70.47
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 5000-9999	RN-MC-MSMC-009999-4Y	$ 108.00	$ 93.96
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 10000-19999	RN-MC-MSMC-019999-1Y	$ 25.00	$ 21.75
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 10000-19999	RN-MC-MSMC-019999-2Y	$ 50.00	$ 43.50
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 10000-19999	RN-MC-MSMC-019999-3Y	$ 67.50	$ 58.73
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 10000-19999	RN-MC-MSMC-019999-4Y	$ 90.00	$ 78.30
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 20000-49999	RN-MC-MSMC-049999-1Y	$ 21.00	$ 18.27
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 20000-49999	RN-MC-MSMC-049999-2Y	$ 42.00	$ 36.54
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 20000-49999	RN-MC-MSMC-049999-3Y	$ 56.70	$ 49.33
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 20000-49999	RN-MC-MSMC-049999-4Y	$ 75.60	$ 65.77
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 50000-74999	RN-MC-MSMC-074999-1Y	$ 17.00	$ 14.79
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 50000-74999	RN-MC-MSMC-074999-2Y	$ 34.00	$ 29.58
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 50000-74999	RN-MC-MSMC-074999-3Y	$ 45.90	$ 39.93
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 50000-74999	RN-MC-MSMC-074999-4Y	$ 61.20	$ 53.24
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 75000-99999	RN-MC-MSMC-099999-1Y	$ 14.00	$ 12.18
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 75000-99999	RN-MC-MSMC-099999-2Y	$ 28.00	$ 24.36
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 75000-99999	RN-MC-MSMC-099999-3Y	$ 37.80	$ 32.89
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 75000-99999	RN-MC-MSMC-099999-4Y	$ 50.40	$ 43.85
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 1 Year 100000+	RN-MC-MSMC-100000+1Y	$ 12.00	$ 10.44
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 2 Year 100000+	RN-MC-MSMC-100000+2Y	$ 24.00	$ 20.88
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 3 Year 100000+	RN-MC-MSMC-100000+3Y	$ 32.40	$ 28.19
FireEye	Renewal-Mobile Threat Prevention - Mobile Security Management Cloud 4 Year 100000+	RN-MC-MSMC-100000+4Y	$ 43.20	$ 37.58
FireEye	MX 900 Appliance Cold Standby- Mobile Threat Prevention - Mobile Security Management	900MX-HWCOLDSB	$ 7,995.00	$ 6,955.65
FireEye	MX 8400 Appliance/Server Cold Standby- Mobile Threat Prevention - Mobile Security Management - Compliance Model AX 8400	8400MX-HWCOLDSB	$ 64,995.00	$ 56,545.65
FireEye	Threat Analytics Platform Short Search 1K events/sec 3M - Platinum-PROMOTION	TAP-1KEPS-SS-3M-P	$ -	$ -
FireEye	Threat Analytics Platform Short Search 1K events/sec 3M - Plat Prio Plus-PROMOTION	TAP-1KEPS-SS-3M-PPP	$ -	$ -
FireEye	Threat Analytics Platform Short Search 1K events/sec 3M - GovUS-PROMOTION	TAP-1KEPS-SS-3M-US	$ -	$ -
FireEye	Threat Analytics Platform Short Search 1K events/sec 3M - GovUS Prio Plus-PROMOTION	TAP-1KEPS-SS-3M-USPP	$ -	$ -
Google	Google Apps for Business: 12 month license/support term; 1 seat;	GAPPS-PREM-1USER-12MO	$ 50.00	$ 48.87
Google	Google Apps for Business Upgrade: 1 month license/support term; 1 seat;	GAPPS-PREM-UPG-1USER-1M	$ 4.17	$ 4.08
Google	Google Apps Vault: 12 month license/support term; 1 seat;	GAPPS-VAULT-1USER-12MO	$ 50.00	$ 48.87
Google	Google Apps Vault Upgrade: 1 month license/support term; 1 seat;	GAPPS-VAULT-UPG-1USER-1	$ 4.17	$ 4.08
Google	Google Apps Unlimited: 12 month license/support term; 1 seat;	GAPPS-UNLIM-1-USER-12-M	$ 120.00	$ 117.28
Google	Google Apps Unlimited Upgrade: 1 month license/support term; 1 seat;	GAPPS-UNLIM-1-USER-1-MO	$ 10.00	$ 9.77
Google	Google Apps Message Encryption: 12 month license/support term; 1 seat;	GAPPS-ME-WITHCOMPOSE-	$ 35.00	$ 34.21
Google	Google Apps Message Encryption Upgrade: 1 month license/support term; 1 seat;	GAPPS-ME-CUSTPRTL-1USER	$ 2.92	$ 2.85
QTS	SOC Reports type II Bundle - Gold NRR	10800100011-000	$ 500.00	$ 488.66
QTS	SOC Reports type II Bundle - Gold MRR	10811100011-000	$ 340.00	$ 332.29
QTS	Security Engineer T&M MRC MRR	10811100016-000	$ 170.00	$ 166.15
QTS	Licensing Services Early Term Fee NRR	11200100003-000	$ 1,010.00	$ 987.10
QTS	Licensing Service Cancellation Fee NRR	11200100004-000	$ 10,100.00	$ 9,871.03

QTS	NetBackup for SQL Server - Tier 1: Single Processor One Time Charge NRR	11200NET00013-000	$ 1,618.75	$ 1,582.05
QTS	Connectivity: MetroConnect Protected 10 Gbps NRR	11400000041-RIC	$ 10,000.00	$ 9,773.30
QTS	Connectivity: IP Bandwith Copper - Setup Fee NRR	11400100001-000	$ 500.00	$ 488.66
QTS	Connectivity: IP Bandwith Fiber - Setup Fee NRR	11400100002-000	$ 1,000.00	$ 977.33
QTS	Connectivity: Copper Cross Connect NRR	11400100003-000	$ 500.00	$ 488.66
QTS	Connectivity: T1 NRR	11400100003-0T1	$ 100.00	$ 97.73
QTS	Connectivity: AT&T Copper Cross Connect NRR	11400100003-ATT	$ 500.00	$ 488.66
QTS	Connectivity: Verizon Business Copper Cross Connect NRR	11400100003-VZB	$ 500.00	$ 488.66
QTS	Connectivity: Verizon Copper Cross Connect NRR	11400100003-VZN	$ 500.00	$ 488.66
QTS	Connectivity: Copper Cross Connect (Home Run) NRR	11400100004-000	$ 2,000.00	$ 1,954.66
QTS	Connectivity: Fiber Cross Connect NRR	11400100005-000	$ 1,000.00	$ 977.33
QTS	Connectivity: AT&T Fiber Cross Connect NRR	11400100005-ATT	$ 1,000.00	$ 977.33
QTS	Connectivity: Verizon Business Fiber Cross Connect NRR	11400100005-VZB	$ 1,000.00	$ 977.33
QTS	Connectivity: Verizon Fiber Cross Connect NRR	11400100005-VZN	$ 1,000.00	$ 977.33
QTS	Connectivity: Fiber Cross Connect (Home Run) NRR	11400100006-000	$ 2,000.00	$ 1,954.66
QTS	Connectivity: MetroConnect Standard 1 Gbps NRR	11400100027-ATL	$ 1,000.00	$ 977.33
QTS	Connectivity: MetroConnect Standard 1 Gbps NRR	11400100027-RIC	$ 2,000.00	$ 1,954.66
QTS	Connectivity: MetroConnect Standard 10 Gbps NRR	11400100028-ATL	$ 5,000.00	$ 4,886.65
QTS	Connectivity: MetroConnect Standard 10 Gbps NRR	11400100028-RIC	$ 10,000.00	$ 9,773.30
QTS	Connectivity: MetroConnect Standard 100 Mbps NRR	11400100034-ATL	$ 1,000.00	$ 977.33
QTS	Connectivity: POTS NRR	11400100035-000	$ 100.00	$ 97.73
QTS	Connectivity: MetroConnect Protected 100 Mbps NRR	11400100039-ATL	$ 1,000.00	$ 977.33
QTS	Connectivity: MetroConnect Protected 1 Gbps NRR	11400100040-ATL	$ 1,000.00	$ 977.33
QTS	Connectivity: MetroConnect Protected 1 Gbps NRR	11400100040-RIC	$ 2,000.00	$ 1,954.66
QTS	Connectivity: MetroConnect Protected 10 Gbps NRR	11400100041-ATL	$ 5,000.00	$ 4,886.65
QTS	Connectivity: Data Center Connect 10MB - Atlanta NRR	11400100045-ATL	$ 300.00	$ 293.20
QTS	Connectivity: Data Center Connect 10MB - Richmond NRR	11400100053-RIC	$ 300.00	$ 293.20
QTS	Connectivity: DC Connect Additional 10Mbps increments (10Mbps-100Mbps) - Atlanta NRR	11400100058-ATL	$ 100.00	$ 97.73
QTS	Connectivity: DC Connect Additional 10Mbps increments (10Mbps-100Mbps) - Richmond NRR	11400100060-RIC	$ 100.00	$ 97.73
QTS	Connectivity: DC Connect Additional 10Mbps increments (110Mbps-500Mbps) - Atlanta NRR	11400100064-ATL	$ 100.00	$ 97.73
QTS	Connectivity: DC Connect Additional 10Mbps increments (110Mbps-500Mbps) - Richmond NRR	11400100066-RIC	$ 100.00	$ 97.73
QTS	Connectivity: DC Connect Additional 10Mbps increments (510Mbps-1Gbps) - Atlanta NRR	11400100070-ATL	$ 100.00	$ 97.73
QTS	Connectivity: DC Connect Additional 10Mbps increments (510Mbps-1Gbps) - Richmond NRR	11400100072-RIC	$ 100.00	$ 97.73
QTS	Connectivity: AT&T Coax Cross Connect NRR	11400100073-ATT	$ 1,000.00	$ 977.33
QTS	Connectivity: Verizon Coax Cross Connect NRR	11400100074-VZN	$ 1,000.00	$ 977.33
QTS	Connectivity: Coax Cross Connect NRR	11400100075-000	$ 1,000.00	$ 977.33
QTS	Connectivity: Copper Cross Connect MRR	11411100021-000	$ 150.00	$ 146.60
QTS	Connectivity: T1 MRR	11411100021-0T1	$ 25.00	$ 24.43
QTS	Connectivity: AT&T Copper Cross Connect MRR	11411100021-ATT	$ 200.00	$ 195.47
QTS	Connectivity: Verizon Business Copper Cross Connect MRR	11411100021-VZB	$ 200.00	$ 195.47
QTS	Connectivity: Verizon Copper Cross Connect MRR	11411100021-VZN	$ 200.00	$ 195.47
QTS	Connectivity: Copper Cross Connect (Home Run) MRR	11411100022-000	$ 5,800.00	$ 5,668.51
QTS	Connectivity: Fiber Cross Connect MRR	11411100023-000	$ 300.00	$ 293.20
QTS	Connectivity: AT&T Fiber Cross Connect MRR	11411100023-ATT	$ 350.00	$ 342.07
QTS	Connectivity: Verizon Business Fiber Cross Connect MRR	11411100023-VNB	$ 350.00	$ 342.07
QTS	Connectivity: Verizon Fiber Cross Connect MRR	11411100023-VZN	$ 350.00	$ 342.07
QTS	Connectivity: Fiber Cross Connect (Home Run) MRR	11411100024-000	$ 2,000.00	$ 1,954.66
QTS	Connectivity: MetroConnect Standard 1 Gbps MRR	11411100027-ATL	$ 1,000.00	$ 977.33
QTS	Connectivity: MetroConnect Standard 1 Gbps MRR	11411100027-RIC	$ 4,500.00	$ 4,397.98

QTS	Connectivity: MetroConnect Standard 10 Gbps MRR	11411100028-ATL	$ 5,000.00	$ 4,886.65
QTS	Connectivity: MetroConnect Standard 10 Gbps MRR	11411100028-RIC	$ 8,500.00	$ 8,307.30
QTS	IP Bandwidth - 1 Gbps port - (1-4 Mbps Commit) MRR	11411100032-G04	$ 100.00	$ 97.73
QTS	IP Bandwidth - 1 Gbps port - (5-9 Mbps Commit) MRR	11411100032-G09	$ 75.00	$ 73.30
QTS	IP Bandwidth - 1 Gbps port - (10-19 Mbps Commit) MRR	11411100032-G19	$ 60.00	$ 58.64
QTS	IP Bandwidth - 1 Gbps port - (500-1000 Mbps Commit) MRR	11411100032-G1G	$ 8.00	$ 7.82
QTS	IP Bandwidth - 1 Gbps port - (100-199 Mbps Commit) MRR	11411100032-G1H	$ 30.00	$ 29.32
QTS	IP Bandwidth - 1 Gbps port - (200-299 Mbps Commit) MRR	11411100032-G2H	$ 25.00	$ 24.43
QTS	IP Bandwidth - 1 Gbps port - (300-399 Mbps Commit) MRR	11411100032-G3H	$ 20.00	$ 19.55
QTS	Space Services - Cage NRR	10000100001-000	$ 48.00	$ 46.91
QTS	Space Services - Cabinet NRR	10000100004-000	$ 975.00	$ 952.90
QTS	Space: Cubicle Space NRR	10000100006-000	$ 100.00	$ 97.73
QTS	Space: Customer Provided Rack Install - One Time Fee NRR	10000100027-000	$ 250.00	$ 244.33
QTS	Space: Rack - (4 Post) NRR	10000100030-000	$ 80.00	$ 78.19
QTS	Space: Rack - (2 Post) NRR	10000100033-000	$ 80.00	$ 78.19
QTS	Space Services: High Density Cabinet 8 kW NRR	10000100056-000	$ 1,500.00	$ 1,465.99
QTS	Space Services: High Density Cabinet 16 kW NRR	10000100057-000	$ 3,600.00	$ 3,518.39
QTS	Space Services: High Density Cage 24 kW NRR	10000100058-000	$ 160.00	$ 156.37
QTS	Space Services: High Density Cage 36 kW + NRR	10000100059-000	$ 160.00	$ 156.37
QTS	Space Services: 3300 sq. ft. Suite - Richmond NRR	10000100066-RIC	$ 80,000.00	$ 78,186.40
QTS	Space Services: 3300 sq. ft. Suite - Metro NRR	10000100067-ATL	$ 80,000.00	$ 78,186.40
QTS	Space Services: 3300 sq. ft. Suite - Suwanee NRR	10000100068-SUW	$ 80,000.00	$ 78,186.40
QTS	Space Services: 3300 sq. ft. Suite - Dallas NRR	10000100069-DFW	$ 80,000.00	$ 78,186.40
QTS	Space Services - Cage MRR	10011100001-000	$ 22.00	$ 21.50
QTS	Space Services - Cabinet MRR	10011100004-000	$ 635.00	$ 620.60
QTS	Space Services - Suite MRR	10011100008-000	$ 30.00	$ 29.32
QTS	Space: Rack - (4 Post) MRR	10011100030-000	$ 40.00	$ 39.09
QTS	Space: Rack - (2 Post) MRR	10011100033-000	$ 40.00	$ 39.09
QTS	Space Services: High Density Cabinet 8 kW MRR	10011100056-000	$ 1,150.00	$ 1,123.93
QTS	Space Services: High Density Cabinet 16 kW MRR	10011100057-000	$ 2,150.00	$ 2,101.26
QTS	Space Services: High Density Cage 24 kW MRR	10011100058-000	$ 40.00	$ 39.09
QTS	Space Services: High Density Cage 36 kW + MRR	10011100059-000	$ 70.00	$ 68.41
QTS	Power 120V 20Amp Primary NRR	10200100001-000	$ 600.00	$ 586.40
QTS	Power 120V 20Amp Primary NRR	10200100001-NYC	$ 1,560.00	$ 1,524.63
QTS	Power 120V 20Amp Redundant NRR	10200100002-000	$ 600.00	$ 586.40
QTS	IP Bandwidth - 1 Gbps port - (20-49 Mbps Commit) MRR	11411100032-G49	$ 50.00	$ 48.87
QTS	IP Bandwidth - 1 Gbps port - (400-499 Mbps Commit) MRR	11411100032-G4H	$ 12.00	$ 11.73
QTS	IP Bandwidth - 1 Gbps port - (50-99 Mbps Commit) MRR	11411100032-G99	$ 40.00	$ 39.09
QTS	IP Bandwidth - 100 Mbps port - (1-4 Mbps Commit) MRR	11411100032-H04	$ 100.00	$ 97.73
QTS	IP Bandwidth - 100 Mbps port - (5-9 Mbps Commit) MRR	11411100032-H09	$ 75.00	$ 73.30
QTS	IP Bandwidth - 100 Mbps port - (10-19 Mbps Commit) MRR	11411100032-H19	$ 60.00	$ 58.64
QTS	IP Bandwidth - 100 Mbps port - (50-100 Mbps Commit) MRR	11411100032-H1H	$ 40.00	$ 39.09
QTS	IP Bandwidth - 100 Mbps port - (20-49 Mbps Commit) MRR	11411100032-H49	$ 50.00	$ 48.87
QTS	IP Bandwidth - 10 Mbps port - (1-4 Mbps Commit) MRR	11411100032-T04	$ 100.00	$ 97.73
QTS	IP Bandwidth - 10 Mbps port - (5-10 Mbps Commit) MRR	11411100032-T10	$ 75.00	$ 73.30
QTS	Connectivity: MetroConnect Standard 100 Mbps MRR	11411100034-ATL	$ 500.00	$ 488.66
QTS	Connectivity: POTS MRR	11411100035-000	$ 25.00	$ 24.43
QTS	Connectivity: MetroConnect Protected 100 Mbps MRR	11411100039-ATL	$ 750.00	$ 733.00
QTS	Connectivity: MetroConnect Protected 1 Gbps MRR	11411100040-ATL	$ 1,500.00	$ 1,465.99

QTS	Connectivity: MetroConnect Protected 1 Gbps MRR	11411100040-RIC	$ 10,000.00	$ 9,773.30
QTS	Connectivity: MetroConnect Protected 10 Gbps MRR	11411100041-ATL	$ 7,500.00	$ 7,329.97
QTS	Connectivity: MetroConnect Protected 10 Gbps MRR	11411100041-RIC	$ 18,000.00	$ 17,591.94
QTS	Connectivity: Data Center Connect 10MB - Atlanta MRR	11411100045-ATL	$ 280.00	$ 273.65
QTS	Connectivity: Data Center Connect 10MB - Richmond MRR	11411100053-RIC	$ 280.00	$ 273.65
QTS	Connectivity: DC Connect Additional 10Mbps increments (10Mbps-100Mbps) - Atlanta MRR	11411100058-ATL	$ 75.00	$ 73.30
QTS	Connectivity: DC Connect Additional 10Mbps increments (10Mbps-100Mbps) - Richmond MRR	11411100060-RIC	$ 75.00	$ 73.30
QTS	Connectivity: DC Connect Additional 10Mbps increments (110Mbps-500Mbps) - Atlanta MRR	11411100064-ATL	$ 60.00	$ 58.64
QTS	Connectivity: DC Connect Additional 10Mbps increments (110Mbps-500Mbps) - Richmond MRR	11411100066-RIC	$ 60.00	$ 58.64
QTS	Connectivity: DC Connect Additional 10Mbps increments (510Mbps-1Gbps) - Atlanta MRR	11411100070-ATL	$ 50.00	$ 48.87
QTS	Power 120V 20Amp Redundant NRR	10200100002-NYC	$ 1,560.00	$ 1,524.63
QTS	Power 120V 30Amp Primary NRR	10200100003-000	$ 600.00	$ 586.40
QTS	Power 120V 30Amp Primary NRR	10200100003-NYC	$ 1,690.00	$ 1,651.69
QTS	Power 120V 30Amp Redundant NRR	10200100004-000	$ 600.00	$ 586.40
QTS	Power 120V 30Amp Redundant NRR	10200100004-NYC	$ 1,690.00	$ 1,651.69
QTS	Power 208v 20Amp Primary NRR	10200100006-000	$ 600.00	$ 586.40
QTS	Power 208v 20Amp Redundant NRR	10200100007-000	$ 600.00	$ 586.40
QTS	Power 208v 30Amp Primary NRR	10200100008-000	$ 600.00	$ 586.40
QTS	Power 208v 30Amp Redundant NRR	10200100009-000	$ 600.00	$ 586.40
QTS	Power 208v 50Amp Primary NRR	10200100010-000	$ 600.00	$ 586.40
QTS	Power 208v 50Amp Redundant NRR	10200100011-000	$ 600.00	$ 586.40
QTS	Power 208v 60Amp Primary NRR	10200100012-000	$ 600.00	$ 586.40
QTS	Power 208v 60Amp Redundant NRR	10200100013-000	$ 600.00	$ 586.40
QTS	Power 3 Phase 208v 20Amp Primary NRR	10200100014-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 20Amp Redundant NRR	10200100015-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 30Amp Primary NRR	10200100016-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 30Amp Primary NRR	10200100016-JCY	$ 1,200.00	$ 1,172.80
QTS	Power 3 Phase 208v 30Amp Redundant NRR	10200100017-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 30Amp Redundant NRR	10200100017-JCY	$ 1,200.00	$ 1,172.80
QTS	Power 3 Phase 208v 50Amp Primary NRR	10200100018-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 50Amp Primary NRR	10200100018-JCY	$ 1,200.00	$ 1,172.80
QTS	Power 3 Phase 208v 50Amp Redundant NRR	10200100019-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 50Amp Redundant NRR	10200100019-JCY	$ 1,200.00	$ 1,172.80
QTS	Power 3 Phase 208v 60Amp Primary NRR	10200100020-000	$ 1,400.00	$ 1,368.26
QTS	Power 3 Phase 208v 60Amp Primary NRR	10200100020-JCY	$ 2,000.00	$ 1,954.66
QTS	Power 3 Phase 208v 60Amp Redundant NRR	10200100021-000	$ 1,400.00	$ 1,368.26
QTS	Connectivity: DC Connect Additional 10Mbps increments (510Mbps-1Gbps) - Richmond MRR	11411100072-RIC	$ 50.00	$ 48.87
QTS	Connectivity: AT&T Coax Cross Connect MRR	11411100073-ATT	$ 250.00	$ 244.33
QTS	Connectivity: Verizon Coax Cross Connect MRR	11411100074-VZN	$ 300.00	$ 293.20
QTS	Connectivity: Coax Cross Connect MRR	11411100075-000	$ 300.00	$ 293.20
QTS	Federal Cloud - DR - Internet Overage MRR	11500000089-000	$ 30.00	$ 29.32
QTS	Federal Cloud - VPU 1 Ghz MRR	11500000097-000	$ 40.00	$ 39.09
QTS	Federal Cloud - RAM 1 GB MRR	11500000098-000	$ 32.00	$ 31.27
QTS	Federal Cloud - Bronze Storage 1GB MRR	11500000099-000	$ 0.41	$ 0.40
QTS	Federal Cloud - Silver Storage 1GB MRR	11500000100-000	$ 0.53	$ 0.52
QTS	Federal Cloud - Gold Storage 1GB MRR	11500000101-000	$ 1.65	$ 1.61
QTS	Federal Cloud - Large Firewall MRR	11500000102-000	$ 225.00	$ 219.90
QTS	Federal Cloud - Internet 1Mbps MRR	11500000103-000	$ 20.00	$ 19.55
QTS	Federal Cloud - Internet Overage MRR	11500000104-000	$ 30.00	$ 29.32

QTS	Federal Cloud - Additional Public IP MRR	11500000105-000	$ 15.00	$ 14.66
QTS	Federal Cloud - Additional Network Segments MRR	11500000106-000	$ 50.00	$ 48.87
QTS	Federal Cloud - Client to Site VPN (Qty 5) MRR	11500000107-000	$ 5.00	$ 4.89
QTS	Federal Cloud - DR - VPU 1Ghz MRR	11500000113-000	$ 23.00	$ 22.48
QTS	Federal Cloud - DR - RAM 1 GB MRR	11500000114-000	$ 19.00	$ 18.57
QTS	Federal Cloud - DR - Bronze Storage 1GB MRR	11500000115-000	$ 0.24	$ 0.23
QTS	Federal Cloud - DR - Silver Storage 1GB MRR	11500000116-000	$ 0.30	$ 0.29
QTS	Federal Cloud - DR -Gold Storage 1GB MRR	11500000117-000	$ 1.23	$ 1.20
QTS	Federal Cloud - DR - Large Firewall MRR	11500000118-000	$ 225.00	$ 219.90
QTS	Federal Cloud - DR - Internet 1Mbps MRR	11500000119-000	$ 20.00	$ 19.55
QTS	Federal Cloud - DR -Additional Public IP MRR	11500000121-000	$ 7.50	$ 7.33
QTS	Federal Cloud - DR - Additional Network Segments MRR	11500000122-000	$ 25.00	$ 24.43
QTS	Power 3 Phase 208v 60Amp Redundant NRR	10200100021-JCY	$ 2,000.00	$ 1,954.66
QTS	Power 120V 20Amp Primary MRR	10211100001-000	$ 360.00	$ 351.84
QTS	Power 120V 20Amp Primary MRR	10211100001-NYC	$ 450.00	$ 439.80
QTS	Power 120V 20Amp Redundant MRR	10211100002-000	$ 90.00	$ 87.96
QTS	Power 120V 20Amp Redundant MRR	10211100002-NYC	$ 225.00	$ 219.90
QTS	Power 120V 30Amp Primary MRR	10211100003-000	$ 520.00	$ 508.21
QTS	Power 120V 30Amp Primary MRR	10211100003-NYC	$ 680.00	$ 664.58
QTS	Power 120V 30Amp Redundant MRR	10211100004-000	$ 130.00	$ 127.05
QTS	Power 120V 30Amp Redundant MRR	10211100004-NYC	$ 340.00	$ 332.29
QTS	Power 208v 20Amp Primary MRR	10211100006-000	$ 600.00	$ 586.40
QTS	Power 208v 20Amp Redundant MRR	10211100007-000	$ 150.00	$ 146.60
QTS	Power 208v 30Amp Primary MRR	10211100008-000	$ 900.00	$ 879.60
QTS	Power 208v 30Amp Redundant MRR	10211100009-000	$ 225.00	$ 219.90
QTS	Power 208v 50Amp Primary MRR	10211100010-000	$ 1,540.00	$ 1,505.09
QTS	Power 208v 50Amp Redundant MRR	10211100011-000	$ 385.00	$ 376.27
QTS	Power 208v 60Amp Primary MRR	10211100012-000	$ 1,760.00	$ 1,720.10
QTS	Power 208v 60Amp Redundant MRR	10211100013-000	$ 440.00	$ 430.03
QTS	Power 3 Phase 208v 20Amp Primary MRR	10211100014-000	$ 1,000.00	$ 977.33
QTS	Power 3 Phase 208v 20Amp Redundant MRR	10211100015-000	$ 250.00	$ 244.33
QTS	Power 3 Phase 208v 30Amp Primary MRR	10211100016-000	$ 1,500.00	$ 1,465.99
QTS	Power 3 Phase 208v 30Amp Primary MRR	10211100016-JCY	$ 2,900.00	$ 2,834.26
QTS	Power 3 Phase 208v 30Amp Redundant MRR	10211100017-000	$ 375.00	$ 366.50
QTS	Power 3 Phase 208v 30Amp Redundant MRR	10211100017-JCY	$ 375.00	$ 366.50
QTS	Power 3 Phase 208v 50Amp Primary MRR	10211100018-000	$ 2,500.00	$ 2,443.32
QTS	Power 3 Phase 208v 50Amp Primary MRR	10211100018-JCY	$ 4,840.00	$ 4,730.28
QTS	Power 3 Phase 208v 50Amp Redundant MRR	10211100019-000	$ 625.00	$ 610.83
QTS	Power 3 Phase 208v 50Amp Redundant MRR	10211100019-JCY	$ 1,210.00	$ 1,182.57
QTS	Power 3 Phase 208v 60Amp Primary MRR	10211100020-000	$ 3,040.00	$ 2,971.08
QTS	Power 3 Phase 208v 60Amp Primary MRR	10211100020-JCY	$ 5,800.00	$ 5,668.51
QTS	Power 3 Phase 208v 60Amp Redundant MRR	10211100021-000	$ 760.00	$ 742.77
QTS	Power 3 Phase 208v 60Amp Redundant MRR	10211100021-JCY	$ 1,450.00	$ 1,417.13
QTS	Power: 500kW - N+1 Configuration - Richmond MRR	10211100102-RIC	$ 80,000.00	$ 78,186.40
QTS	Power: 500kW - N+1 Configuration - Metro MRR	10211100103-ATL	$ 80,000.00	$ 78,186.40
QTS	Power: 500kW - N+1 Configuration - Suwanee MRR	10211100104-SUW	$ 80,000.00	$ 78,186.40
QTS	Power: 500kW - N+1 Configuration - Dallas MRR	10211100105-DFW	$ 80,000.00	$ 78,186.40
QTS	Other Custom Data Center Services NRR	10300100034-000	$ 1.00	$ 0.98
QTS	Other Custom Data Center Services MRR	10311100033-000	$ 1.00	$ 0.98

QTS	DBA/Application Developer MRC NRR	10600100001-000	$ 220.00	$ 215.01
QTS	SQL Base Support NRR	10600100005-000	$ 500.00	$ 488.66
QTS	SQL Base Support Cluster NRR	10600100007-000	$ 1,000.00	$ 977.33
QTS	SQL Engineering T&M NRR	10600100008-000	$ 200.00	$ 195.47
QTS	Application Early Termination Fee NRR	10600100020-000	$ 10,100.00	$ 9,871.03
QTS	Application Service Cancellation Fee NRR	10600100021-000	$ 10,100.00	$ 9,871.03
QTS	SQL Base Support MRR	10611100005-000	$ 1,650.00	$ 1,612.59
QTS	SQL Base Support Cluster MRR	10611100006-000	$ 2,500.00	$ 2,443.32
QTS	SQL Engineering T&M MRR	10611100008-000	$ 200.00	$ 195.47
QTS	DBA/Application Developer MRC MRR	10611100020-000	$ 220.00	$ 215.01
QTS	Basic Monitoring - Unmanaged NRR	10700100001-000	$ 33.84	$ 33.07
QTS	Basic Monitoring -Managed NRR	10700100002-000	$ 33.84	$ 33.07
QTS	Enhanced Monitoring - Unmanaged NRR	10700100003-000	$ 42.30	$ 41.34
QTS	Enhanced Monitoring - Managed NRR	10700100004-000	$ 42.30	$ 41.34
QTS	Advanced Monitoring - Unmanaged NRR	10700100005-000	$ 67.68	$ 66.15
QTS	Enterprise Cloud - Back-up services GB Transferred MRR	11511000093-000	$ 0.18	$ 0.18
QTS	Enterprise Cloud - Back-up services GB Usage MRR	11511000120-000	$ 0.18	$ 0.18
QTS	QVI Backup MRR	11511000039-000	$ 0.20	$ 0.20
QTS	Enterprise Cloud - DR - Bronze Storage 1GB MRR	11511000084-000	$ 0.22	$ 0.22
QTS	DRaaS - Bronze Storage 1GB MRR	11511000145-000	$ 0.22	$ 0.22
QTS	Enterprise Cloud - DR - Silver Storage 1GB MRR	11511000085-000	$ 0.26	$ 0.26
QTS	DRaaS - Silver Storage 1GB MRR	11511000146-000	$ 0.26	$ 0.26
QTS	Enterprise Cloud - Bronze Storage 1GB MRR	11511000068-000	$ 0.33	$ 0.33
QTS	DRaaS - EC Reservation - Bronze Storage 1GB MRR	11511000156-000	$ 0.33	$ 0.33
QTS	DR-SAN Disk Capacity GBs MRR	11511000050-000	$ 0.35	$ 0.35
QTS	Enterprise Cloud - Silver Storage 1GB MRR	11511000069-000	$ 0.41	$ 0.41
QTS	DRaaS - EC Reservation - Silver Storage 1GB MRR	11511000157-000	$ 0.41	$ 0.41
QTS	QVI Additional SAN Storage MRR	11511000020-000	$ 0.41	$ 0.41
QTS	QVI Backup Overage MRR	11500000040-000	$ 0.50	$ 0.50
QTS	QVI Infrastructure Improvement Credit (GSA) MRR	11511000169-000	$ 1.00	$ 0.99
QTS	System Services Custom MRR	10511100014-000	$ 1.00	$ 0.99
QTS	Storage Services Custom MRR	11011100031-000	$ 1.00	$ 0.99
QTS	Licensing Services Custom MRR	11211100001-000	$ 1.00	$ 0.99
QTS	Security Services Custom MRR	10811100013-000	$ 1.00	$ 0.99
QTS	System Services Custom NRR	10500100014-000	$ 1.00	$ 0.99
QTS	Security Services Custom NRR	10800100013-000	$ 1.00	$ 0.99
QTS	Storage Services Custom NRR	11000100039-000	$ 1.00	$ 0.99
QTS	Licensing Services Custom NRR	11200100001-000	$ 1.00	$ 0.99
QTS	QVI Infrastructure Improvement Credit (GSA) NRR	11500000169-000	$ 1.00	$ 0.99
QTS	Additional QVI IP addresses MRR	11511000012-000	$ 1.00	$ 0.99
QTS	Enterprise Cloud - DR -Gold Storage 1GB MRR	11511000086-000	$ 1.03	$ 1.02
QTS	DRaaS - Gold Storage 1GB MRR	11511000147-000	$ 1.03	$ 1.02
QTS	Enterprise Cloud - Gold Storage 1GB MRR	11511000070-000	$ 1.44	$ 1.42
QTS	DRaaS - EC Reservation - Gold Storage 1GB MRR	11511000158-000	$ 1.44	$ 1.42
QTS	Enterprise Cloud- Client to Site VPN (Qty 5) MRR	11511000076-000	$ 4.95	$ 4.85
QTS	Enterprise Cloud - DR- Client to Site VPN (Qty 5) MRR	11511000092-000	$ 4.95	$ 4.85
QTS	DRaaS - Client to Site VPN (Qty 5) MRR	11511000153-000	$ 4.95	$ 4.85
QTS	DRaaS - EC Reservation - Client to Site VPN (Qty 5) MRR	11511000164-000	$ 4.95	$ 4.85
QTS	Additional remote clients for VPN Sessions MRR	11511000014-000	$ 6.50	$ 6.36

QTS	Enterprise Cloud - DR -Additional Public IP MRR	11511000090-000	$ 7.50	$ 7.34
QTS	DRaaS - Additional Public IP MRR	11511000151-000	$ 7.50	$ 7.34
QTS	QVI per port cost (3 Ports are required per physical server) MRR	11511000008-000	$ 12.00	$ 11.73
QTS	Enterprise Cloud - DR - RAM 1 GB MRR	11511000083-000	$ 13.00	$ 12.71
QTS	DRaaS - RAM 1 GB MRR	11511000144-000	$ 13.00	$ 12.71
QTS	Enterprise Cloud - Additional Public IP MRR	11511000074-000	$ 15.00	$ 14.66
QTS	DRaaS - EC Reservation - Additional Public IP MRR	11511000162-000	$ 15.00	$ 14.66
QTS	Enterprise Cloud - DR - VPU 1Ghz MRR	11511000082-000	$ 16.00	$ 15.64
QTS	DRaaS - VPU 1Ghz MRR	11511000143-000	$ 16.00	$ 15.64
QTS	Enterprise Cloud - Internet 1Mbps MRR	11511000072-000	$ 18.00	$ 17.59
QTS	Enterprise Cloud - DR - Internet 1Mbps MRR	11511000088-000	$ 18.00	$ 17.59
QTS	DRaaS - Internet 1Mbps MRR	11511000149-000	$ 18.00	$ 17.59
QTS	DRaaS - EC Reservation - Internet 1Mbps MRR	11511000160-000	$ 18.00	$ 17.59
QTS	Additional IP Bandwidth - QVI MRR	11511000007-000	$ 18.00	$ 17.59
QTS	QVI Additional VM VPU MRR	11511000016-000	$ 21.00	$ 20.52
QTS	DRaaS - EC Reservation - RAM 1 GB MRR	11511000155-000	$ 22.75	$ 22.23
QTS	Enterprise Cloud - RAM 1 GB MRR	11511000067-000	$ 23.00	$ 22.48
QTS	Enterprise Cloud - DR - Additional Network Segments MRR	11511000091-000	$ 25.00	$ 24.43
QTS	DRaaS - Additional Network Segments MRR	11511000152-000	$ 25.00	$ 24.43
QTS	QVI Additional VM RAM MRR	11511000017-000	$ 25.00	$ 24.43
QTS	QVI - Windows Standard MRR	11511000023-000	$ 25.00	$ 24.43
QTS	Enterprise Cloud - Internet Overage MRR	11500000073-000	$ 27.00	$ 26.39
QTS	Enterprise Cloud - DR - Internet Overage MRR	11511000120-001	$ 27.00	$ 26.39
QTS	Enterprise Cloud - VPU 1 Ghz MRR	11511000066-000	$ 27.00	$ 26.39
QTS	DRaaS - Internet Overage MRR	11511000150-000	$ 27.00	$ 26.39
QTS	DRaaS - EC Reservation - VPU 1Ghz MRR	11511000154-000	$ 27.00	$ 26.39
QTS	DRaaS - EC Reservation - Internet Overage MRR	11511000161-000	$ 27.00	$ 26.39
QTS	IP Bandwidth - Bursting Overage - QVI MRR	11411100013-000	$ 27.00	$ 26.39
QTS	Additional Site-To-Site VPN Connection NRR	11500000013-000	$ 30.00	$ 29.32
QTS	Additional remote clients for VPN Sessions NRR	11500000014-000	$ 30.00	$ 29.32
QTS	QVI Active Directory for Windows clustering NRR	11500000028-000	$ 35.00	$ 34.21
QTS	Enterprise Cloud - Cloud Network Port MRR	11511000134-000	$ 35.00	$ 34.21
QTS	Enterprise Cloud - Additional Network Segments MRR	11511000075-000	$ 50.00	$ 48.87
QTS	DRaaS - EC Reservation - Additional Network Segments MRR	11511000163-000	$ 50.00	$ 48.87
QTS	QVI - RedHat Advanced / Enterprise per VM MRR	11511000023-002	$ 55.00	$ 53.75
QTS	Virtual Load Balancing NRR	11500000009-000	$ 60.00	$ 58.64
QTS	QVI Additional VM VPU NRR	11500000016-000	$ 60.00	$ 58.64
QTS	QVI Additional VM RAM NRR	11500000017-000	$ 60.00	$ 58.64
QTS	QVI Network - Pair of redundant virtual Firewalls 1 Site to Site VPN or 5 client to Site 1 Meg of Bandwidth NRR	11500000038-000	$ 60.00	$ 58.64
QTS	DR-VM Additional RAM GBs NRR	11500000048-000	$ 60.00	$ 58.64
QTS	DR-VM Additional VPU NRR	11500000049-000	$ 60.00	$ 58.64
QTS	DRaaS - Replication Service per VM MRR	11511000141-000	$ 60.00	$ 58.64
QTS	Optional Space and Power - 110 20amp Power and 1U rack space. MRR	11511000006-000	$ 65.00	$ 63.53
QTS	DR-HA VM with Replication NRR	11500000055-000	$ 75.00	$ 73.30
QTS	DR - HA Physical Server Windows Standard-Linux NRR	11500000056-000	$ 75.00	$ 73.30
QTS	DR - HA Physical Server Windows Enterprise NRR	11500000057-000	$ 75.00	$ 73.30
QTS	DR - HA Physical Server Windows Data Center NRR	11500000058-000	$ 75.00	$ 73.30
QTS	Enterprise Cloud - Additional Standard Firewall MRR	11511000130-000	$ 75.00	$ 73.30
QTS	Additional Site-To-Site VPN Connection MRR	11511000013-000	$ 80.00	$ 78.19

QTS	Managed VM Server (Includes HA VM OS Management & Licenses Monitoring 40GB useable storage RAID 5 SAN Storage) NRR	11500000005-000	$ 90.00	$ 87.96
QTS	Managed VPN MRR	10911100002-000	$ 91.97	$ 89.89
QTS	Dedicated Storage Management MRR	11011100066-000	$ 100.00	$ 97.73
QTS	Managed Network Hardware MRR	10911100021-000	$ 100.00	$ 97.73
QTS	Managed Network Hardware NRR	10900100021-000	$ 100.00	$ 97.73
QTS	Dedicated Storage Management NRR	11000100066-000	$ 100.00	$ 97.73
QTS	SQL Standard per 2 Core (Min 4 Core) MRR	11211100006-000	$ 119.99	$ 117.27
QTS	Remote Hands & Eyes - Pre-packaged MRR	10311100013-000	$ 120.00	$ 117.28
QTS	Remote Hands & Eyes - Pre-packaged NRR	10300100003-000	$ 120.00	$ 117.28
QTS	DR-HA VM with Replication MRR	11511000055-000	$ 120.00	$ 117.28
QTS	Remote Hands & Eyes MRR	10311100003-000	$ 125.00	$ 122.17
QTS	Remote Hands & Eyes NRR	10300100001-000	$ 125.00	$ 122.17
QTS	QVI - Windows Data Center MRR	11511000023-001	$ 125.00	$ 122.17
QTS	QVI - RedHat Advanced / Enterprise 2 Socket Physical MRR	11511000023-003	$ 125.00	$ 122.17
QTS	DR-VM with Replication MRR	11511000046-000	$ 135.00	$ 131.94
QTS	Virtual Load Balancing MRR	11511000009-000	$ 140.00	$ 136.83
QTS	Additional Subnet Setup Fee NRR	11500000007-000	$ 150.00	$ 146.60
QTS	Additional QVI IP addresses NRR	11500000012-000	$ 150.00	$ 146.60
QTS	QVI Additional SAN Storage NRR	11500000020-000	$ 150.00	$ 146.60
QTS	QVI Backup NRR	11500000039-000	$ 150.00	$ 146.60
QTS	DR-SAN Disk Capacity GBs NRR	11500000050-000	$ 150.00	$ 146.60
QTS	DRaaS - Physical Server replication (P2V) Set-up NRR	11500000142-000	$ 150.00	$ 146.60
QTS	Networking Services Custom MRR	10911100012-000	$ 169.48	$ 165.64
QTS	Networking Services Custom NRR	10900100016-000	$ 169.48	$ 165.64
QTS	Enterprise Cloud - Cloud Engineering Hourly Services MRR	11511000094-001	$ 175.00	$ 171.03
QTS	DRaaS - Physical Server replication (P2V) MRR	11511000142-000	$ 175.00	$ 171.03
QTS	QVI Base Support - Set-up NRR	11500000000-000	$ 200.00	$ 195.47
QTS	SERVER A -Small - Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backup)	11500000001-000	$ 200.00	$ 195.47
QTS	SERVER B - Medium Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backup	11500000002-000	$ 200.00	$ 195.47
QTS	SERVER C -Large Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backup) I	11500000003-000	$ 200.00	$ 195.47
QTS	SERVER D - Custom Config Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape	11500000004-000	$ 200.00	$ 195.47
QTS	Managed OS Windows MRR	10511100002-000	$ 202.41	$ 197.82
QTS	Managed OS Linux MRR	10511100004-000	$ 202.41	$ 197.82
QTS	Managed OS Solaris MRR	10511100006-000	$ 202.41	$ 197.82
QTS	Enterprise Cloud - Large Firewall MRR	11511000071-000	$ 225.00	$ 219.90
QTS	Enterprise Cloud - DR - Large Firewall MRR	11511000087-000	$ 225.00	$ 219.90
QTS	DRaaS - EC Reservation - Large Firewall MRR	11511000159-000	$ 225.00	$ 219.90
QTS	Basic Monitoring - Unmanaged MRR	10711100001-000	$ 46.06	$ 45.02
QTS	Basic Monitoring -Managed MRR	10711100002-000	$ 102.46	$ 100.14
QTS	Enhanced Monitoring - Unmanaged MRR	10711100003-000	$ 68.57	$ 67.02
QTS	Enhanced Monitoring - Managed MRR	10711100004-000	$ 124.97	$ 122.14
QTS	Advanced Monitoring - Unmanaged MRR	10711100005-000	$ 113.69	$ 111.11
QTS	Advanced Monitoring - Managed MRR	10711100006-000	$ 170.09	$ 166.23
QTS	Monitoring Internet Services - Unmanaged MRR	10711100013-000	$ 25.00	$ 24.43
QTS	Monitoring Internet Services - Managed MRR	10711100014-000	$ 100.00	$ 97.73
QTS	Monitoring Engineering T&M MRR	10711100021-000	$ 169.20	$ 165.36
QTS	Security Engineer T&M MRC NRR	10800100003-000	$ 170.00	$ 166.15
QTS	SOC Report - Second Report Distribution NRR	10800100005-000	$ 500.00	$ 488.66
QTS	DR - HA Physical Server Windows Data Center MRR	11511000058-000	$ 750.00	$ 733.00

QTS	SERVER B - Medium -Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backu	11511000002-000	$ 900.00	$ 879.60
QTS	DRaaS - Replication Service -Set-up NRR	11500000141-000	$ 1,000.00	$ 977.33
QTS	SERVER C - Large Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backup) I	11511000003-000	$ 1,150.00	$ 1,123.93
QTS	SERVER D - Custom Config - Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape	11511000004-000	$ 1,750.00	$ 1,710.33
QTS	DR - Additional Client to Site VPN MRR	11511000064-000	$ 8.00	$ 7.83
QTS	DR-VM Additional RAM GBs MRR	11511000048-000	$ 15.00	$ 14.66
QTS	DR-VM Additional VPU MRR	11511000049-000	$ 15.00	$ 14.66
QTS	DR- Additional Site to Site VPN MRR	11511000065-000	$ 25.00	$ 24.43
QTS	DR - HA Data Center Connect Base Fee MRR	11511000059-000	$ 200.00	$ 195.47
QTS	DR-On Demand Base Network MRR	11511000047-000	$ 340.00	$ 332.29
QTS	Federal Cloud - DR- Client to Site VPN (Qty 5) MRR	11500000123-000	$ 5.00	$ 4.89
QTS	Federal Cloud - Back-up services -GB Transferred MRR	11500000124-000	$ 0.24	$ 0.23
QTS	Federal Cloud - Cloud Engineering Services Hourly MRR	11511000094-000	$ 175.00	$ 171.03
QTS	VM Cloud Credit	11511000165-000	$ 1.00	$ 0.98
QTS	Advanced Monitoring - Managed NRR	10700100006-000	$ 67.68	$ 66.15
QTS	Monitoring Internet Services - Unmanaged NRR	10700100013-000	$ 50.00	$ 48.87
QTS	Monitoring Internet Services - Managed NRR	10700100014-000	$ 50.00	$ 48.87
QTS	Monitoring Engineering T&M NRR	10700100017-000	$ 169.20	$ 165.36
QTS	Managed Router MRR	10911100017-000	$ 239.12	$ 233.70
QTS	Managed OS Windows NRR	10500100002-000	$ 250.00	$ 244.33
QTS	Managed OS Linux NRR	10500100004-000	$ 250.00	$ 244.33
QTS	Managed OS Solaris NRR	10500100006-000	$ 250.00	$ 244.33
QTS	QVI Network Only - Connection back to Colo Space. (requires managed switch per standard cost). NRR	11500000015-000	$ 250.00	$ 244.33
QTS	Managed VM Server (Includes HA VM OS Management & Licenses Monitoring 40GB useable storage RAID 5 SAN Storage) MRR	11511000005-000	$ 250.00	$ 244.33
QTS	QVI Active Directory for Windows clustering MRR	11511000028-000	$ 250.00	$ 244.33
QTS	QVI - RedHat Advanced / Enterprise 4 Socket Physical MRR	11511000023-004	$ 250.00	$ 244.33
QTS	Managed Switch MRR	10911100009-000	$ 266.32	$ 260.28
QTS	Standard Load Balancing NRR	10900100006-000	$ 271.17	$ 265.02
QTS	QVI Base Support MRR	11511000000-000	$ 275.00	$ 268.77
QTS	Standard Load Balancing MRR	10911100006-000	$ 278.34	$ 272.03
QTS	DR - HA Physical Server Windows Standard-Linux MRR	11511000056-000	$ 280.00	$ 273.65
QTS	QVI Network - Pair of redundant virtual Firewalls 1 Site to Site VPN or 5 client to Site 1 Meg of Bandwidth MRR	11511000038-000	$ 285.00	$ 278.54
QTS	Managed OS AIX MRR	10511100007-000	$ 315.64	$ 308.48
QTS	HA Load Balancing MRR	10911100007-000	$ 326.51	$ 319.11
QTS	Managed VPN NRR	10900100002-000	$ 338.96	$ 331.28
QTS	On-Clouding MRR	11500000137-000	$ 350.00	$ 342.07
QTS	Firewall Management MRR	10911100004-000	$ 358.89	$ 350.75
QTS	DR-On Demand Base Network NRR	11500000047-000	$ 375.00	$ 366.50
QTS	Managed Switch NRR	10900100009-000	$ 406.78	$ 397.56
QTS	Firewall Management (HA Pair) MRR	10911100005-000	$ 407.06	$ 397.83
QTS	Managed OS AIX NRR	10500100007-000	$ 422.41	$ 412.83
QTS	HA Load Balancing NRR	10900100007-000	$ 440.65	$ 430.66
QTS	DR - HA Physical Server Windows Enterprise MRR	11511000057-000	$ 450.00	$ 439.80
QTS	SQL Enterprise - per 2 Core (Min 4 Core) MRR	11211100007-000	$ 460.15	$ 449.72
QTS	Managed Router NRR	10900100017-000	$ 474.55	$ 463.79
QTS	Firewall Management NRR	10900100004-000	$ 508.45	$ 496.92
QTS	QVI Network Only - Connection back to Colo Space. (requires managed switch per standard cost). MRR	11511000015-000	$ 600.00	$ 586.40
QTS	SERVER A - Small - Managed Linux/Windows Server (Includes hardware OS Management Anti-virus Monitoring 300GB Transfer per month Tape Backup)	11511000001-000	$ 675.00	$ 659.70
QTS	Firewall Management (HA Pair) NRR	10900100005-000	$ 677.93	$ 662.56

Salesforce.com	Console for Sales Cloud	204-1535	$ 120.00	$ 114.91
Salesforce.com	Console for Sales Cloud Government Cloud	204-1535GC	$ 36.00	$ 34.46
Salesforce.com	Identity Connect	204-1536	$ 12.00	$ 11.49
Salesforce.com	Identity Connect Government Cloud	204-1536GC	$ 3.60	$ 3.45
Salesforce.com	Pardot - Standard (price is per org)	204-1537	$ 12,000.00	$ 11,490.98
Salesforce.com	Pardot - Pro (price is per org)	204-1538	$ 24,000.00	$ 22,981.96
Salesforce.com	Pardot - Ultimate (price is per org)	204-1539	$ 36,000.00	$ 34,472.95
Salesforce.com	Premier Success Plan Professional Edition (Service Cloud)	204-1540	$ 117.00	$ 111.99
Salesforce.com	Premier Success Plan Enterprise Edition (Service Cloud)	204-1541	$ 243.00	$ 232.59
Salesforce.com	Premier+ Success Plan Professional Edition (Service Cloud)	204-1542	$ 195.00	$ 186.65
Salesforce.com	Premier+ Success Plan Enterprise Edition (Service Cloud)	204-1543	$ 405.00	$ 387.66
Salesforce.com	Premier Success Plan Enterprise Edition (Force Enterprise Edition)	204-1544	$ 144.00	$ 137.83
Salesforce.com	Premier+ Success Plan Enterprise Edition (Force Enterprise Edition)	204-1545	$ 240.00	$ 229.72
Salesforce.com	Customer Community Members Sandbox (100 Members)	204-1554	$ 1,800.00	$ 1,722.92
Salesforce.com	Customer Community Members Sandbox (500 Members)	204-1555	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Members Sandbox (5000 Members)	204-1556	$ 14,400.00	$ 13,783.38
Salesforce.com	Customer Community Members Sandbox (25000 Members)	204-1557	$ 36,000.00	$ 34,458.44
Salesforce.com	Customer Community Members Sandbox (250000 Members)	204-1558	$ 180,000.00	$ 172,292.19
Salesforce.com	Customer Community Logins Sandbox (2000 Logins/Month)	204-1559	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Logins Sandbox (20000 Logins/Month)	204-1560	$ 14,400.00	$ 13,783.38
Salesforce.com	Customer Community Logins Sandbox (100000 Logins/Month)	204-1561	$ 36,000.00	$ 34,458.44
Salesforce.com	Customer Community Logins Sandbox (1000000 Logins/Month)	204-1562	$ 180,000.00	$ 172,292.19
Salesforce.com	Customer Community Plus (20 Members)	204-1563	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Plus (20 Members) Government Cloud	204-1563GC	$ 1,080.00	$ 1,033.75
Salesforce.com	Customer Community Plus (100 Members)	204-1564	$ 12,000.00	$ 11,486.15
Salesforce.com	Customer Community Plus (100 Members) Government Cloud	204-1564GC	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Plus (200 Logins/Month)	204-1565	$ 8,400.00	$ 8,040.30
Salesforce.com	Expansion Pack for PE	204-1148	$ 420.00	$ 402.19
Salesforce.com	Content Add-on for UE	204-1160	$ 420.00	$ 402.19
Salesforce.com	Content Edition for UE	204-1161	$ 420.00	$ 402.19
Salesforce.com	Ideas Only User	204-1163	$ 60.00	$ 57.45
Salesforce.com	Force.com Sites 1 Million Additional Page Views	204-1169	$ 12,000.00	$ 11,490.98
Salesforce.com	Marketing for PE	204-1170	$ 1,800.00	$ 1,723.65
Salesforce.com	Expansion Pack for PE Premium Support	204-1190	$ 63.00	$ 60.33
Salesforce.com	Web Services API for PE Premium Support	204-1191	$ 45.00	$ 43.09
Salesforce.com	Content Add-on for PE Premium Support	204-1192	$ 63.00	$ 60.33
Salesforce.com	Content Edition for PE Premium Support	204-1193	$ 63.00	$ 60.33
Salesforce.com	Salesforce for Force.com Edition Admin for EE Premium Support	204-1194	$ 90.00	$ 86.19
Salesforce.com	Salesforce Mobile for Partner Portal for EE Premium Support	204-1195	$ 45.00	$ 43.09
Salesforce.com	Sales Cloud Group Edition	204-1300	$ 300.00	$ 287.27
Salesforce.com	Sales Cloud Professional Edition	204-1301	$ 780.00	$ 746.91
Salesforce.com	Sales Cloud Enterprise Edition	204-1302	$ 1,500.00	$ 1,436.37
Salesforce.com	Sales Cloud Enterprise Edition Government Cloud	204-1302GC	$ 450.00	$ 430.73
Salesforce.com	Sales Cloud Unlimited Edition	204-1303	$ 3,000.00	$ 2,872.75
Salesforce.com	Sales Cloud Unlimited Edition Government Cloud	204-1303GC	$ 150.00	$ 143.58
Salesforce.com	Sales Cloud Contact Manager Edition	204-1304	$ 60.00	$ 57.45
Salesforce.com	Service Cloud Professional Edition	204-1305	$ 780.00	$ 746.91
Salesforce.com	Service Cloud Enterprise Edition	204-1306	$ 1,620.00	$ 1,551.28
Salesforce.com	Service Cloud Enterprise Edition Government Cloud	204-1306GC	$ 486.00	$ 465.19

Salesforce.com	Service Cloud Unlimited Edition	204-1307	$ 3,120.00	$ 2,987.66
Salesforce.com	Service Cloud Unlimited Edition Government Cloud	204-1307GC	$ 156.00	$ 149.32
Salesforce.com	Service Cloud Knowledge Pack Enterprise Edition	204-1308	$ 2,220.00	$ 2,125.83
Salesforce.com	Service Cloud Knowledge Pack Enterprise Edition Government Cloud	204-1308GC	$ 666.00	$ 637.48
Salesforce.com	Service Cloud Knowledge Pack Unlimited Edition	204-1309	$ 3,720.00	$ 3,562.21
Salesforce.com	Service Cloud Knowledge Pack Unlimited Edition Government Cloud	204-1309GC	$ 186.00	$ 178.04
Salesforce.com	Chatter Plus Professional	204-1310	$ 180.00	$ 172.36
Salesforce.com	Chatter Plus Enterprise	204-1311	$ 180.00	$ 172.36
Salesforce.com	Chatter Plus Enterprise Government Cloud	204-1311GC	$ 54.00	$ 51.69
Salesforce.com	Chatter Plus Unlimted	204-1312	$ 180.00	$ 172.36
Salesforce.com	Chatter Plus Unlimted Government Cloud	204-1312GC	$ 9.00	$ 8.61
Salesforce.com	Knowledge Only Enterprise Edition	204-1313	$ 600.00	$ 574.55
Salesforce.com	Knowledge Only Enterprise Edition Government Cloud	204-1313GC	$ 180.00	$ 172.29
Salesforce.com	Knowledge Only Unlimited Edition	204-1314	$ 600.00	$ 574.55
Salesforce.com	Knowledge Only Unlimited Edition Government Cloud	204-1314GC	$ 30.00	$ 28.72
Salesforce.com	Force.com Enterprise Edition	204-1315	$ 600.00	$ 574.55
Salesforce.com	Force.com Enterprise Edition Government Cloud	204-1315GC	$ 288.00	$ 275.67
Salesforce.com	Force.com Unlimited Edition	204-1316	$ 900.00	$ 861.82
Salesforce.com	Force.com Unlimited Edition Government Cloud	204-1316GC	$ 90.00	$ 86.15
Salesforce.com	Force.com (One App) Enterprise Edition	204-1317	$ 180.00	$ 172.36
Salesforce.com	Force.com (One App) Unlimted Edition	204-1318	$ 180.00	$ 172.36
Salesforce.com	Force.com (Admin) Enterprise Edition	204-1319	$ 600.00	$ 574.55
Salesforce.com	Force.com (Admin) Unlimited Edition	204-1320	$ 900.00	$ 861.82
Salesforce.com	Additional API Calls - 10000 per day (price is per org) Professional	204-1321	$ 300.00	$ 287.27
Salesforce.com	Additional API Calls - 10000 per day (price is per org) Enterprise	204-1322	$ 300.00	$ 287.27
Salesforce.com	Additional API Calls - 10000 per day (price is per org) Unlimted	204-1323	$ 300.00	$ 287.27
Salesforce.com	Analytics - 5 Additional Dynamic Dashboards (price is per org) Enterprise	204-1324	$ 3,000.00	$ 2,872.75
Salesforce.com	Analytics - 5 Additional Dynamic Dashboards (price is per org) Unlimited	204-1325	$ 3,000.00	$ 2,872.75
Salesforce.com	Analytics - 1 Add'l Sched. Dashboards per Hour (price is per org) Enterprise	204-1326	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 1 Add'l Sched. Dashboards per Hour (price is per org) Unlimited	204-1327	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 1 Add'l Sched. Reports per Hour (price is per org) Enterprise	204-1328	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 1 Add'l Sched. Reports per Hour (price is per org) Unlimted	204-1329	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 1 Add'l Sched. Snapshots per Hour (price is per org) Enterprise	204-1330	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 1 Add'l Sched. Snapshots per Hour (price is per org) Unlimited	204-1331	$ 6,000.00	$ 5,745.49
Salesforce.com	Data Storage (50MB) (price is per org) Group Edition	204-1332	$ 300.00	$ 287.27
Salesforce.com	Data Storage (50MB) (price is per org) Professional Edition	204-1333	$ 300.00	$ 287.27
Salesforce.com	Data Storage (50MB) (price is per org) Enterprise Edition	204-1334	$ 300.00	$ 287.27
Salesforce.com	Data Storage (50MB) (price is per org) Enterprise Edition Government Cloud	204-1334GC	$ 90.00	$ 86.15
Salesforce.com	Data Storage (50MB) (price is per org) Unlimited Edition	204-1335	$ 300.00	$ 287.27
Salesforce.com	Data Storage (50MB) (price is per org) Unlimited Edition Government Cloud	204-1335GC	$ 15.00	$ 14.36
Salesforce.com	Data Storage (500MB) (price is per org) Group Edition	204-1336	$ 1,500.00	$ 1,436.37
Salesforce.com	Data Storage (500MB) (price is per org) Professional Edition	204-1337	$ 1,500.00	$ 1,436.37
Salesforce.com	Data Storage (500MB) (price is per org) Enterprise Edition	204-1338	$ 1,500.00	$ 1,436.37
Salesforce.com	Data Storage (500MB) (price is per org) Enterprise Edition Government Cloud	204-1338GC	$ 450.00	$ 430.73
Salesforce.com	Data Storage (500MB) (price is per org) Unlimited Edition	204-1339	$ 1,500.00	$ 1,436.37
Salesforce.com	Data Storage (500MB) (price is per org) Unlimited Edition Government Cloud	204-1339GC	$ 75.00	$ 71.79
Salesforce.com	Expansion Pack Professional Edition	204-1340	$ 420.00	$ 402.19
Salesforce.com	Expansion Pack Enterprise Edition	204-1341	$ 420.00	$ 402.19
Salesforce.com	File Storage (1GB) (price is per org)	204-1342	$ 60.00	$ 57.45

Salesforce.com	File Storage (1GB) (price is per org) Government Cloud	204-1342GC	$ 18.00	$ 17.23
Salesforce.com	File Storage (10GB) (price is per org)	204-1343	$ 498.00	$ 476.88
Salesforce.com	File Storage (10GB) (price is per org) Government Cloud	204-1343GC	$ 149.40	$ 143.00
Salesforce.com	Heroku Starter	204-1344	$ 48,000.00	$ 45,963.93
Salesforce.com	Heroku Small	204-1345	$ 96,000.00	$ 91,927.86
Salesforce.com	Heroku Medium	204-1346	$ 192,000.00	$ 183,855.72
Salesforce.com	Heroku Large	204-1347	$ 384,000.00	$ 367,711.44
Salesforce.com	Knowledge Enterprise Edition	204-1348	$ 600.00	$ 574.55
Salesforce.com	Knowledge Unlimted Edition	204-1349	$ 600.00	$ 574.55
Salesforce.com	Live Agent Enterprise Edition	204-1350	$ 600.00	$ 574.55
Salesforce.com	Live Agent Unlimted Edition	204-1351	$ 600.00	$ 574.55
Salesforce.com	Mobile	204-1352	$ 600.00	$ 574.55
Salesforce.com	Offline	204-1353	$ 300.00	$ 287.27
Salesforce.com	Profiles and Page Layouts	204-1354	$ 300.00	$ 287.27
Salesforce.com	Salesforce for Google Apps	204-1355	$ 120.00	$ 114.91
Salesforce.com	Web Services API	204-1362	$ 300.00	$ 287.27
Salesforce.com	Weekly Export Service (price per org)	204-1363	$ 600.00	$ 574.55
Salesforce.com	Site.com Contributor-only (User License)	204-1369	$ 240.00	$ 229.82
Salesforce.com	Site.com Publisher-only (User License)	204-1370	$ 1,500.00	$ 1,436.37
Salesforce.com	Site.com Contributor (Feature License)	204-1371	$ 240.00	$ 229.82
Salesforce.com	Site.com Publisher (Feature License)	204-1372	$ 1,500.00	$ 1,436.37
Salesforce.com	Site.com Published Site (price is per site)	204-1373	$ 18,000.00	$ 17,236.47
Salesforce.com	Database.com (Standard Users)	204-1374	$ 120.00	$ 114.91
Salesforce.com	Database.com (100 Lite Users)	204-1375	$ 120.00	$ 114.91
Salesforce.com	Database.com (Administrator)	204-1376	$ 120.00	$ 114.91
Salesforce.com	Additional Records (100000) (price is per org)	204-1377	$ 120.00	$ 114.91
Salesforce.com	Additional Transactions (5000 per day) (price is per org)	204-1378	$ 120.00	$ 114.91
Salesforce.com	Authenticated Sites (100 Named Users)	204-1379	$ 1,200.00	$ 1,149.10
Salesforce.com	Authenticated Sites (1000 Named Users)	204-1380	$ 6,000.00	$ 5,745.49
Salesforce.com	Authenticated Sites (5000 Named Users)	204-1381	$ 18,000.00	$ 17,236.47
Salesforce.com	Authenticated Sites (25000 Named Users)	204-1382	$ 60,000.00	$ 57,454.91
Salesforce.com	Authenticated Sites (5000 Logins/month)	204-1383	$ 6,000.00	$ 5,745.49
Salesforce.com	Authenticated Sites (20000 Logins/month)	204-1384	$ 18,000.00	$ 17,236.47
Salesforce.com	Authenticated Sites (100000 Logins/month)	204-1385	$ 60,000.00	$ 57,454.91
Salesforce.com	Service Cloud Portal (100 Named Users)	204-1386	$ 6,000.00	$ 5,745.49
Salesforce.com	Service Cloud Portal (1000 Named Users)	204-1387	$ 24,000.00	$ 22,981.96
Salesforce.com	Service Cloud Portal (5000 Named Users)	204-1388	$ 60,000.00	$ 57,454.91
Salesforce.com	Service Cloud Portal (25000 Named Users)	204-1389	$ 120,000.00	$ 114,909.82
Salesforce.com	Service Cloud Portal (5000 Logins/month)	204-1390	$ 24,000.00	$ 22,981.96
Salesforce.com	Service Cloud Portal (20000 Logins/month)	204-1391	$ 60,000.00	$ 57,454.91
Salesforce.com	Service Cloud Portal (100000 Logins/month)	204-1392	$ 120,000.00	$ 114,909.82
Salesforce.com	Customer Portal - Enterprise Administration (1 Login/mo)	204-1393	$ 48.00	$ 45.96
Salesforce.com	Customer Portal - Enterprise Administration (Named User)	204-1394	$ 120.00	$ 114.91
Salesforce.com	Partner Portal (Named User)	204-1395	$ 420.00	$ 402.19
Salesforce.com	Content for Partner Portal and Customer Portal	204-1396	$ 420.00	$ 402.19
Salesforce.com	Mobile for Partner Portal	204-1397	$ 300.00	$ 287.27
Salesforce.com	Sites Pageviews (1 Million/month) - (price is per org)	204-1398	$ 12,000.00	$ 11,490.98
Salesforce.com	Chatter Answers for Portal Users (Logins/month)	204-1399	$ 2.40	$ 2.30
Salesforce.com	Chatter Answers for Portal Users (Named)	204-1400	$ 12.00	$ 11.49

Salesforce.com	Marketing Cloud Package Enterprise	204-1401	$ 480,000.00	$ 459,639.29
Salesforce.com	Radian6 Basic	204-1402	$ 12,000.00	$ 11,490.98
Salesforce.com	Radian6 Pro	204-1403	$ 36,000.00	$ 34,472.95
Salesforce.com	Radian6 Corporate	204-1404	$ 96,000.00	$ 91,927.86
Salesforce.com	Radian6 Enterprise	204-1405	$ 348,000.00	$ 333,238.49
Salesforce.com	R6 Add on Insights Credits (10000)	204-1406	$ 1,200.00	$ 1,149.10
Salesforce.com	R6 Add on 50000 additional mentions	204-1407	$ 12,000.00	$ 11,490.98
Salesforce.com	R6 Add on 1 million additional mentions	204-1408	$ 60,000.00	$ 57,454.91
Salesforce.com	R6 Add on Social Accounts	204-1409	$ 9,000.00	$ 8,618.24
Salesforce.com	R6 Add on PT: Optimize Your Topic Profile	204-1410	$ 3,000.00	$ 2,872.75
Salesforce.com	R6 Add on Topic Management Service (1 x fee)	204-1411	$ 6,000.00	$ 5,745.49
Salesforce.com	R6 Add on Topic management Service (monthly)	204-1412	$ 6,000.00	$ 5,745.49
Salesforce.com	R6 Add on Topic Management Service (TSS)	204-1413	$ 6,000.00	$ 5,745.49
Salesforce.com	R6 Add on Rapid TSS (RTSS)	204-1414	$ 12,000.00	$ 11,490.98
Salesforce.com	R6 Add on TSS/RTSS Additional Keyword	204-1415	$ 1,800.00	$ 1,723.65
Salesforce.com	R6 Add on TSS/RTSS Additional Dashboard	204-1416	$ 3,000.00	$ 2,872.75
Salesforce.com	Brand Overview Report	204-1417	$ 5,000.00	$ 4,787.91
Salesforce.com	On-Site Training (Price is per day + expenses minimum 2 days)	204-1418	$ 2,500.00	$ 2,393.95
Salesforce.com	Social Media Analyst (on going) FT	204-1419	$ 108,000.00	$ 103,418.84
Salesforce.com	Social Media Analyst (on going) HT	204-1420	$ 60,000.00	$ 57,454.91
Salesforce.com	Social Media Senior Analyst (on-going) FT	204-1421	$ 144,000.00	$ 137,891.79
Salesforce.com	Social Media Senior Analyst (on-going) HT	204-1422	$ 78,000.00	$ 74,691.39
Salesforce.com	Project Manager FT	204-1423	$ 192,000.00	$ 183,855.72
Salesforce.com	Project Manager HT	204-1424	$ 103,680.00	$ 99,282.09
Salesforce.com	Project Manager QT	204-1425	$ 59,520.00	$ 56,995.27
Salesforce.com	Command Center CVE (on-going)	204-1426	$ 5,000.00	$ 4,787.91
Salesforce.com	Embedded Edition User for Acumen Schoolforce Silver Application (1-499 users)	204-1427	$ 125.00	$ 119.70
Salesforce.com	Embedded Edition User for Acumen Schoolforce Silver Application (500-2000 users)	204-1428	$ 89.00	$ 85.22
Salesforce.com	Embedded Edition User for Acumen Schoolforce Silver Application (2000+ users)	204-1429	$ 70.00	$ 67.03
Salesforce.com	Embedded Edition User for Acumen Schoolforce Gold Application (1-499 users)	204-1430	$ 154.00	$ 147.47
Salesforce.com	Embedded Edition User for Acumen Schoolforce Gold Application (500-2000 users)	204-1431	$ 111.00	$ 106.29
Salesforce.com	Embedded Edition User for Acumen Schoolforce Gold Application (2000+ users)	204-1432	$ 85.00	$ 81.39
Salesforce.com	ISV Portal Bundle for Acumen Schoolforce Gold Application (Bundles include 100 ISV Portal licenses)	204-1433	$ 341.00	$ 326.54
Salesforce.com	Data Storage for Schoolforce Gold (500MB) (price is per org)	204-1434	$ 2,273.00	$ 2,176.58
Salesforce.com	Marketing Cloud Package Basic	204-1435	$ 60,000.00	$ 57,454.91
Salesforce.com	Marketing Cloud Package Pro	204-1436	$ 120,000.00	$ 114,909.82
Salesforce.com	Marketing Cloud Package Corporate	204-1437	$ 240,000.00	$ 229,819.65
Salesforce.com	Buddy Media Enterprise	204-1438	$ 480,000.00	$ 459,639.29
Salesforce.com	Buddy Media (stand alone)	204-1439	$ 45,000.00	$ 43,091.18
Salesforce.com	Buddy Social Accounts	204-1440	$ 9,000.00	$ 8,618.24
Salesforce.com	Buddy Media 1 million additional open web sharing PV's	204-1441	$ 1,020.00	$ 976.73
Salesforce.com	Buddy Media 1 million additional open web syndication PV's	204-1442	$ 1,020.00	$ 976.73
Salesforce.com	Buy Buddy	204-1443	$ 6,000.00	$ 5,745.49
Salesforce.com	Buddy Social Account Reports	204-1444	$ 9,600.00	$ 9,192.79
Salesforce.com	Buddy Aggregate Dashboard Reports	204-1445	$ 12,000.00	$ 11,490.98
Salesforce.com	Buddy Quarterly Content	204-1446	$ 44,400.00	$ 42,516.63
Salesforce.com	Buddy One-time content	204-1447	$ 132,000.00	$ 126,400.81
Salesforce.com	Buddy Quarterly Competitive Intelligence Analysis	204-1448	$ 84,000.00	$ 80,436.88
Salesforce.com	Buddy One-time Competitive Intelligence Analysis	204-1449	$ 24,000.00	$ 22,981.96

Salesforce.com	Buddy Quarterly Facebook Wall or Twitter Optimization Analysis	204-1450	$ 16,800.00	$ 16,087.38
Salesforce.com	Buddy One time Facebook Wall or Twitter Optimization Analysis	204-1451	$ 48,000.00	$ 45,963.93
Salesforce.com	Force.com (1 Enterprise Application) Enterprise Edition	204-1452	$ 300.00	$ 287.15
Salesforce.com	Force.com (1 Enterprise Application) Enterprise Edition Government Cloud	204-1452GC	$ 90.00	$ 86.15
Salesforce.com	Force.com (1 Enterprise Application) Unlimited Edition	204-1453	$ 300.00	$ 287.15
Salesforce.com	Force.com (1 Enterprise Application) Unlimited Edition Government Cloud	204-1453GC	$ 15.00	$ 14.36
Salesforce.com	Force.com (1 Light Application) Enterprise Edition	204-1454	$ 120.00	$ 114.86
Salesforce.com	Force.com (1 Light Application) Enterprise Edition Government Cloud	204-1454GC	$ 36.00	$ 34.46
Salesforce.com	Force.com (1 Light Application) Unlimited Edition	204-1455	$ 120.00	$ 114.86
Salesforce.com	Force.com (1 Light Application) Unlimited Edition Government Cloud	204-1455GC	$ 6.00	$ 5.74
Salesforce.com	Force.com (Administrator) User Subscription Enterprise Edition	204-1456	$ 600.00	$ 574.31
Salesforce.com	Force.com (Administrator) User Subscription Enterprise Edition Government Cloud	204-1456GC	$ 180.00	$ 172.29
Salesforce.com	Force.com (Administrator) User Subscription Unlimited Edition	204-1457	$ 900.00	$ 861.46
Salesforce.com	Force.com (Administrator) User Subscription Unlimited Edition Government Cloud	204-1457GC	$ 45.00	$ 43.07
Salesforce.com	Remedyforce (BMC)	204-1458	$ 948.00	$ 907.41
Salesforce.com	Data Storage (50MB) (price is per org)	204-1459	$ 300.00	$ 287.27
Salesforce.com	Data Storage (500MB) (price is per org)	204-1460	$ 1,500.00	$ 1,436.37
Salesforce.com	Data.com Corporate Clean	204-1461	$ 300.00	$ 287.27
Salesforce.com	Data.com Corporate Prospector	204-1462	$ 1,500.00	$ 1,436.37
Salesforce.com	Data.com Corporate Records Additional (price is each)	204-1463	$ 0.50	$ 0.48
Salesforce.com	Data.com Premium Clean	204-1464	$ 420.00	$ 402.18
Salesforce.com	Data.com Premium Prospector	204-1465	$ 1,980.00	$ 1,896.01
Salesforce.com	Data.com Premium Records Additional (price is each)	204-1466	$ 0.65	$ 0.62
Salesforce.com	Data.com Services - QuickStart	204-1467	$ 5,000.00	$ 4,787.91
Salesforce.com	Partner Community Members (20 Members)	204-1468	$ 8,400.00	$ 8,043.69
Salesforce.com	Partner Community Members (20 Members) Government Cloud	204-1468GC	$ 2,520.00	$ 2,412.09
Salesforce.com	Partner Community Members (100 Members)	204-1469	$ 30,000.00	$ 28,727.46
Salesforce.com	Partner Community Members (100 Members) Government Cloud	204-1469GC	$ 9,000.00	$ 8,614.61
Salesforce.com	Partner Community Members (500 Members)	204-1470	$ 96,000.00	$ 91,927.86
Salesforce.com	Partner Community Members (500 Members) Government Cloud	204-1470GC	$ 28,800.00	$ 27,566.75
Salesforce.com	Customer Community Members (500 Members)	204-1478	$ 12,000.00	$ 11,490.98
Salesforce.com	Customer Community Members (500 Members) Government Cloud	204-1478GC	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Members (250000 Members)	204-1481	$ 600,000.00	$ 574,549.12
Salesforce.com	Customer Community Members (250000 Members) Government Cloud	204-1481GC	$ 180,000.00	$ 172,292.19
Salesforce.com	Customer Community Logins (2000 Logins/Month)	204-1482	$ 12,000.00	$ 11,490.98
Salesforce.com	Customer Community Logins (2000 Logins/Month) Government Cloud	204-1482GC	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Logins (100000 Logins/Month)	204-1484	$ 120,000.00	$ 114,909.82
Salesforce.com	Customer Community Logins (1000000 Logins/Month)	204-1485	$ 600,000.00	$ 574,549.12
Salesforce.com	Customer Community Logins (1000000 Logins/Month) Government Cloud	204-1485GC	$ 180,000.00	$ 172,292.19
Salesforce.com	Sales Cloud Performance Edition	204-1486	$ 3,420.00	$ 3,274.93
Salesforce.com	Service Cloud Performance Edition	204-1487	$ 3,420.00	$ 3,274.93
Salesforce.com	Service Cloud Knowledge Pack Performance Edition	204-1488	$ 3,420.00	$ 3,274.93
Salesforce.com	Company Community Only	204-1489	$ 240.00	$ 229.82
Salesforce.com	Identity Only	204-1490	$ 60.00	$ 57.45
Salesforce.com	Identity Only Government Cloud	204-1490GC	$ 18.00	$ 17.23
Salesforce.com	Work.com Motivate	204-1491	$ 120.00	$ 114.91
Salesforce.com	Work.com Align	204-1492	$ 180.00	$ 172.36
Salesforce.com	Work.com Perform	204-1493	$ 240.00	$ 229.82
Salesforce.com	Force.com Performance	204-1494	$ 1,800.00	$ 1,723.65

Salesforce.com	Force.com Performance (Admin)	204-1495	$ 900.00	$ 861.82
Salesforce.com	Partner Community Members Sandbox (20 Members)	204-1498	$ 2,520.00	$ 2,413.11
Salesforce.com	Partner Community Members Sandbox (100 Members)	204-1499	$ 9,000.00	$ 8,618.24
Salesforce.com	Partner Community Members Sandbox (500 Members)	204-1500	$ 28,800.00	$ 27,578.36
Salesforce.com	Partner Community Members Sandbox (2500 Members)	204-1501	$ 126,000.00	$ 120,655.31
Salesforce.com	Partner Community Members Sandbox (10000 Members)	204-1502	$ 450,000.00	$ 430,911.84
Salesforce.com	Partner Community Logins Sandbox (200 Logins/Month)	204-1503	$ 9,000.00	$ 8,618.24
Salesforce.com	Partner Community Logins Sandbox (1000 Logins/Month)	204-1504	$ 28,800.00	$ 27,578.36
Salesforce.com	Partner Community Logins Sandbox (5000 Logins/Month)	204-1505	$ 126,000.00	$ 120,655.31
Salesforce.com	Partner Community Logins Sandbox (20000 Logins/Month)	204-1506	$ 450,000.00	$ 430,911.84
Salesforce.com	Partner Community Members Premier Support (20 Members)	204-1507	$ 1,260.00	$ 1,206.55
Salesforce.com	Partner Community Members Premier Support (100 Members)	204-1508	$ 4,500.00	$ 4,309.12
Salesforce.com	Partner Community Members Premier Support (500 Members)	204-1509	$ 14,400.00	$ 13,789.18
Salesforce.com	Partner Community Members Premier Support (2500 Members)	204-1510	$ 63,000.00	$ 60,327.66
Salesforce.com	Partner Community Members Premier Support (10000 Members)	204-1511	$ 225,000.00	$ 215,455.92
Salesforce.com	Partner Community Logins Premier Support (200 Logins/Month)	204-1512	$ 4,500.00	$ 4,309.12
Salesforce.com	Partner Community Logins Premier Support (1000 Logins/Month)	204-1513	$ 14,400.00	$ 13,789.18
Salesforce.com	Partner Community Logins Premier Support (5000 Logins/Month)	204-1514	$ 63,000.00	$ 60,327.66
Salesforce.com	Partner Community Logins Premier Support (20000 Logins/Month)	204-1515	$ 225,000.00	$ 215,455.92
Salesforce.com	Partner Community Members Premier Support+ (20 Members)	204-1516	$ 2,100.00	$ 2,010.92
Salesforce.com	Partner Community Members Premier Support+ (100 Members)	204-1517	$ 7,500.00	$ 7,181.86
Salesforce.com	Partner Community Members Premier Support+ (500 Members)	204-1518	$ 24,000.00	$ 22,981.96
Salesforce.com	Partner Community Members Premier Support+ (2500 Members)	204-1519	$ 105,000.00	$ 100,546.10
Salesforce.com	Partner Community Members Premier Support+ (10000 Members)	204-1520	$ 375,000.00	$ 359,093.20
Salesforce.com	Partner Community Logins Premier Support+ (200 Logins/Month)	204-1521	$ 7,500.00	$ 7,181.86
Salesforce.com	Partner Community Logins Premier Support+ (1000 Logins/Month)	204-1522	$ 24,000.00	$ 22,981.96
Salesforce.com	Partner Community Logins Premier Support+ (5000 Logins/Month)	204-1523	$ 105,000.00	$ 100,546.10
Salesforce.com	Partner Community Logins Premier Support+ (20000 Logins/Month)	204-1525	$ 375,000.00	$ 359,093.20
Salesforce.com	Force.com EE	204-1526	$ 960.00	$ 919.28
Salesforce.com	Force.com UE	204-1527	$ 1,800.00	$ 1,723.65
Salesforce.com	Force.com PXE	204-1528	$ 1,800.00	$ 1,723.65
Salesforce.com	Sales Cloud Group Edition Premier + Success Plan	204-1300PPS	$ 75.00	$ 71.82
Salesforce.com	Sales Cloud Group Edition Premier Success Plan	204-1300PS	$ 45.00	$ 43.09
Salesforce.com	Sales Cloud Group Edition Sandbox (Developer Pro)	204-1300SBD	$ 15.00	$ 14.36
Salesforce.com	Sales Cloud Group Edition Sandbox (Full Copy)	204-1300SBF	$ 90.00	$ 86.18
Salesforce.com	Sales Cloud Group Edition Sandbox (Partial Copy)	204-1300SBP	$ 60.00	$ 57.45
Salesforce.com	Sales Cloud Professional Edition Premier + Success	204-1301PPS	$ 195.00	$ 186.73
Salesforce.com	Sales Cloud Professional Edition Premier Success	204-1301PS	$ 117.00	$ 112.04
Salesforce.com	Sales Cloud Professional Edition Sandbox (Developer Pro)	204-1301SBD	$ 39.00	$ 37.35
Salesforce.com	Sales Cloud Professional Edition Sandbox (Full Copy)	204-1301SBF	$ 234.00	$ 224.07
Salesforce.com	Sales Cloud Professional Edition Sandbox (Partial Copy)	204-1301SBP	$ 156.00	$ 149.38
Salesforce.com	Sales Cloud Enterprise Edition Premier + Success	204-1302PPS	$ 375.00	$ 359.09
Salesforce.com	Sales Cloud Enterprise Edition Premier Success	204-1302PS	$ 225.00	$ 215.46
Salesforce.com	Sales Cloud Enterprise Edition Sandbox (Developer Pro)	204-1302SBD	$ 75.00	$ 71.82
Salesforce.com	Sales Cloud Enterprise Edition Sandbox (Full Copy)	204-1302SBF	$ 450.00	$ 430.91
Salesforce.com	Sales Cloud Enterprise Edition Sandbox (Partial Copy)	204-1302SBP	$ 300.00	$ 287.27
Salesforce.com	Sales Cloud Unlimited Edition Sandbox (Developer Pro)	204-1303SBD	$ 150.00	$ 143.64
Salesforce.com	Sales Cloud Unlimited Edition Sandbox (Full Copy)	204-1303SBF	$ 900.00	$ 861.82
Salesforce.com	Sales Cloud Unlimited Edition Sandbox (Partial Copy)	204-1303SBP	$ 600.00	$ 574.55

Salesforce.com	Sales Cloud Contact Manager Edition Government Cloud	204-1304GC	$ 18.00	$ 17.24
Salesforce.com	Sales Cloud Contact Manager Edition Premier + Success	204-1304PPS	$ 15.00	$ 14.36
Salesforce.com	Sales Cloud Contact Manager Edition Premier Success	204-1304PS	$ 9.00	$ 8.62
Salesforce.com	Sales Cloud Contact Manager Edition Sandbox (Developer Pro)	204-1304SBD	$ 3.00	$ 2.87
Salesforce.com	Sales Cloud Contact Manager Edition Sandbox (Full Copy)	204-1304SBF	$ 18.00	$ 17.24
Salesforce.com	Sales Cloud Contact Manager Edition Sandbox (Partial Copy)	204-1304SBP	$ 12.00	$ 11.49
Salesforce.com	Service Cloud Professional Edition Government Cloud	204-1305GC	$ 234.00	$ 224.07
Salesforce.com	Service Cloud Professional Edition Premier + Success	204-1305PPS	$ 195.00	$ 186.73
Salesforce.com	Service Cloud Professional Edition Premier Success	204-1305PS	$ 117.00	$ 112.04
Salesforce.com	Service Cloud Professional Edition Sandbox (Developer Pro)	204-1305SBD	$ 39.00	$ 37.35
Salesforce.com	Service Cloud Professional Edition Sandbox (Full Copy)	204-1305SBF	$ 234.00	$ 224.07
Salesforce.com	Service Cloud Professional Edition Sandbox (Partial Copy)	204-1305SBP	$ 156.00	$ 149.38
Salesforce.com	Service Cloud Enterprise Edition Premier + Success	204-1306PPS	$ 405.00	$ 387.82
Salesforce.com	Service Cloud Enterprise Edition Premier Success	204-1306PS	$ 243.00	$ 232.69
Salesforce.com	Service Cloud Enterprise Edition Sandbox (Developer Pro)	204-1306SBD	$ 81.00	$ 77.56
Salesforce.com	Service Cloud Enterprise Edition Sandbox (Full Copy)	204-1306SBF	$ 486.00	$ 465.38
Salesforce.com	Service Cloud Enterprise Edition Sandbox (Partial Copy)	204-1306SBP	$ 324.00	$ 310.26
Salesforce.com	Service Cloud Unlimted Edition Sandbox (Developer Pro)	204-1307SBD	$ 156.00	$ 149.38
Salesforce.com	Service Cloud Unlimited Edition Sandbox (Full Copy)	204-1307SBF	$ 936.00	$ 896.30
Salesforce.com	Service Cloud Unlimted Edition Sandbox (Partial Copy)	204-1307SBP	$ 624.00	$ 597.53
Salesforce.com	Service Cloud Knowledge Pack Enterprise Edition Sandbox (Developer Pro)	204-1308SBD	$ 111.00	$ 106.29
Salesforce.com	Service Cloud Knowledge Pack Enterprise Edition Sandbox (Full Copy)	204-1308SBF	$ 666.00	$ 637.75
Salesforce.com	Service Cloud Knowledge Pack Enterprise Edition Sandbox (Partial Copy)	204-1308SBP	$ 444.00	$ 425.17
Salesforce.com	Service Cloud Knowledge Pack Unlimited Edition Sandbox (Developer Pro)	204-1309SBD	$ 186.00	$ 178.11
Salesforce.com	Service Cloud Knowledge Pack Unlimited Edition Sandbox (Full Copy)	204-1309SBF	$ 1,116.00	$ 1,068.66
Salesforce.com	Service Cloud Knowledge Pack Unlimited Edition Sandbox (Partial Copy)	204-1309SBP	$ 744.00	$ 712.44
Salesforce.com	Force.com Enterprise Edition Premier + Success	204-1315PPS	$ 930.00	$ 890.55
Salesforce.com	Force.com Enterprise Edition Premier Success	204-1315PS	$ 558.00	$ 534.33
Salesforce.com	Force.com Enterprise Edition Sandbox (Developer Pro)	204-1315SBD	$ 186.00	$ 178.11
Salesforce.com	Force.com Enterprise Edition Sandbox (Full Copy)	204-1315SBF	$ 1,116.00	$ 1,068.66
Salesforce.com	Force.com Enterprise Edition Sandbox (Partial Copy)	204-1315SBP	$ 744.00	$ 712.44
Salesforce.com	Force.com (Admin) Enterprise Edition Government Cloud	204-1319GC	$ 270.00	$ 258.55
Salesforce.com	Force.com (Admin) Enterprise Edition Premier + Success	204-1319PPS	$ 225.00	$ 215.46
Salesforce.com	Force.com (Admin) Enterprise Edition Premier Success	204-1319PS	$ 135.00	$ 129.27
Salesforce.com	Force.com (Admin) Enterprise Edition Sandbox (Developer Pro)	204-1319SBD	$ 45.00	$ 43.09
Salesforce.com	Force.com (Admin) Enterprise Edition Sandbox (Full Copy)	204-1319SBF	$ 270.00	$ 258.55
Salesforce.com	Force.com (Admin) Unlimited Edition Government Cloud	204-1320GC	$ 270.00	$ 258.55
Salesforce.com	Force.com (Admin) Unlimited Edition Sandbox (Developer Pro)	204-1320SBD	$ 45.00	$ 43.09
Salesforce.com	Force.com (Admin) Unlimited Edition Sandbox (Full Copy)	204-1320SBF	$ 270.00	$ 258.55
Salesforce.com	Force.com (Admin) Unlimited Edition Sandbox (Partial Copy)	204-1320SBP	$ 180.00	$ 172.36
Salesforce.com	Sales Cloud Performance Edition Sandbox (Developer Pro)	204-1486SBD	$ 171.00	$ 163.75
Salesforce.com	Sales Cloud Performance Edition Sandbox (Full Copy)	204-1486SBF	$ 1,026.00	$ 982.48
Salesforce.com	Sales Cloud Performance Edition Sandbox (Partial Copy)	204-1486SBP	$ 684.00	$ 654.99
Salesforce.com	Service Cloud Performance Edition Sandbox (Developer Pro)	204-1487SBD	$ 171.00	$ 163.75
Salesforce.com	Service Cloud Performance Edition Sandbox (Full Copy)	204-1487SBF	$ 1,026.00	$ 982.48
Salesforce.com	Service Cloud Performance Edition Sandbox (Partial Copy)	204-1487SBP	$ 684.00	$ 654.99
Salesforce.com	Force.com EE Government Cloud	204-1526GC	$ 288.00	$ 275.78
Salesforce.com	Force.com EE Premier + Success	204-1526PPS	$ 240.00	$ 229.82
Salesforce.com	Force.com EE Premier Success	204-1526PS	$ 144.00	$ 137.89

Salesforce.com	Force.com EE Sandbox (Developer Pro)	204-1526SBD	$ 48.00	$ 45.96
Salesforce.com	Force.com EE Sandbox (Full Copy)	204-1526SBF	$ 288.00	$ 275.78
Salesforce.com	Force.com EE Sandbox (Partial Copy)	204-1526SBP	$ 192.00	$ 183.86
Salesforce.com	Force.com UE Government Cloud	204-1527GC	$ 540.00	$ 517.09
Salesforce.com	Force.com UE Sandbox (Developer Pro)	204-1527SBD	$ 90.00	$ 86.18
Salesforce.com	Force.com UE Sandbox (Full Copy)	204-1527SBF	$ 540.00	$ 517.09
Salesforce.com	Force.com UE Sandbox (Partial Copy)	204-1527SBP	$ 360.00	$ 344.73
Salesforce.com	Force.com PXE Sandbox (Developer Pro)	204-1528SBD	$ 90.00	$ 86.18
Salesforce.com	Force.com PXE Sandbox (Full Copy)	204-1528SBF	$ 540.00	$ 517.09
Salesforce.com	Force.com PXE Sandbox (Partial Copy)	204-1528SBP	$ 360.00	$ 344.73
Salesforce.com	Additional Scheduled Analytics Bundle (price is per org)	204-1582	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 5 Additional Dynamic Dashboards (price is per org)	204-1583	$ 3,000.00	$ 2,872.75
Salesforce.com	Analytics Cloud - Wave Platform	204-1584	$ 480,000.00	$ 459,639.29
Salesforce.com	Analytics Cloud - Builder	204-1585	$ 3,000.00	$ 2,872.75
Salesforce.com	Analytics Cloud - Explorer	204-1586	$ 1,500.00	$ 1,436.37
Salesforce.com	Console for Sales Cloud	204-1587	$ 120.00	$ 114.91
Salesforce.com	Data Storage (10GB) (price is per org)	204-1588	$ 12,000.00	$ 11,490.98
Salesforce.com	File Storage (1TB) (price is per org)	204-1589	$ 3,600.00	$ 3,447.29
Salesforce.com	Customer Community Members (5000 Members)	204-1479	$ 52,800.00	$ 50,539.04
Salesforce.com	Customer Community Members (5000 Members) Government Cloud	204-1479GC	$ 15,840.00	$ 15,161.71
Salesforce.com	Customer Community Members (25000 Members)	204-1480	$ 132,000.00	$ 126,347.61
Salesforce.com	Customer Community Members (25000 Members) Government Cloud	204-1480GC	$ 39,600.00	$ 37,904.28
Salesforce.com	Customer Community Logins (20000 Logins/Month)	204-1483	$ 52,800.00	$ 50,539.04
Salesforce.com	Customer Community Logins (20000 Logins/Month) Government Cloud	204-1483GC	$ 15,840.00	$ 15,161.71
Salesforce.com	Partner Community Members (2500 Members)	204-1471	$ 384,000.00	$ 367,556.68
Salesforce.com	Partner Community Members (2500 Members) Government Cloud	204-1471GC	$ 115,200.00	$ 110,267.00
Salesforce.com	Partner Community Members Premier Support+ (2500 Members)	204-1471PPS	$ 96,000.00	$ 91,889.17
Salesforce.com	Partner Community Members Premier Support (2500 Members)	204-1471PS	$ 57,600.00	$ 55,133.50
Salesforce.com	Partner Community Members Sandbox (2500 Members)	204-1471SB	$ 115,200.00	$ 110,267.00
Salesforce.com	Partner Community Members (10000 Members)	204-1472	$ 810,000.00	$ 775,314.86
Salesforce.com	Partner Community Members (10000 Members) Government Cloud	204-1472GC	$ 243,000.00	$ 232,594.46
Salesforce.com	Partner Community Members Premier Support+ (10000 Members)	204-1472PPS	$ 202,500.00	$ 193,828.72
Salesforce.com	Partner Community Members Premier Support (10000 Members)	204-1472PS	$ 121,500.00	$ 116,297.23
Salesforce.com	Partner Community Logins (200 Logins/Month)	204-1473	$ 24,000.00	$ 22,972.29
Salesforce.com	Partner Community Logins (200 Logins/Month) Government Cloud	204-1473GC	$ 7,200.00	$ 6,891.69
Salesforce.com	Partner Community Logins Premier Support+ (200 Logins/Month)	204-1473PPS	$ 6,000.00	$ 5,743.07
Salesforce.com	Partner Community Logins Premier Support (200 Logins/Month)	204-1473PS	$ 3,600.00	$ 3,445.84
Salesforce.com	Partner Community Logins Sandbox (200 Logins/Month)	204-1473SB	$ 7,200.00	$ 6,891.69
Salesforce.com	Partner Community Logins (1000 Logins/Month)	204-1474	$ 78,000.00	$ 74,659.95
Salesforce.com	Partner Community Logins (1000 Logins/Month) Government Cloud	204-1474GC	$ 23,400.00	$ 22,397.98
Salesforce.com	Partner Community Logins Premier Support+ (1000 Logins/Month)	204-1474PPS	$ 19,500.00	$ 18,664.99
Salesforce.com	Partner Community Logins Premier Support (1000 Logins/Month)	204-1474PS	$ 11,700.00	$ 11,198.99
Salesforce.com	Partner Community Logins Sandbox (1000 Logins/Month)	204-1474SB	$ 23,400.00	$ 22,397.98
Salesforce.com	Partner Community Logins (5000 Logins/Month)	204-1475	$ 240,000.00	$ 229,722.92
Salesforce.com	Partner Community Logins (5000 Logins/Month) Government Cloud	204-1475GC	$ 72,000.00	$ 68,916.88
Salesforce.com	Partner Community Logins Premier Support+ (5000 Logins/Month)	204-1475PPS	$ 60,000.00	$ 57,430.73
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members Sanbox (Developer Pro)	204-1641SBD	$ 8.00	$ 7.73
Salesforce.com	Salesforce Event Monitoring (10% of List Price per $100 of List Licence)	204-EM	$ 10.00	$ 9.65
Salesforce.com	Field Audit Trail (10% of List Price per $100 of List Licence)	204-FAT	$ 10.00	$ 9.65

Salesforce.com	Platform Encryption (20% of List Price per $100 of List Licence)	204-PLT-E	$ 20.00	$ 19.29
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members Premier Success	204-1641PS	$ 24.00	$ 23.15
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members Sanbox (Developer Pro)	204-1647SBD	$ 24.00	$ 23.15
Salesforce.com	Salesforce Shield (30% of List Price per $100 of List Licence)	204-SFS	$ 30.00	$ 28.94
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month Sanbox (Developer Pro)	204-1644SBD	$ 30.00	$ 28.94
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members (Partial Copy)	204-1641SBP	$ 32.00	$ 30.87
Salesforce.com	Customer Community Members- 10 Members Sanbox (Developer Pro)	204-1631SBD	$ 40.00	$ 38.59
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members Premier+ Success	204-1641PPS	$ 40.00	$ 38.59
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members Government Cloud	204-1641GC	$ 48.00	$ 46.30
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members Sandbox (Full Copy)	204-1641SBF	$ 48.00	$ 46.30
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) Sanbox (Developer Pro)	204-1637SBD	$ 60.00	$ 57.88
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members Premier Success	204-1647PS	$ 72.00	$ 69.45
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month Premier Success	204-1644PS	$ 90.00	$ 86.82
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month Sanbox (Developer Pro)	204-1645SBD	$ 96.00	$ 92.60
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members (Partial Copy)	204-1647SBP	$ 96.00	$ 92.60
Salesforce.com	Customer Community Plus- 10 Members Sanbox (Developer Pro)	204-1619SBD	$ 120.00	$ 115.76
Salesforce.com	Customer Community Members- 10 Members Premier Success	204-1631PS	$ 120.00	$ 115.76
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month (Partial Copy)	204-1644SBP	$ 120.00	$ 115.76
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members Premier+ Success	204-1647PPS	$ 120.00	$ 115.76
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members Government Cloud	204-1647GC	$ 144.00	$ 138.91
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members Sandbox (Full Copy)	204-1647SBF	$ 144.00	$ 138.91
Salesforce.com	Customer Community Logins- 200 Logins/Month Sanbox (Developer Pro)	204-1634SBD	$ 150.00	$ 144.70
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month Premier+ Success	204-1644PPS	$ 150.00	$ 144.70
Salesforce.com	Customer Community Members- 10 Members (Partial Copy)	204-1631SBP	$ 160.00	$ 154.34
Salesforce.com	Additional 10 Objects for Customer Community Members- 10 Members	204-1641	$ 160.00	$ 154.34
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) Premier Success	204-1637PS	$ 180.00	$ 173.63
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month Government Cloud	204-1644GC	$ 180.00	$ 173.63
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month Sandbox (Full Copy)	204-1644SBF	$ 180.00	$ 173.63
Salesforce.com	Customer Community Members- 10 Members Premier+ Success	204-1631PPS	$ 200.00	$ 192.93
Salesforce.com	Customer Community Member (100 Members) Sandbox (Developer Pro)	204-1477SBD	$ 210.00	$ 202.57
Salesforce.com	Customer Community Members- 10 Members Government Cloud	204-1631GC	$ 240.00	$ 231.51
Salesforce.com	Customer Community Members- 10 Members Sandbox (Full Copy)	204-1631SBF	$ 240.00	$ 231.51
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) (Partial Copy)	204-1637SBP	$ 240.00	$ 231.51
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month Sanbox (Developer Pro)	204-1653SBD	$ 280.00	$ 270.10
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month Premier Success	204-1645PS	$ 288.00	$ 277.81
Salesforce.com	Partner Community Members - 10 Members Sandbox (Developer Pro)	204-1612SBD	$ 300.00	$ 289.39
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) Premier+ Success	204-1637PPS	$ 300.00	$ 289.39
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month Sanbox (Developer Pro)	204-1646SBD	$ 300.00	$ 289.39
Salesforce.com	Customer Community Plus- 10 Members Premier Success	204-1619PS	$ 360.00	$ 347.27
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) Government Cloud	204-1637GC	$ 360.00	$ 347.27
Salesforce.com	Additional 10 Objects for Partner Community (10 Member) Sandbox (Full Copy)	204-1637SBF	$ 360.00	$ 347.27
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members Sanbox (Developer Pro)	204-1648SBD	$ 360.00	$ 347.27
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month (Partial Copy)	204-1645SBP	$ 384.00	$ 370.42
Salesforce.com	Customer Community Logins- 200 Logins/Month Premier Success	204-1634PS	$ 450.00	$ 434.09
Salesforce.com	Customer Community Logins- 1000 Logins/Month Sanbox (Developer Pro)	204-1635SBD	$ 450.00	$ 434.09
Salesforce.com	Customer Community Plus- 10 Members (Partial Copy)	204-1619SBP	$ 480.00	$ 463.02
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members Sanbox (Developer Pro)	204-1642SBD	$ 480.00	$ 463.02
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month Premier+ Success	204-1645PPS	$ 480.00	$ 463.02
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10 Members	204-1647	$ 480.00	$ 463.02

Salesforce.com	Heroku - 1 Dyno	204-1610	$ 540.00	$ 520.90
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month Government Cloud	204-1645GC	$ 576.00	$ 555.63
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month Sandbox (Full Copy)	204-1645SBF	$ 576.00	$ 555.63
Salesforce.com	Data.com Premium Add on	204-1609	$ 600.00	$ 578.78
Salesforce.com	Customer Community Plus- 10 Members Premier+ Success	204-1619PPS	$ 600.00	$ 578.78
Salesforce.com	Customer Community Logins- 200 Logins/Month (Partial Copy)	204-1634SBP	$ 600.00	$ 578.78
Salesforce.com	Additional 10 Objects for Customer Community Logins- 200 Logins/Month	204-1644	$ 600.00	$ 578.78
Salesforce.com	Salesforce Engage	204-1673	$ 600.00	$ 578.78
Salesforce.com	Customer Community Member (500 Members) Sandbox (Developer Pro)	204-1478SBD	$ 600.00	$ 578.78
Salesforce.com	Customer Community Logins (2000 logins/month) Sandbox (Developer Pro)	204-1482SBD	$ 600.00	$ 578.78
Salesforce.com	Customer Community Member (100 Members) Premier Success	204-1477PS	$ 630.00	$ 607.72
Salesforce.com	Customer Community Plus- 10 Members Government Cloud	204-1619GC	$ 720.00	$ 694.54
Salesforce.com	Customer Community Plus- 10 Members Sandbox (Full Copy)	204-1619SBF	$ 720.00	$ 694.54
Salesforce.com	Customer Community Logins- 200 Logins/Month Premier+ Success	204-1634PPS	$ 750.00	$ 723.48
Salesforce.com	Customer Community Members- 10 Members	204-1631	$ 800.00	$ 771.71
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month Premier Success	204-1653PS	$ 840.00	$ 810.29
Salesforce.com	Customer Community Member (100 Members) Sandbox (Partial Copy)	204-1477SBP	$ 840.00	$ 810.29
Salesforce.com	Partner Community Members - 10 Members Premier Success	204-1612PS	$ 900.00	$ 868.17
Salesforce.com	Customer Community Logins- 200 Logins/Month Government Cloud	204-1634GC	$ 900.00	$ 868.17
Salesforce.com	Customer Community Logins- 200 Logins/Month Sandbox (Full Copy)	204-1634SBF	$ 900.00	$ 868.17
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month Premier Success	204-1646PS	$ 900.00	$ 868.17
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month Sanbox (Developer Pro)	204-1654SBD	$ 900.00	$ 868.17
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Sandbox (Developer Pro)	204-1640SBD	$ 960.00	$ 926.05
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members Sanbox (Developer Pro)	204-1643SBD	$ 1,020.00	$ 983.93
Salesforce.com	Customer Community Member (100 Members) Premier+ Success	204-1477PPS	$ 1,050.00	$ 1,012.87
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members Premier Success	204-1648PS	$ 1,080.00	$ 1,041.81
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month (Partial Copy)	204-1653SBP	$ 1,120.00	$ 1,080.39
Salesforce.com	Partner Community Members - 10 Members Sandbox (Partial Copy)	204-1612SBP	$ 1,200.00	$ 1,157.56
Salesforce.com	Additional 10 Objects for Partner Community Members (10 Members)	204-1637	$ 1,200.00	$ 1,157.56
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month (Partial Copy)	204-1646SBP	$ 1,200.00	$ 1,157.56
Salesforce.com	Pardot- Database - Additional Database Contacts (10000)	204-1657	$ 1,200.00	$ 1,157.56
Salesforce.com	Pardot- Database - File Hosting (500MB)	204-1661	$ 1,200.00	$ 1,157.56
Salesforce.com	Pardot- Database - Inbound Marketing (SEO & Competitor)	204-1664	$ 1,200.00	$ 1,157.56
Salesforce.com	Customer Community Member (100 Members) Sandbox (Full Copy)	204-1477SBF	$ 1,260.00	$ 1,215.44
Salesforce.com	Customer Community Logins- 1000 Logins/Month Premier Success	204-1635PS	$ 1,350.00	$ 1,302.26
Salesforce.com	Customer Community Plus- 1000 Logins/Month Sanbox (Developer Pro)	204-1626SBD	$ 1,400.00	$ 1,350.49
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month Premier+ Success	204-1653PPS	$ 1,400.00	$ 1,350.49
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members Premier Success	204-1642PS	$ 1,440.00	$ 1,389.07
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members (Partial Copy)	204-1648SBP	$ 1,440.00	$ 1,389.07
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members Sanbox (Developer Pro)	204-1649SBD	$ 1,440.00	$ 1,389.07
Salesforce.com	Partner Community Members - 10 Members Premier+ Success	204-1612PPS	$ 1,500.00	$ 1,446.95
Salesforce.com	Customer Community Logins- 5000 Logins/Month Sanbox (Developer Pro)	204-1636SBD	$ 1,500.00	$ 1,446.95
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month Premier+ Success	204-1646PPS	$ 1,500.00	$ 1,446.95
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members Sanbox (Developer Pro)	204-1650SBD	$ 1,620.00	$ 1,562.71
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month Government Cloud	204-1653GC	$ 1,680.00	$ 1,620.59
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month Sandbox (Full Copy)	204-1653SBF	$ 1,680.00	$ 1,620.59
Salesforce.com	Partner Community Members - 10 Members Government Cloud	204-1612GC	$ 1,800.00	$ 1,736.34
Salesforce.com	Partner Community Members - 10 Members Sandbox (Full Copy)	204-1612SBF	$ 1,800.00	$ 1,736.34
Salesforce.com	Customer Community Plus- 500 Members Sanbox (Developer Pro)	204-1620SBD	$ 1,800.00	$ 1,736.34

Salesforce.com	Customer Community Logins- 1000 Logins/Month (Partial Copy)	204-1635SBP	$ 1,800.00	$ 1,736.34
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month Government Cloud	204-1646GC	$ 1,800.00	$ 1,736.34
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month Sandbox (Full Copy)	204-1646SBF	$ 1,800.00	$ 1,736.34
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members Premier+ Success	204-1648PPS	$ 1,800.00	$ 1,736.34
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month Sanbox (Developer Pro)	204-1655SBD	$ 1,800.00	$ 1,736.34
Salesforce.com	Customer Community Member (500 Members) Premier Success	204-1478PS	$ 1,800.00	$ 1,736.34
Salesforce.com	Customer Community Logins (2000 logins/month) Premier Success	204-1482PS	$ 1,800.00	$ 1,736.34
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members (Partial Copy)	204-1642SBP	$ 1,920.00	$ 1,852.10
Salesforce.com	Additional 10 Objects for Customer Community Logins- 1000 Logins/Month	204-1645	$ 1,920.00	$ 1,852.10
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members Government Cloud	204-1648GC	$ 2,160.00	$ 2,083.61
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members Sandbox (Full Copy)	204-1648SBF	$ 2,160.00	$ 2,083.61
Salesforce.com	Customer Community Logins- 1000 Logins/Month Premier+ Success	204-1635PPS	$ 2,250.00	$ 2,170.43
Salesforce.com	Customer Community Plus- 10 Members	204-1619	$ 2,400.00	$ 2,315.12
Salesforce.com	Customer Community Members- 2500 Members Sanbox (Developer Pro)	204-1632SBD	$ 2,400.00	$ 2,315.12
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members Premier+ Success	204-1642PPS	$ 2,400.00	$ 2,315.12
Salesforce.com	Public Communities Page Views (1 million/month) Sanbox (Developer Pro)	204-1656SBD	$ 2,400.00	$ 2,315.12
Salesforce.com	Pardot- Database - Automation Rules (50)	204-1670	$ 2,400.00	$ 2,315.12
Salesforce.com	Customer Community Member (500 Members) Sandbox (Partial Copy)	204-1478SBP	$ 2,400.00	$ 2,315.12
Salesforce.com	Customer Community Logins (2000 logins/month) Sandbox (Partial Copy)	204-1482SBP	$ 2,400.00	$ 2,315.12
Salesforce.com	Customer Community Logins- 1000 Logins/Month Government Cloud	204-1635GC	$ 2,700.00	$ 2,604.51
Salesforce.com	Customer Community Logins- 1000 Logins/Month Sandbox (Full Copy)	204-1635SBF	$ 2,700.00	$ 2,604.51
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month Premier Success	204-1654PS	$ 2,700.00	$ 2,604.51
Salesforce.com	Customer Community Member (5000 Members) Sandbox (Developer Pro)	204-1479SBD	$ 2,700.00	$ 2,604.51
Salesforce.com	Customer Community Member (5000 Members) Sandbox (Partial Copy)	204-1479SBP	$ 2,700.00	$ 2,604.51
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Premier Success	204-1640PS	$ 2,880.00	$ 2,778.15
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members Government Cloud	204-1642GC	$ 2,880.00	$ 2,778.15
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members Sandbox (Full Copy)	204-1642SBF	$ 2,880.00	$ 2,778.15
Salesforce.com	Customer Community Logins- 200 Logins/Month	204-1634	$ 3,000.00	$ 2,893.90
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members Sanbox (Developer Pro)	204-1651SBD	$ 3,000.00	$ 2,893.90
Salesforce.com	Customer Community Member (500 Members) Premier+ Success	204-1478PPS	$ 3,000.00	$ 2,893.90
Salesforce.com	Customer Community Logins (2000 logins/month) Premier+ Success	204-1482PPS	$ 3,000.00	$ 2,893.90
Salesforce.com	Customer Community Logins (20000 logins/month) Sandbox (Developer Pro)	204-1483SBD	$ 3,000.00	$ 2,893.90
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members Premier Success	204-1643PS	$ 3,060.00	$ 2,951.78
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month (Partial Copy)	204-1654SBP	$ 3,600.00	$ 3,472.69
Salesforce.com	Customer Community Member (500 Members) Sandbox (Full Copy)	204-1478SBF	$ 3,600.00	$ 3,472.69
Salesforce.com	Customer Community Logins (2000 logins/month) Sandbox (Full Copy)	204-1482SBF	$ 3,600.00	$ 3,472.69
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Sandbox (Partial Copy)	204-1640SBP	$ 3,840.00	$ 3,704.20
Salesforce.com	Pardot- Database - Quick Start (one time fee)	204-1671	$ 4,000.00	$ 3,858.54
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members (Partial Copy)	204-1643SBP	$ 4,080.00	$ 3,935.71
Salesforce.com	Customer Community Plus- 1000 Logins/Month Premier Success	204-1626PS	$ 4,200.00	$ 4,051.47
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) Sanbox (Developer Pro)	204-1638SBD	$ 4,320.00	$ 4,167.22
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members Premier Success	204-1649PS	$ 4,320.00	$ 4,167.22
Salesforce.com	Customer Community Plus- 5000 Logins/Month Sanbox (Developer Pro)	204-1627SBD	$ 4,500.00	$ 4,340.86
Salesforce.com	Customer Community Logins- 5000 Logins/Month Premier Success	204-1636PS	$ 4,500.00	$ 4,340.86
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members Sanbox (Developer Pro)	204-1652SBD	$ 4,500.00	$ 4,340.86
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month Premier+ Success	204-1654PPS	$ 4,500.00	$ 4,340.86
Salesforce.com	Partner Community Logins- 2000 Logins/Month Sandbox (Developer Pro)	204-1616SBD	$ 4,800.00	$ 4,630.25
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Premier+ Success	204-1640PPS	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Custom Object Intergration (4)	204-1658	$ 4,800.00	$ 4,630.25

Salesforce.com	Pardot- Database - API Access (100000/day)	204-1659	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Advanced Email Analytics	204-1660	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Advanced Dynamic Content	204-1662	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Google Adwords Integration	204-1665	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Social Profiles & Lookups	204-1667	$ 4,800.00	$ 4,630.25
Salesforce.com	Pardot- Database - Expansion Pack	204-1669	$ 4,800.00	$ 4,630.25
Salesforce.com	BCC Email Compliance	204-1672	$ 4,800.00	$ 4,630.25
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members Premier Success	204-1650PS	$ 4,860.00	$ 4,688.12
Salesforce.com	Customer Community Members- 10000 Members Sanbox (Developer Pro)	204-1633SBD	$ 5,100.00	$ 4,919.64
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members Premier+ Success	204-1643PPS	$ 5,100.00	$ 4,919.64
Salesforce.com	Customer Community Plus- 500 Members Premier Success	204-1620PS	$ 5,400.00	$ 5,209.03
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month Government Cloud	204-1654GC	$ 5,400.00	$ 5,209.03
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month Sandbox (Full Copy)	204-1654SBF	$ 5,400.00	$ 5,209.03
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month Premier Success	204-1655PS	$ 5,400.00	$ 5,209.03
Salesforce.com	Customer Community Plus- 1000 Logins/Month (Partial Copy)	204-1626SBP	$ 5,600.00	$ 5,401.95
Salesforce.com	Additional 10 Objects for Customer Community Plus- 1000 Logins/Month	204-1653	$ 5,600.00	$ 5,401.95
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Government Cloud	204-1640GC	$ 5,760.00	$ 5,556.30
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month Sandbox (Full Copy)	204-1640SBF	$ 5,760.00	$ 5,556.30
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members (Partial Copy)	204-1649SBP	$ 5,760.00	$ 5,556.30
Salesforce.com	Partner Community Members - 10 Members	204-1612	$ 6,000.00	$ 5,787.81
Salesforce.com	Customer Community Logins- 5000 Logins/Month (Partial Copy)	204-1636SBP	$ 6,000.00	$ 5,787.81
Salesforce.com	Additional 10 Objects for Customer Community Logins- 5000 Logins/Month	204-1646	$ 6,000.00	$ 5,787.81
Salesforce.com	Pardot- Database - Dedicated IP	204-1663	$ 6,000.00	$ 5,787.81
Salesforce.com	Pardot- Database - Custom User Roles (Unlimited)	204-1666	$ 6,000.00	$ 5,787.81
Salesforce.com	Customer Community Logins (100000 logins/month) Sandbox (Developer Pro)	204-1484SBD	$ 6,000.00	$ 5,787.81
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members Government Cloud	204-1643GC	$ 6,120.00	$ 5,903.56
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members Sandbox (Full Copy)	204-1643SBF	$ 6,120.00	$ 5,903.56
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members (Partial Copy)	204-1650SBP	$ 6,480.00	$ 6,250.83
Salesforce.com	Customer Community Plus- 1000 Logins/Month Premier+ Success	204-1626PPS	$ 7,000.00	$ 6,752.44
Salesforce.com	Customer Community Plus- 500 Members (Partial Copy)	204-1620SBP	$ 7,200.00	$ 6,945.37
Salesforce.com	Customer Community Plus- 2500 Members Sanbox (Developer Pro)	204-1621SBD	$ 7,200.00	$ 6,945.37
Salesforce.com	Customer Community Members- 2500 Members Premier Success	204-1632PS	$ 7,200.00	$ 6,945.37
Salesforce.com	Additional 10 Objects for Customer Community Plus- 500 Members	204-1648	$ 7,200.00	$ 6,945.37
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members Premier+ Success	204-1649PPS	$ 7,200.00	$ 6,945.37
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month (Partial Copy)	204-1655SBP	$ 7,200.00	$ 6,945.37
Salesforce.com	Public Communities Page Views (1 million/month) Premier Success	204-1656PS	$ 7,200.00	$ 6,945.37
Salesforce.com	Customer Community Logins- 5000 Logins/Month Premier+ Success	204-1636PPS	$ 7,500.00	$ 7,234.76
Salesforce.com	Customer Community Member (25000 Members) Sandbox (Developer Pro)	204-1480SBD	$ 7,500.00	$ 7,234.76
Salesforce.com	Customer Community Plus- 5000 Members Sanbox (Developer Pro)	204-1622SBD	$ 8,100.00	$ 7,813.54
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members Premier+ Success	204-1650PPS	$ 8,100.00	$ 7,813.54
Salesforce.com	Customer Community Member (5000 Members) Premier Success	204-1479PS	$ 8,100.00	$ 7,813.54
Salesforce.com	Customer Community Plus- 1000 Logins/Month Government Cloud	204-1626GC	$ 8,400.00	$ 8,102.93
Salesforce.com	Customer Community Plus- 1000 Logins/Month Sandbox (Full Copy)	204-1626SBF	$ 8,400.00	$ 8,102.93
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members Government Cloud	204-1649GC	$ 8,640.00	$ 8,334.44
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members Sandbox (Full Copy)	204-1649SBF	$ 8,640.00	$ 8,334.44
Salesforce.com	Customer Community Plus- 500 Members Premier+ Success	204-1620PPS	$ 9,000.00	$ 8,681.71
Salesforce.com	Customer Community Plus- 20000 Logins/Month Sanbox (Developer Pro)	204-1628SBD	$ 9,000.00	$ 8,681.71
Salesforce.com	Customer Community Logins- 1000 Logins/Month	204-1635	$ 9,000.00	$ 8,681.71
Salesforce.com	Customer Community Logins- 5000 Logins/Month Government Cloud	204-1636GC	$ 9,000.00	$ 8,681.71

Salesforce.com	Customer Community Logins- 5000 Logins/Month Sandbox (Full Copy)	204-1636SBF	$ 9,000.00	$ 8,681.71
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members Premier Success	204-1651PS	$ 9,000.00	$ 8,681.71
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month Premier+ Success	204-1655PPS	$ 9,000.00	$ 8,681.71
Salesforce.com	Customer Community Logins (20000 logins/month) Premier Success	204-1483PS	$ 9,000.00	$ 8,681.71
Salesforce.com	Customer Community Members- 2500 Members (Partial Copy)	204-1632SBP	$ 9,600.00	$ 9,260.49
Salesforce.com	Additional 10 Objects for Customer Community Members- 2500 Members	204-1642	$ 9,600.00	$ 9,260.49
Salesforce.com	Public Communities Page Views (1 million/month) (Partial Copy)	204-1656SBP	$ 9,600.00	$ 9,260.49
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members Government Cloud	204-1650GC	$ 9,720.00	$ 9,376.25
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members Sandbox (Full Copy)	204-1650SBF	$ 9,720.00	$ 9,376.25
Salesforce.com	Customer Community Plus- 500 Members Government Cloud	204-1620GC	$ 10,800.00	$ 10,418.06
Salesforce.com	Customer Community Plus- 500 Members Sandbox (Full Copy)	204-1620SBF	$ 10,800.00	$ 10,418.06
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month Government Cloud	204-1655GC	$ 10,800.00	$ 10,418.06
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month Sandbox (Full Copy)	204-1655SBF	$ 10,800.00	$ 10,418.06
Salesforce.com	Customer Community Members- 2500 Members Premier+ Success	204-1632PPS	$ 12,000.00	$ 11,575.62
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) Sanbox (Developer Pro)	204-1639SBD	$ 12,000.00	$ 11,575.62
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members (Partial Copy)	204-1651SBP	$ 12,000.00	$ 11,575.62
Salesforce.com	Public Communities Page Views (1 million/month) Premier+ Success	204-1656PPS	$ 12,000.00	$ 11,575.62
Salesforce.com	Pardot- Database - Phone Support	204-1668	$ 12,000.00	$ 11,575.62
Salesforce.com	Customer Community Logins (20000 logins/month) Sandbox (Partial Copy)	204-1483SBP	$ 12,000.00	$ 11,575.62
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) Premier Success	204-1638PS	$ 12,960.00	$ 12,501.67
Salesforce.com	Customer Community Plus- 5000 Logins/Month Premier Success	204-1627PS	$ 13,500.00	$ 13,022.57
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members Premier Success	204-1652PS	$ 13,500.00	$ 13,022.57
Salesforce.com	Customer Community Member (5000 Members) Premier+ Success	204-1479PPS	$ 13,500.00	$ 13,022.57
Salesforce.com	Heroku - 1000 Add On Credit	204-1611	$ 14,400.00	$ 13,890.74
Salesforce.com	Partner Community Logins- 2000 Logins/Month Premier Success	204-1616PS	$ 14,400.00	$ 13,890.74
Salesforce.com	Customer Community Members- 2500 Members Government Cloud	204-1632GC	$ 14,400.00	$ 13,890.74
Salesforce.com	Customer Community Members- 2500 Members Sandbox (Full Copy)	204-1632SBF	$ 14,400.00	$ 13,890.74
Salesforce.com	Public Communities Page Views (1 million/month) Government Cloud	204-1656GC	$ 14,400.00	$ 13,890.74
Salesforce.com	Public Communities Page Views (1 million/month) Sandbox (Full Copy)	204-1656SBF	$ 14,400.00	$ 13,890.74
Salesforce.com	Customer Community Plus- 10000 Members Sanbox (Developer Pro)	204-1623SBD	$ 15,000.00	$ 14,469.52
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members Premier+ Success	204-1651PPS	$ 15,000.00	$ 14,469.52
Salesforce.com	Customer Community Logins (20000 logins/month) Premier+ Success	204-1483PPS	$ 15,000.00	$ 14,469.52
Salesforce.com	Customer Community Members- 10000 Members Premier Success	204-1633PS	$ 15,300.00	$ 14,758.91
Salesforce.com	Customer Community Member (5000 Members) Sandbox (Full Copy)	204-1479SBF	$ 16,200.00	$ 15,627.08
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) (Partial Copy)	204-1638SBP	$ 17,280.00	$ 16,668.89
Salesforce.com	Customer Community Plus- 5000 Logins/Month (Partial Copy)	204-1627SBP	$ 18,000.00	$ 17,363.43
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members Government Cloud	204-1651GC	$ 18,000.00	$ 17,363.43
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members Sandbox (Full Copy)	204-1651SBF	$ 18,000.00	$ 17,363.43
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members (Partial Copy)	204-1652SBP	$ 18,000.00	$ 17,363.43
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Logins/Month	204-1654	$ 18,000.00	$ 17,363.43
Salesforce.com	Customer Community Logins (20000 logins/month) Sandbox (Full Copy)	204-1483SBF	$ 18,000.00	$ 17,363.43
Salesforce.com	Customer Community Plus- 5000 Members Premier Success	204-1622PS	$ 24,300.00	$ 23,440.62
Salesforce.com	Customer Community Members- 10000 Members Premier+ Success	204-1633PPS	$ 25,500.00	$ 24,598.19
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) Government Cloud	204-1638GC	$ 25,920.00	$ 25,003.33
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) Sandbox (Full Copy)	204-1638SBF	$ 25,920.00	$ 25,003.33
Salesforce.com	Customer Community Plus- 5000 Logins/Month Government Cloud	204-1627GC	$ 27,000.00	$ 26,045.14
Salesforce.com	Customer Community Plus- 5000 Logins/Month Sandbox (Full Copy)	204-1627SBF	$ 27,000.00	$ 26,045.14
Salesforce.com	Customer Community Plus- 20000 Logins/Month Premier Success	204-1628PS	$ 27,000.00	$ 26,045.14
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members Government Cloud	204-1652GC	$ 27,000.00	$ 26,045.14

Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members Sandbox (Full Copy)	204-1652SBF	$ 27,000.00	$ 26,045.14
Salesforce.com	Customer Community Plus- 1000 Logins/Month	204-1626	$ 28,000.00	$ 27,009.77
Salesforce.com	Partner Community Logins- 2000 Logins/Month Government Cloud	204-1616GC	$ 28,800.00	$ 27,781.48
Salesforce.com	Partner Community Logins- 2000 Logins/Month Sandbox (Full Copy)	204-1616SBF	$ 28,800.00	$ 27,781.48
Salesforce.com	Customer Community Plus- 2500 Members (Partial Copy)	204-1621SBP	$ 28,800.00	$ 27,781.48
Salesforce.com	Additional 10 Objects for Customer Community Plus- 2500 Members	204-1649	$ 28,800.00	$ 27,781.48
Salesforce.com	Customer Community Logins- 5000 Logins/Month	204-1636	$ 30,000.00	$ 28,939.04
Salesforce.com	Customer Community Member (25000 Members) Sandbox (Partial Copy)	204-1480SBP	$ 30,000.00	$ 28,939.04
Salesforce.com	Customer Community Member (250000 Members) Sandbox (Developer Pro)	204-1481SBD	$ 30,000.00	$ 28,939.04
Salesforce.com	Customer Community Logins (100000 logins/month) Premier+ Success	204-1484PPS	$ 30,000.00	$ 28,939.04
Salesforce.com	Customer Community Logins (1000000 logins/month) Sandbox (Developer Pro)	204-1485SBD	$ 30,000.00	$ 28,939.04
Salesforce.com	Customer Community Members- 10000 Members Government Cloud	204-1633GC	$ 30,600.00	$ 29,517.82
Salesforce.com	Customer Community Members- 10000 Members Sandbox (Full Copy)	204-1633SBF	$ 30,600.00	$ 29,517.82
Salesforce.com	Customer Community Plus- 5000 Members (Partial Copy)	204-1622SBP	$ 32,400.00	$ 31,254.17
Salesforce.com	Additional 10 Objects for Customer Community Plus- 5000 Members	204-1650	$ 32,400.00	$ 31,254.17
Salesforce.com	Customer Community Plus- 500 Members	204-1620	$ 36,000.00	$ 34,726.85
Salesforce.com	Customer Community Plus- 2500 Members Premier+ Success	204-1621PPS	$ 36,000.00	$ 34,726.85
Salesforce.com	Customer Community Plus- 20000 Logins/Month (Partial Copy)	204-1628SBP	$ 36,000.00	$ 34,726.85
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) Premier Success	204-1639PS	$ 36,000.00	$ 34,726.85
Salesforce.com	Additional 10 Objects for Customer Community Plus- 20000 Logins/Month	204-1655	$ 36,000.00	$ 34,726.85
Salesforce.com	Customer Community Logins (100000 logins/month) Sandbox (Full Copy)	204-1484SBF	$ 36,000.00	$ 34,726.85
Salesforce.com	Customer Community Member (25000 Members) Premier+ Success	204-1480PPS	$ 37,500.00	$ 36,173.80
Salesforce.com	Customer Community Plus- 5000 Members Premier+ Success	204-1622PPS	$ 40,500.00	$ 39,067.71
Salesforce.com	Customer Community Plus- 2500 Members Government Cloud	204-1621GC	$ 43,200.00	$ 41,672.22
Salesforce.com	Customer Community Plus- 2500 Members Sandbox (Full Copy)	204-1621SBF	$ 43,200.00	$ 41,672.22
Salesforce.com	Customer Community Plus- 10000 Members Premier Success	204-1623PS	$ 45,000.00	$ 43,408.56
Salesforce.com	Customer Community Plus- 20000 Logins/Month Premier+ Success	204-1628PPS	$ 45,000.00	$ 43,408.56
Salesforce.com	Customer Community Member (25000 Members) Sandbox (Full Copy)	204-1480SBF	$ 45,000.00	$ 43,408.56
Salesforce.com	Customer Community Members- 2500 Members	204-1632	$ 48,000.00	$ 46,302.47
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) (Partial Copy)	204-1639SBP	$ 48,000.00	$ 46,302.47
Salesforce.com	Public Communities Page Views (1 million/month)	204-1656	$ 48,000.00	$ 46,302.47
Salesforce.com	Customer Community Plus- 5000 Members Government Cloud	204-1622GC	$ 48,600.00	$ 46,881.25
Salesforce.com	Customer Community Plus- 5000 Members Sandbox (Full Copy)	204-1622SBF	$ 48,600.00	$ 46,881.25
Salesforce.com	Customer Community Plus- 20000 Logins/Month Government Cloud	204-1628GC	$ 54,000.00	$ 52,090.28
Salesforce.com	Customer Community Plus- 20000 Logins/Month Sandbox (Full Copy)	204-1628SBF	$ 54,000.00	$ 52,090.28
Salesforce.com	Partner Community Members- 25000 Members Sandbox (Developer Pro)	204-1614SBD	$ 60,000.00	$ 57,878.09
Salesforce.com	Customer Community Plus- 10000 Members (Partial Copy)	204-1623SBP	$ 60,000.00	$ 57,878.09
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) Premier+ Success	204-1639PPS	$ 60,000.00	$ 57,878.09
Salesforce.com	Additional 10 Objects for Customer Community Plus- 10000 Members	204-1651	$ 60,000.00	$ 57,878.09
Salesforce.com	Partner Community Members- 5000 Members Premier Success	204-1613PS	$ 64,800.00	$ 62,508.33
Salesforce.com	Customer Community Plus- 25000 Members Premier Success	204-1624PS	$ 67,500.00	$ 65,112.85
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) Government Cloud	204-1639GC	$ 72,000.00	$ 69,453.70
Salesforce.com	Additional 10 Objects for Partner Community (25000 Member) Sandbox (Full Copy)	204-1639SBF	$ 72,000.00	$ 69,453.70
Salesforce.com	Customer Community Plus- 10000 Members Premier+ Success	204-1623PPS	$ 75,000.00	$ 72,347.61
Salesforce.com	Partner Community Members- 5000 Members Sandbox (Partial Copy)	204-1613SBP	$ 86,400.00	$ 83,344.44
Salesforce.com	Additional 10 Objects for Partner Community Members (5000 Members)	204-1638	$ 86,400.00	$ 83,344.44
Salesforce.com	Customer Community Plus- 10000 Members Government Cloud	204-1623GC	$ 90,000.00	$ 86,817.13
Salesforce.com	Customer Community Plus- 10000 Members Sandbox (Full Copy)	204-1623SBF	$ 90,000.00	$ 86,817.13
Salesforce.com	Customer Community Plus- 25000 Members (Partial Copy)	204-1624SBP	$ 90,000.00	$ 86,817.13

Salesforce.com	Customer Community Plus- 5000 Logins/Month	204-1627	$ 90,000.00	$ 86,817.13
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members	204-1652	$ 90,000.00	$ 86,817.13
Salesforce.com	Customer Community Member (250000 Members) Premier Success	204-1481PS	$ 90,000.00	$ 86,817.13
Salesforce.com	Customer Community Logins (1000000 logins/month) Premier Success	204-1485PS	$ 90,000.00	$ 86,817.13
Salesforce.com	Partner Community Logins- 2000 Logins/Month	204-1616	$ 96,000.00	$ 92,604.94
Salesforce.com	Customer Community Members- 10000 Members	204-1633	$ 102,000.00	$ 98,392.75
Salesforce.com	Partner Community Members- 5000 Members Premier+ Success	204-1613PPS	$ 108,000.00	$ 104,180.55
Salesforce.com	Customer Community Plus- 25000 Members Premier+ Success	204-1624PPS	$ 112,500.00	$ 108,521.41
Salesforce.com	Customer Community Member (250000 Members) Sandbox (Partial Copy)	204-1481SBP	$ 120,000.00	$ 115,756.17
Salesforce.com	Customer Community Logins (1000000 logins/month) Sandbox (Partial Copy)	204-1485SBP	$ 120,000.00	$ 115,756.17
Salesforce.com	Partner Community Members- 5000 Members Government Cloud	204-1613GC	$ 129,600.00	$ 125,016.66
Salesforce.com	Partner Community Members- 5000 Members Sandbox (Full Copy)	204-1613SBF	$ 129,600.00	$ 125,016.66
Salesforce.com	Customer Community Plus- 25000 Members Government Cloud	204-1624GC	$ 135,000.00	$ 130,225.69
Salesforce.com	Customer Community Plus- 25000 Members Sandbox (Full Copy)	204-1624SBF	$ 135,000.00	$ 130,225.69
Salesforce.com	Customer Community Plus- 2500 Members	204-1621	$ 144,000.00	$ 138,907.41
Salesforce.com	Customer Community Member (250000 Members) Premier+ Success	204-1481PPS	$ 150,000.00	$ 144,695.21
Salesforce.com	Customer Community Logins (1000000 logins/month) Premier+ Success	204-1485PPS	$ 150,000.00	$ 144,695.21
Salesforce.com	Customer Community Plus- 5000 Members	204-1622	$ 162,000.00	$ 156,270.83
Salesforce.com	Partner Community Members- 25000 Members Premier Success	204-1614PS	$ 180,000.00	$ 173,634.26
Salesforce.com	Customer Community Plus- 20000 Logins/Month	204-1628	$ 180,000.00	$ 173,634.26
Salesforce.com	Customer Community Member (250000 Members) Sandbox (Full Copy)	204-1481SBF	$ 180,000.00	$ 173,634.26
Salesforce.com	Customer Community Logins (1000000 logins/month) Sandbox (Full Copy)	204-1485SBF	$ 180,000.00	$ 173,634.26
Salesforce.com	Partner Community Members- 25000 Members Sandbox (Partial Copy)	204-1614SBP	$ 240,000.00	$ 231,512.34
Salesforce.com	Additional 10 Objects for Partner Community Members (25000 Members)	204-1639	$ 240,000.00	$ 231,512.34
Salesforce.com	Partner Community Members- 25000 Members Premier+ Success	204-1614PPS	$ 300,000.00	$ 289,390.43
Salesforce.com	Partner Community Members Sandbox (20 Members)	204-1468SB	$ 2,520.00	$ 2,413.11
Salesforce.com	Partner Community Members Sandbox (100 Members)	204-1469SB	$ 9,000.00	$ 8,618.24
Salesforce.com	Partner Community Members Sandbox (500 Members)	204-1470SB	$ 28,800.00	$ 27,578.36
Salesforce.com	Partner Community Members Sandbox (10000 Members)	204-1472SB	$ 450,000.00	$ 430,911.84
Salesforce.com	Partner Community Members Premier Support (20 Members)	204-1468PS	$ 1,260.00	$ 1,206.55
Salesforce.com	Partner Community Members Premier Support (100 Members)	204-1469PS	$ 4,500.00	$ 4,309.12
Salesforce.com	Partner Community Members Premier Support (500 Members)	204-1470PS	$ 14,400.00	$ 13,789.18
Salesforce.com	Partner Community Members Premier Support+ (20 Members)	204-1468PPS	$ 2,100.00	$ 2,010.92
Salesforce.com	Partner Community Members Premier Support+ (100 Members)	204-1469PPS	$ 7,500.00	$ 7,181.86
Salesforce.com	Partner Community Members Premier Support+ (500 Members)	204-1470PPS	$ 24,000.00	$ 22,981.96
Salesforce.com	Customer Community Members Sandbox (500 Members)	204-1478SB	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Members Sandbox (5000 Members)	204-1479SB	$ 14,400.00	$ 13,783.38
Salesforce.com	Customer Community Plus (20 Members) Premier Support	204-1563PS	$ 540.00	$ 516.88
Salesforce.com	Customer Community Plus (100 Members) Premier Support	204-1564PS	$ 1,800.00	$ 1,722.92
Salesforce.com	Customer Community Plus (200 Logins/Month) Premier Support	204-1565PS	$ 1,260.00	$ 1,206.05
Salesforce.com	Customer Community Plus (2000 Logins/Month) Premier Support	204-1566PS	$ 7,200.00	$ 6,891.69
Salesforce.com	Customer Community Plus (20 Members) Premier+ Support	204-1563PPS	$ 900.00	$ 861.46
Salesforce.com	Customer Community Plus (100 Members) Premier+ Support	204-1564PPS	$ 3,000.00	$ 2,871.54
Salesforce.com	Customer Community Plus (200 Logins/Month) Premier+ Support	204-1565PPS	$ 2,100.00	$ 2,010.08
Salesforce.com	Customer Community Plus (2000 Logins/Month) Premier+ Support	204-1566PPS	$ 12,000.00	$ 11,486.15
Salesforce.com	Customer Community Plus (20 Members) Sandbox	204-1563SB	$ 1,080.00	$ 1,033.75
Salesforce.com	Customer Community Plus (100 Members) Sandbox	204-1564SB	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Plus (200 Logins/Month) Sandbox	204-1565SB	$ 2,520.00	$ 2,412.09
Salesforce.com	Customer Community Plus (2000 Logins/Month) Sandbox	204-1566SB	$ 14,400.00	$ 13,783.38

Salesforce.com	Lightning Connect (Price is per connection)	204-1674	$ 48,000.00	$ 46,302.47
Salesforce.com	Analytics Cloud - Additional Data Rows (100 Million)	204-1675	$ 48,000.00	$ 46,302.47
Salesforce.com	Analytics Cloud - Additional Data Rows (100 Million) Government Cloud	204-1675GC	$ 14,400.00	$ 13,890.74
Salesforce.com	Analytics Cloud - Sales Wave Analytics App	204-1676	$ 900.00	$ 868.17
Salesforce.com	Customer Community Plus- 10000 Members	204-1623	$ 300,000.00	$ 289,390.43
Salesforce.com	Partner Community Members- 25000 Members Government Cloud	204-1614GC	$ 360,000.00	$ 347,268.51
Salesforce.com	Partner Community Members- 25000 Members Sandbox (Full Copy)	204-1614SBF	$ 360,000.00	$ 347,268.51
Salesforce.com	Partner Community Members- 5000 Members	204-1613	$ 432,000.00	$ 416,722.22
Salesforce.com	Customer Community Plus- 25000 Members	204-1624	$ 450,000.00	$ 434,085.64
Salesforce.com	Partner Community Members- 25000 Members	204-1614	$ 1,200,000.00	$ 1,157,561.71
Salesforce.com	Customer Community Logins (100000 logins/month) Premier Success	204-1484PS	$ 18,000.00	$ 17,363.43
Salesforce.com	Partner Community Logins- 2000 Logins/Month Sandbox (Partial Copy)	204-1616SBP	$ 19,200.00	$ 18,520.99
Salesforce.com	Additional 10 Objects for Partner Community Logins- 2000 Logins/Month	204-1640	$ 19,200.00	$ 18,520.99
Salesforce.com	Customer Community Members- 10000 Members (Partial Copy)	204-1633SBP	$ 20,400.00	$ 19,678.55
Salesforce.com	Additional 10 Objects for Customer Community Members- 10000 Members	204-1643	$ 20,400.00	$ 19,678.55
Salesforce.com	Partner Community Members- 5000 Members Sandbox (Developer Pro)	204-1613SBD	$ 21,600.00	$ 20,836.11
Salesforce.com	Customer Community Plus- 2500 Members Premier Success	204-1621PS	$ 21,600.00	$ 20,836.11
Salesforce.com	Additional 10 Objects for Partner Community (5000 Member) Premier+ Success	204-1638PPS	$ 21,600.00	$ 20,836.11
Salesforce.com	Customer Community Plus- 25000 Members Sanbox (Developer Pro)	204-1624SBD	$ 22,500.00	$ 21,704.28
Salesforce.com	Customer Community Plus- 5000 Logins/Month Premier+ Success	204-1627PPS	$ 22,500.00	$ 21,704.28
Salesforce.com	Additional 10 Objects for Customer Community Plus- 25000 Members Premier+ Success	204-1652PPS	$ 22,500.00	$ 21,704.28
Salesforce.com	Customer Community Member (25000 Members) Premier Success	204-1480PS	$ 22,500.00	$ 21,704.28
Salesforce.com	Partner Community Logins- 2000 Logins/Month Premier+ Success	204-1616PPS	$ 24,000.00	$ 23,151.23
Salesforce.com	Customer Community Logins (100000 logins/month) Sandbox (Partial Copy)	204-1484SBP	$ 24,000.00	$ 23,151.23
Salesforce.com	Partner Community Logins Premier Support (5000 Logins/Month)	204-1475PS	$ 36,000.00	$ 34,458.44
Salesforce.com	Partner Community Logins Sandbox (5000 Logins/Month)	204-1475SB	$ 72,000.00	$ 68,916.88
Salesforce.com	Partner Community Logins (20000 Logins/Month)	204-1476	$ 480,000.00	$ 459,445.84
Salesforce.com	Partner Community Logins (20000 Logins/Month) Government Cloud	204-1476GC	$ 144,000.00	$ 137,833.75
Salesforce.com	Partner Community Logins Premier Support (20000 Logins/Month)	204-1476PS	$ 72,000.00	$ 68,916.88
Salesforce.com	Partner Community Logins Sandbox (20000 Logins/Month)	204-1476SB	$ 144,000.00	$ 137,833.75
Salesforce.com	Customer Community Members (100 Members)	204-1477	$ 4,200.00	$ 4,020.15
Salesforce.com	Customer Community Members (100 Members) Government Cloud	204-1477GC	$ 1,260.00	$ 1,206.05
Salesforce.com	Customer Community Members Sandbox (100 Members)	204-1477SB	$ 1,260.00	$ 1,206.05
Salesforce.com	Customer Community Logins (100000 Logins/Month) Government Cloud	204-1484GC	$ 36,000.00	$ 34,458.44
Salesforce.com	Analytics Cloud - Sales Wave Analytics App Government Cloud	204-1676GC	$ 270.00	$ 260.45
Salesforce.com	Apex Debugger	204-1677	$ 18,000.00	$ 17,363.43
Salesforce.com	Apex Debugger	204-1677GC	$ 5,400.00	$ 5,209.03
Salesforce.com	Platform Cache	204-1678	$ 3,600.00	$ 3,472.69
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition	204-1679	$ 3,600.00	$ 3,472.69
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition Government Cloud	204-1679GC	$ 1,080.00	$ 1,041.81
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition Premier Success	204-1679PS	$ 540.00	$ 520.90
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition Premier + Success	204-1679PPS	$ 900.00	$ 868.17
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition Sandbox (Developer Pro)	204-1679SBD	$ 180.00	$ 173.63
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition (Sandbox Full Copy)	204-1679SBF	$ 1,080.00	$ 1,041.81
Salesforce.com	Service Cloud Government Connect (Vlocity) Enterprise Edition (Sandbox Partial Copy)	204-1679SBP	$ 720.00	$ 694.54
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition	204-1680	$ 5,400.00	$ 5,209.03
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition Government Cloud	204-1680GC	$ 270.00	$ 260.45
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition Premier Success	204-1680PS	$ 810.00	$ 781.35
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition Premier + Success	204-1680PPS	$ 1,350.00	$ 1,302.26

Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition Sandbox (Developer Pro)	204-1680SBD	$ 270.00	$ 260.45
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition (Sandbox Full Copy)	204-1680SBF	$ 1,620.00	$ 1,562.71
Salesforce.com	Service Cloud Government Connect (Vlocity) Unlimited Edition (Sandbox Partial Copy)	204-1680SBP	$ 270.00	$ 260.45
Salesforce.com	SOS	204-1681	$ 1,800.00	$ 1,736.34
Salesforce.com	Force.com App Bundle PXE	204-1529	$ 960.00	$ 919.28
Salesforce.com	Force.com App Bundle UE	204-1530	$ 960.00	$ 919.28
Salesforce.com	Force.com App Bundle UE Government Cloud	204-1530GC	$ 48.00	$ 45.94
Salesforce.com	Force.com Admin PXE	204-1531	$ 900.00	$ 861.82
Salesforce.com	Additional Scheduled Analytics Bundle (price is per org)	204-1532	$ 6,000.00	$ 5,745.49
Salesforce.com	Analytics - 5 Additional Dynamic Dashboards (price is per org)	204-1533	$ 3,000.00	$ 2,872.75
Salesforce.com	Company Community (add on for Force.com)	204-1534	$ 240.00	$ 229.82
Salesforce.com	Customer Community Plus (200 Logins/Month) Government Cloud	204-1565GC	$ 2,520.00	$ 2,412.09
Salesforce.com	Customer Community Plus (2000 Logins/Month)	204-1566	$ 48,000.00	$ 45,944.58
Salesforce.com	Customer Community Plus (2000 Logins/Month) Government Cloud	204-1566GC	$ 14,400.00	$ 13,783.38
Salesforce.com	Customer Community Plus (20 Members) Premier Support	204-1567	$ 540.00	$ 516.88
Salesforce.com	Customer Community Plus (100 Members) Premier Support	204-1568	$ 1,800.00	$ 1,722.92
Salesforce.com	Customer Community Plus (200 Logins/Month) Premier Support	204-1569	$ 1,260.00	$ 1,206.05
Salesforce.com	Customer Community Plus (2000 Logins/Month) Premier Support	204-1570	$ 7,200.00	$ 6,891.69
Salesforce.com	Customer Community Plus (20 Members) Premier+ Support	204-1571	$ 900.00	$ 861.46
Salesforce.com	Customer Community Plus (100 Members) Premier+ Support	204-1572	$ 3,000.00	$ 2,871.54
Salesforce.com	Customer Community Plus (200 Logins/Month) Premier+ Support	204-1573	$ 2,100.00	$ 2,010.08
Salesforce.com	Customer Community Plus (2000 Logins/Month) Premier+ Support	204-1574	$ 12,000.00	$ 11,486.15
Salesforce.com	Customer Community Plus (20 Members) Sandbox	204-1575	$ 1,080.00	$ 1,033.75
Salesforce.com	Customer Community Plus (100 Members) Sandbox	204-1576	$ 3,600.00	$ 3,445.84
Salesforce.com	Customer Community Plus (200 Logins/Month) Sandbox	204-1577	$ 2,520.00	$ 2,412.09
Salesforce.com	Customer Community Plus (2000 Logins/Month) Sandbox	204-1578	$ 14,400.00	$ 13,783.38
Salesforce.com	Employee Community only	204-1579	$ 240.00	$ 229.72
Salesforce.com	Employee Community only Government Cloud	204-1579GC	$ 72.00	$ 68.92
Salesforce.com	Employee Help Desk only	204-1580	$ 60.00	$ 57.43
Salesforce.com	Employee Help Desk only Government Cloud	204-1580GC	$ 18.00	$ 17.23
Salesforce.com	Files Connect	204-1590	$ 84.00	$ 80.44
Salesforce.com	Sites Pageviews (1 Million/month) - (price is per org)	204-1591	$ 24,000.00	$ 22,981.96
Salesforce.com	Unlimited Apps Pack	204-1592	$ 900.00	$ 861.82
Salesforce.com	Desk.com - Standard	204-1593	$ 420.00	$ 402.18
Salesforce.com	Desk.com - Pro	204-1594	$ 840.00	$ 804.37
Salesforce.com	Desk.com - Business	204-1595	$ 1,320.00	$ 1,264.01
Salesforce.com	Desk.com - Flex Bundle 1 (20 hours)	204-1596	$ 360.00	$ 344.73
Salesforce.com	Desk.com - Flex Bundle 2 (50 hours)	204-1597	$ 780.00	$ 746.91
Salesforce.com	Desk.com - Flex Bundle 3 (100 hours)	204-1598	$ 1,380.00	$ 1,321.46
Salesforce.com	Desk.com - Flex Bundle 4 (250 hours)	204-1599	$ 3,000.00	$ 2,872.75
Salesforce.com	Desk.com - Flex Bundle 5 (500 hours)	204-1600	$ 5,100.00	$ 4,883.67
Salesforce.com	Desk.com - Portal SSL	204-1601	$ 348.00	$ 333.24
Salesforce.com	Desk - Configuration +	204-1602	$ 3,000.00	$ 2,872.75
Salesforce.com	Desk - Advanced	204-1603	$ 3,500.00	$ 3,351.54
Salesforce.com	Desk - Data Import	204-1604	$ 1,500.00	$ 1,436.37
Salesforce.com	External Identity (25000 Unique Users/month) 5	204-1605	$ 24,000.00	$ 22,981.96
Salesforce.com	External Identity (250000 Unique Users/month) 5	204-1606	$ 120,000.00	$ 114,909.82
Salesforce.com	External Identity (1000000 Unique Users/month) 5	204-1607	$ 200,000.00	$ 191,516.37
Salesforce.com	External Identity (5000000 Unique Users/month) 5	204-1608	$ 500,000.00	$ 478,790.93

SAP	SAP ByDesign Base Fee	8000340	$ 1,650.00	$ 1,468.50
SAP	SAP ByDesign Enterprise Private Edition	8000274	$ 16,500.00	$ 14,685.00
SAP	SAP ByDesign CRM Sales Team User	8000046	$ 87.00	$ 77.43
SAP	SAP ByDesign Project Management Team User	8002711	$ 87.00	$ 77.43
SAP	SAP By Design Standard Enterprise User	8000045	$ 146.00	$ 129.94
SAP	SAP ByDesign SCM Enterprise User	8000044	$ 197.00	$ 175.33
SAP	SAP ByDesign Standard Self-Service User	8000049	$ 17.00	$ 15.13
SAP	SAP ByDesign SCM Self-Service User	8000048	$ 24.00	$ 21.36
SAP	SAP ByDesign Project Mgt Self Service User	8000047	$ 24.00	$ 21.36
SAP	SAP ByDesign Localization Fee	8002712	$ 880.00	$ 783.20
SAP	SAP ByDesign Test Tenant	8002713	$ 1,155.00	$ 1,027.95
SAP	SAP ByDesign Additional Productive Tenant	8000275	$ 1,155.00	$ 1,027.95
SAP	SAP Cloud Applications Studio	8000570	$ 184.00	$ 163.76
SAP	SAP Communication Center by ANCILE, base	8002954	$ 18,370.00	$ 16,349.30
SAP	SAP Communication Center by ANCILE, user	8002955	$ 26.00	$ 23.14
SAP	SAP Assessment Mgmt by Questionmark	8002535-1	$ 2.67	$ 2.38
SAP	SAP Assessment Mgmt by Questionmark	8002535-2	$ 2.58	$ 2.30
SAP	SAP Assessment Mgmt by Questionmark	8002535-3	$ 2.48	$ 2.21
SAP	SAP Assessment Mgmt by Questionmark	8002535-4	$ 2.39	$ 2.13
SAP	SAP Assessment Mgmt by Questionmark	8002535-5	$ 2.29	$ 2.04
SAP	SAP Assessment Mgmt by Questionmark	8002535-6	$ 2.20	$ 1.96
SAP	SAP Assessment Mgmt by Questionmark	8002535-7	$ 2.10	$ 1.87
SAP	SAP Assessment Mgmt by Questionmark	8002535-8	$ 2.01	$ 1.79
SAP	SAP Assessment Mgmt by Questionmark	8002535-9	$ 1.91	$ 1.70
SAP	SAP Assessment Mgmt by Questionmark	8002535-10	$ 1.52	$ 1.35
SAP	SAP Assessment Mgmt by Questionmark	8002535-11	$ 1.44	$ 1.28
SAP	SAP SuccessFactors Perform & Reward Package	8003753-1	$ 107.00	$ 95.23
SAP	SAP SuccessFactors Perform & Reward Package	8003753-2	$ 96.00	$ 85.44
SAP	SAP SuccessFactors Perform & Reward Package	8003753-3	$ 79.00	$ 70.31
SAP	SAP SuccessFactors Perform & Reward Package	8003753-4	$ 67.00	$ 59.63
SAP	SAP SuccessFactors Perform & Reward Package	8003753-5	$ 58.00	$ 51.62
SAP	SAP SuccessFactors Perform & Reward Package	8003753-6	$ 52.00	$ 46.28
SAP	SAP SuccessFactors Perform & Reward Package	8003753-7	$ 49.00	$ 43.61
SAP	SAP SuccessFactors Perform & Reward Package	8003753-8	$ 47.00	$ 41.83
SAP	SAP SuccessFactors Perform & Reward Package	8003753-9	$ 45.00	$ 40.05
SAP	SAP SuccessFactors Perform & Reward Package	8003753-10	$ 43.00	$ 38.27
SAP	SAP SuccessFactors Talent Management Package	8003754-1	$ 239.00	$ 212.71
SAP	SAP SuccessFactors Talent Management Package	8003754-2	$ 219.00	$ 194.91
SAP	SAP SuccessFactors Talent Management Package	8003754-3	$ 191.00	$ 169.99
SAP	SAP SuccessFactors Talent Management Package	8003754-4	$ 190.00	$ 169.10
SAP	SAP SuccessFactors Talent Management Package	8003754-5	$ 169.00	$ 150.41
SAP	SAP SuccessFactors Talent Management Package	8003754-6	$ 148.00	$ 131.72
SAP	SAP SuccessFactors Talent Management Package	8003754-7	$ 135.00	$ 120.15
SAP	SAP SuccessFactors Talent Management Package	8003754-8	$ 123.00	$ 109.47
SAP	SAP SuccessFactors Talent Management Package	8003754-9	$ 113.00	$ 100.57
SAP	SAP SuccessFactors Talent Management Package	8003754-10	$ 103.00	$ 91.67
SAP	SAP SuccessFactors Talent Management Package	8003754-11	$ 95.00	$ 84.55
SAP	SAP SuccessFactors Advanced Learning Package	8003754-12	$ 95.00	$ 84.55
SAP	SAP SuccessFactors Advanced Learning Package	8003754-13	$ 86.00	$ 76.54

SAP	SAP SuccessFactors Advanced Learning Package	8003754-14	$ 77.00	$ 68.53
SAP	SAP SuccessFactors Advanced Learning Package	8003754-15	$ 69.00	$ 61.41
SAP	SAP SuccessFactors Advanced Learning Package	8003754-16	$ 60.00	$ 53.40
SAP	SAP SuccessFactors Advanced Learning Package	8003754-17	$ 53.00	$ 47.17
SAP	SAP SuccessFactors Advanced Learning Package	8003754-18	$ 48.00	$ 42.72
SAP	SAP SuccessFactors Advanced Learning Package	8003754-19	$ 44.00	$ 39.16
SAP	SAP SuccessFactors Advanced Learning Package	8003754-20	$ 40.00	$ 35.60
SAP	SAP SuccessFactors Advanced Learning Package	8003754-21	$ 38.00	$ 33.82
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-1	$ 527.00	$ 469.03
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-2	$ 497.00	$ 442.33
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-3	$ 433.00	$ 385.37
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-4	$ 415.00	$ 369.35
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-5	$ 367.00	$ 326.63
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-6	$ 323.00	$ 287.47
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-7	$ 292.00	$ 259.88
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-8	$ 263.00	$ 234.07
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-9	$ 245.00	$ 218.05
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-10	$ 226.00	$ 201.14
SAP	SAP SuccessFactors Enterprise basic Package, BOOMI	8003942-11	$ 211.00	$ 187.79
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-1	$ 543.00	$ 483.27
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-2	$ 511.00	$ 454.79
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-3	$ 445.00	$ 396.05
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-4	$ 427.00	$ 380.03
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-5	$ 377.00	$ 335.53
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-6	$ 333.00	$ 296.37
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-7	$ 300.00	$ 267.00
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-8	$ 270.00	$ 240.30
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-9	$ 252.00	$ 224.28
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-10	$ 232.00	$ 206.48
SAP	SAP SuccessFactors Enterprise Package, BOOMI	8003757-11	$ 217.00	$ 193.13
SAP	SF-Perform & Reward Bundle for Small Business	8000720-1	$ 85.00	$ 75.65
SAP	SF-Perform & Reward Bundle for Small Business	8000720-2	$ 66.00	$ 58.74
SAP	SF-Perform & Reward Bundle for Small Business	8000720-3	$ 56.00	$ 49.84
SAP	SF-Perform & Reward Bundle for Small Business	8000720-4	$ 47.00	$ 41.83
SAP	SF-Perform & Reward Bundle for Small Business	8000720-5	$ 33.00	$ 29.37
SAP	SF-Perform & Reward Bundle for Small Business	8000720-6	$ 33.00	$ 29.37
SAP	SAP SuccessFactors Performance & Goals	8003776-1	$ 68.00	$ 60.52
SAP	SAP SuccessFactors Performance & Goals	8003776-2	$ 61.00	$ 54.29
SAP	SAP SuccessFactors Performance & Goals	8003776-3	$ 50.00	$ 44.50
SAP	SAP SuccessFactors Performance & Goals	8003776-4	$ 43.00	$ 38.27
SAP	SAP SuccessFactors Performance & Goals	8003776-5	$ 37.00	$ 32.93
SAP	SAP SuccessFactors Performance & Goals	8003776-6	$ 33.00	$ 29.37
SAP	SAP SuccessFactors Performance & Goals	8003776-7	$ 31.00	$ 27.59
SAP	SAP SuccessFactors Performance & Goals	8003776-8	$ 30.00	$ 26.70
SAP	SAP SuccessFactors Performance & Goals	8003776-9	$ 29.00	$ 25.81
SAP	SAP SuccessFactors Performance & Goals	8003776-10	$ 27.00	$ 24.03
SAP	SAP SuccessFactors Compensation	8003773-1	$ 38.00	$ 33.82
SAP	SAP SuccessFactors Compensation	8003773-2	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Compensation	8003773-3	$ 28.00	$ 24.92

SAP	SAP SuccessFactors Compensation	8003773-4	$ 24.00	$ 21.36
SAP	SAP SuccessFactors Compensation	8003773-5	$ 21.00	$ 18.69
SAP	SAP SuccessFactors Compensation	8003773-6	$ 19.00	$ 16.91
SAP	SAP SuccessFactors Compensation	8003773-7	$ 18.00	$ 16.02
SAP	SAP SuccessFactors Compensation	8003773-8	$ 17.00	$ 15.13
SAP	SAP SuccessFactors Compensation	8003773-9	$ 16.00	$ 14.24
SAP	SAP SuccessFactors Compensation	8003773-10	$ 15.00	$ 13.35
SAP	SAP SuccessFactors Succession & Development	8003774-1	$ 38.00	$ 33.82
SAP	SAP SuccessFactors Succession & Development	8003774-2	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Succession & Development	8003774-3	$ 28.00	$ 24.92
SAP	SAP SuccessFactors Succession & Development	8003774-4	$ 24.00	$ 21.36
SAP	SAP SuccessFactors Succession & Development	8003774-5	$ 21.00	$ 18.69
SAP	SAP SuccessFactors Succession & Development	8003774-6	$ 19.00	$ 16.91
SAP	SAP SuccessFactors Succession & Development	8003774-7	$ 18.00	$ 16.02
SAP	SAP SuccessFactors Succession & Development	8003774-8	$ 17.00	$ 15.13
SAP	SAP SuccessFactors Succession & Development	8003774-9	$ 16.00	$ 14.24
SAP	SAP SuccessFactors Succession & Development	8003774-10	$ 15.00	$ 13.35
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-1	$ 112.00	$ 99.68
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-2	$ 101.00	$ 89.89
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-3	$ 83.00	$ 73.87
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-4	$ 71.00	$ 63.19
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-5	$ 61.00	$ 54.29
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-6	$ 55.00	$ 48.95
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-7	$ 52.00	$ 46.28
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-8	$ 49.00	$ 43.61
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-9	$ 47.00	$ 41.83
SAP	SAP SuccessFactors Employee Central, BOOMI	8003769-10	$ 45.00	$ 40.05
SAP	SAP SuccessFactors Workforce Analytics	8003771-1	$ 118.00	$ 105.02
SAP	SAP SuccessFactors Workforce Analytics	8003771-2	$ 106.00	$ 94.34
SAP	SAP SuccessFactors Workforce Analytics	8003771-3	$ 94.00	$ 83.66
SAP	SAP SuccessFactors Workforce Analytics	8003771-4	$ 85.00	$ 75.65
SAP	SAP SuccessFactors Workforce Analytics	8003771-5	$ 77.00	$ 68.53
SAP	SAP SuccessFactors Workforce Analytics	8003771-6	$ 68.00	$ 60.52
SAP	SAP SuccessFactors Workforce Analytics	8003771-7	$ 59.00	$ 52.51
SAP	SAP SuccessFactors Workforce Analytics	8003771-8	$ 55.00	$ 48.95
SAP	SAP SuccessFactors Workforce Analytics	8003771-9	$ 51.00	$ 45.39
SAP	SAP SuccessFactors Workforce Analytics	8003771-10	$ 47.00	$ 41.83
SAP	SAP SuccessFactors Workforce Planning	8003772-1	$ 59.00	$ 52.51
SAP	SAP SuccessFactors Workforce Planning	8003772-2	$ 53.00	$ 47.17
SAP	SAP SuccessFactors Workforce Planning	8003772-3	$ 47.00	$ 41.83
SAP	SAP SuccessFactors Workforce Planning	8003772-4	$ 42.00	$ 37.38
SAP	SAP SuccessFactors Workforce Planning	8003772-5	$ 38.00	$ 33.82
SAP	SAP SuccessFactors Workforce Planning	8003772-6	$ 34.00	$ 30.26
SAP	SAP SuccessFactors Workforce Planning	8003772-7	$ 29.00	$ 25.81
SAP	SAP SuccessFactors Workforce Planning	8003772-8	$ 28.00	$ 24.92
SAP	SAP SuccessFactors Workforce Planning	8003772-9	$ 25.00	$ 22.25
SAP	SAP SuccessFactors Workforce Planning	8003772-10	$ 24.00	$ 21.36
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-1	$ 177.00	$ 157.53
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-2	$ 159.00	$ 141.51

SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-3	$ 141.00	$ 125.49
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-4	$ 127.00	$ 113.03
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-5	$ 115.00	$ 102.35
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-6	$ 102.00	$ 90.78
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-7	$ 88.00	$ 78.32
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-8	$ 83.00	$ 73.87
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-9	$ 76.00	$ 67.64
SAP	SAP SuccessFactors WorkforceAnalytics & Planning	8003770-10	$ 71.00	$ 63.19
SAP	SF-Limited Active Users - Learning	8000603-1	$ 19.00	$ 16.91
SAP	SF-Limited Active Users - Learning	8000603-2	$ 18.00	$ 16.02
SAP	SF-Limited Active Users - Learning	8000603-3	$ 17.00	$ 15.13
SAP	SF-Limited Active Users - Learning	8000603-4	$ 16.00	$ 14.24
SAP	SF-Limited Active Users - Learning	8000603-5	$ 14.00	$ 12.46
SAP	SF-Limited Active Users - Learning	8000603-6	$ 13.00	$ 11.57
SAP	SF-Limited Active Users - Learning	8000603-7	$ 11.00	$ 9.79
SAP	SF-Limited Active Users - Learning	8000603-8	$ 9.30	$ 8.28
SAP	SF-Limited Active Users - Learning	8000603-9	$ 7.99	$ 7.11
SAP	SF-Limited Active Users - Learning	8000603-10	$ 7.43	$ 6.61
SAP	SAP SuccessFactors Learning	8003763-1	$ 28.00	$ 24.92
SAP	SAP SuccessFactors Learning	8003763-2	$ 26.00	$ 23.14
SAP	SAP SuccessFactors Learning	8003763-3	$ 26.00	$ 23.14
SAP	SAP SuccessFactors Learning	8003763-4	$ 25.00	$ 22.25
SAP	SAP SuccessFactors Learning	8003763-5	$ 22.00	$ 19.58
SAP	SAP SuccessFactors Learning	8003763-6	$ 20.00	$ 17.80
SAP	SAP SuccessFactors Learning	8003763-7	$ 17.00	$ 15.13
SAP	SAP SuccessFactors Learning	8003763-8	$ 14.00	$ 12.46
SAP	SAP SuccessFactors Learning	8003763-9	$ 12.00	$ 10.68
SAP	SAP SuccessFactors Learning	8003763-10	$ 11.00	$ 9.79
SAP	SF-Transactional Active Users - Learning	8000730-1	$ 9.40	$ 8.37
SAP	SF-Transactional Active Users - Learning	8000730-2	$ 5.41	$ 4.81
SAP	SF-Transactional Active Users - Learning	8000730-3	$ 5.13	$ 4.57
SAP	SF-Transactional Active Users - Learning	8000730-4	$ 4.62	$ 4.11
SAP	SF-Transactional Active Users - Learning	8000730-5	$ 4.15	$ 3.69
SAP	SF-Transactional Active Users - Learning	8000730-6	$ 3.75	$ 3.34
SAP	SF-Transactional Active Users - Learning	8000730-7	$ 3.37	$ 3.00
SAP	SF-Transactional Active Users - Learning	8000730-8	$ 3.04	$ 2.71
SAP	SF-Transactional Active Users - Learning	8000730-9	$ 2.73	$ 2.43
SAP	SF-Transactional Active Users - Learning	8000730-10	$ 2.45	$ 2.18
SAP	SF-External Active Users - Learning	8000665-1	$ 19.00	$ 16.91
SAP	SF-External Active Users - Learning	8000665-2	$ 18.00	$ 16.02
SAP	SF-External Active Users - Learning	8000665-3	$ 17.00	$ 15.13
SAP	SF-External Active Users - Learning	8000665-4	$ 16.00	$ 14.24
SAP	SF-External Active Users - Learning	8000665-5	$ 14.00	$ 12.46
SAP	SF-External Active Users - Learning	8000665-6	$ 13.00	$ 11.57
SAP	SF-External Active Users - Learning	8000665-7	$ 11.00	$ 9.79
SAP	SF-External Active Users - Learning	8000665-8	$ 9.30	$ 8.28
SAP	SF-External Active Users - Learning	8000665-9	$ 7.99	$ 7.11
SAP	SF-External Active Users - Learning	8000665-10	$ 7.43	$ 6.61
SAP	SAP SuccessFactors Employee Central Payroll	8000773-1	$ 113.00	$ 100.57

SAP	SAP SuccessFactors Employee Central Payroll	8000773-2	$ 86.00	$ 76.54
SAP	SAP SuccessFactors Employee Central Payroll	8000773-3	$ 63.00	$ 56.07
SAP	SAP SuccessFactors Employee Central Payroll	8000773-4	$ 52.00	$ 46.28
SAP	SAP SuccessFactors Employee Central Payroll	8000773-5	$ 44.00	$ 39.16
SAP	SAP SuccessFactors Employee Central Payroll	8000773-6	$ 37.00	$ 32.93
SAP	SAP SuccessFactors Employee Central Payroll	8000773-7	$ 32.00	$ 28.48
SAP	SAP SuccessFactors Employee Central Payroll	8000773-8	$ 28.00	$ 24.92
SAP	SAP SuccessFactors Employee Central Payroll	8000773-9	$ 23.00	$ 20.47
SAP	SAP SuccessFactors Onboarding	8003775-1	$ 15.00	$ 13.35
SAP	SAP SuccessFactors Onboarding	8003775-2	$ 14.00	$ 12.46
SAP	SAP SuccessFactors Onboarding	8003775-3	$ 12.00	$ 10.68
SAP	SAP SuccessFactors Onboarding	8003775-4	$ 11.00	$ 9.79
SAP	SAP SuccessFactors Onboarding	8003775-5	$ 9.02	$ 8.03
SAP	SAP SuccessFactors Onboarding	8003775-6	$ 7.98	$ 7.10
SAP	SAP SuccessFactors Onboarding	8003775-7	$ 7.52	$ 6.69
SAP	SAP SuccessFactors Onboarding	8003775-8	$ 7.06	$ 6.28
SAP	SAP SuccessFactors Onboarding	8003775-9	$ 6.45	$ 5.74
SAP	SAP SuccessFactors Onboarding	8003775-10	$ 6.02	$ 5.36
SAP	SAP SuccessFactors Recruiting	8003765-1	$ 36.00	$ 32.04
SAP	SAP SuccessFactors Recruiting	8003765-2	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Recruiting	8003765-3	$ 33.00	$ 29.37
SAP	SAP SuccessFactors Recruiting	8003765-4	$ 31.00	$ 27.59
SAP	SAP SuccessFactors Recruiting	8003765-5	$ 29.00	$ 25.81
SAP	SAP SuccessFactors Recruiting	8003765-6	$ 25.00	$ 22.25
SAP	SAP SuccessFactors Recruiting	8003765-7	$ 22.00	$ 19.58
SAP	SAP SuccessFactors Recruiting	8003765-8	$ 18.00	$ 16.02
SAP	SAP SuccessFactors Recruiting	8003765-9	$ 15.00	$ 13.35
SAP	SAP Success Factors Recruiting Marketing	8003766-1	$ 26.00	$ 23.14
SAP	SAP Success Factors Recruiting Marketing	8003766-2	$ 25.00	$ 22.25
SAP	SAP Success Factors Recruiting Marketing	8003766-3	$ 25.00	$ 22.25
SAP	SAP Success Factors Recruiting Marketing	8003766-4	$ 24.00	$ 21.36
SAP	SAP Success Factors Recruiting Marketing	8003766-5	$ 24.00	$ 21.36
SAP	SAP Success Factors Recruiting Marketing	8003766-6	$ 23.00	$ 20.47
SAP	SAP Success Factors Recruiting Marketing	8003766-7	$ 22.00	$ 19.58
SAP	SAP Success Factors Recruiting Marketing	8003766-8	$ 21.00	$ 18.69
SAP	SAP Success Factors Recruiting Marketing	8003766-9	$ 19.00	$ 16.91
SAP	SAP Success Factors Recruiting Marketing	8003766-10	$ 16.00	$ 14.24
SAP	SAP Success Factors Recruiting Marketing	8003766-11	$ 13.00	$ 11.57
SAP	SAP Success Factors Recruiting Marketing	8003766-12	$ 10.00	$ 8.90
SAP	SAP SuccessFactors Learning Analytics	8000986-1	$ 7.43	$ 6.61
SAP	SAP SuccessFactors Learning Analytics	8000986-2	$ 7.06	$ 6.28
SAP	SAP SuccessFactors Learning Analytics	8000986-3	$ 6.85	$ 6.10
SAP	SAP SuccessFactors Learning Analytics	8000986-4	$ 6.54	$ 5.82
SAP	SAP SuccessFactors Learning Analytics	8000986-5	$ 5.80	$ 5.16
SAP	SAP SuccessFactors Learning Analytics	8000986-6	$ 5.21	$ 4.64
SAP	SAP SuccessFactors Learning Analytics	8000986-7	$ 4.47	$ 3.98
SAP	SAP SuccessFactors Learning Analytics	8000986-8	$ 3.71	$ 3.30
SAP	SAP SuccessFactors Learning Analytics	8000986-9	$ 3.20	$ 2.85
SAP	SAP SuccessFactors Learning Analytics	8000986-10	$ 2.97	$ 2.64

SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-1	$ 56.00	$ 49.84
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-2	$ 51.00	$ 45.39
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-3	$ 42.00	$ 37.38
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-4	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-5	$ 30.00	$ 26.70
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-6	$ 28.00	$ 24.92
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-7	$ 26.00	$ 23.14
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-8	$ 25.00	$ 22.25
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-9	$ 24.00	$ 21.36
SAP	SAP SuccessFactors Employee Central Non-Employee User, Boomi	8000987-10	$ 22.00	$ 19.58
SAP	SF - Activity Based Users - Learning	8000361-1	$ 117.00	$ 104.13
SAP	SF - Activity Based Users - Learning	8000361-2	$ 59.00	$ 52.51
SAP	SF - Activity Based Users - Learning	8000361-3	$ 58.00	$ 51.62
SAP	SF - Activity Based Users - Learning	8000361-4	$ 58.00	$ 51.62
SAP	SF - Activity Based Users - Learning	8000361-5	$ 56.00	$ 49.84
SAP	SF - Activity Based Users - Learning	8000361-6	$ 53.00	$ 47.17
SAP	SF - Activity Based Users - Learning	8000361-7	$ 50.00	$ 44.50
SAP	SF - Activity Based Users - Learning	8000361-8	$ 46.00	$ 40.94
SAP	SF - Activity Based Users - Learning	8000361-9	$ 39.00	$ 34.71
SAP	SF - Activity Based Users - Learning	8000361-10	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Validated Learning	8003764-1	$ 35.00	$ 31.15
SAP	SAP SuccessFactors Validated Learning	8003764-2	$ 33.00	$ 29.37
SAP	SAP SuccessFactors Validated Learning	8003764-3	$ 32.00	$ 28.48
SAP	SAP SuccessFactors Validated Learning	8003764-4	$ 31.00	$ 27.59
SAP	SAP SuccessFactors Validated Learning	8003764-5	$ 27.00	$ 24.03
SAP	SAP SuccessFactors Validated Learning	8003764-6	$ 24.00	$ 21.36
SAP	SAP SuccessFactors Validated Learning	8003764-7	$ 21.00	$ 18.69
SAP	SAP SuccessFactors Validated Learning	8003764-8	$ 17.00	$ 15.13
SAP	SAP SuccessFactors Validated Learning	8003764-9	$ 15.00	$ 13.35
SAP	SAP SuccessFactors Validated Learning	8003764-10	$ 14.00	$ 12.46
SAP	SAP Success Factors Recruiting Management	8003767-1	$ 24.00	$ 21.36
SAP	SAP Success Factors Recruiting Management	8003767-2	$ 23.00	$ 20.47
SAP	SAP Success Factors Recruiting Management	8003767-3	$ 22.00	$ 19.58
SAP	SAP Success Factors Recruiting Management	8003767-4	$ 21.00	$ 18.69
SAP	SAP Success Factors Recruiting Management	8003767-5	$ 20.00	$ 17.80
SAP	SAP Success Factors Recruiting Management	8003767-6	$ 19.00	$ 16.91
SAP	SAP Success Factors Recruiting Management	8003767-7	$ 18.00	$ 16.02
SAP	SAP Success Factors Recruiting Management	8003767-8	$ 17.00	$ 15.13
SAP	SAP Success Factors Recruiting Management	8003767-9	$ 15.00	$ 13.35
SAP	SAP Success Factors Recruiting Management	8003767-10	$ 13.00	$ 11.57
SAP	SAP Success Factors Recruiting Management	8003767-11	$ 11.00	$ 9.79
SAP	SAP Success Factors Recruiting Management	8003767-12	$ 9.40	$ 8.37
SAP	SF-Foundation Product	8000368-1	$ 18.00	$ 16.02
SAP	SF-Foundation Product	8000368-2	$ 16.00	$ 14.24
SAP	SF-Foundation Product	8000368-3	$ 13.00	$ 11.57
SAP	SF-Foundation Product	8000368-4	$ 11.00	$ 9.79
SAP	SF-Foundation Product	8000368-5	$ 9.49	$ 8.45
SAP	SF-Foundation Product	8000368-6	$ 8.61	$ 7.66
SAP	SF-Foundation Product	8000368-7	$ 8.08	$ 7.19

SAP	SF-Foundation Product	8000368-8	$ 7.73	$ 6.88
SAP	SF-Foundation Product	8000368-9	$ 7.38	$ 6.57
SAP	SF-Foundation Product	8000368-10	$ 7.02	$ 6.25
SAP	SF-Skills Content Library	8000728-1	$ 19.00	$ 16.91
SAP	SF-Skills Content Library	8000728-2	$ 19.00	$ 16.91
SAP	SF-Skills Content Library	8000728-3	$ 19.00	$ 16.91
SAP	SF-Skills Content Library	8000728-4	$ 13.00	$ 11.57
SAP	SF-Skills Content Library	8000728-5	$ 12.00	$ 10.68
SAP	SF-Skills Content Library	8000728-6	$ 12.00	$ 10.68
SAP	SF-Skills Content Library	8000728-7	$ 8.81	$ 7.84
SAP	SF-Skills Content Library	8000728-8	$ 7.05	$ 6.27
SAP	SF-Skills Content Library	8000728-9	$ 6.26	$ 5.57
SAP	SF-Skills Content Library	8000728-10	$ 3.76	$ 3.35
SAP	SF-Skills Content Library	8000728-11	$ 2.35	$ 2.09
SAP	SF-Skills Content Library	8000728-12	$ 2.12	$ 1.89
SAP	SF-Additional Instances-Test	8003622	$ 9,398.00	$ 8,364.22
SAP	SF-Additional Instances-Production	8003623	$ 9,398.00	$ 8,364.22
SAP	BOOMI - Integration for Recruiting	8000943	$ 7,049.00	$ 6,273.61
SAP	Data Center Migration	8000988	$ 9,398.00	$ 8,364.22
SAP	SF-Attachment Storage Fee	8000374	$ 1.88	$ 1.67
SAP	SF-Visual Publisher	8000725	$ 14,097.00	$ 12,546.33
SAP	SF-BOOMI : Professional Edition Package	8000513	$ 12,405.00	$ 11,040.45
SAP	SAP HANA Cloud Platform, extension package for SAP SuccessFactors, base edition	8003951	$ 1.10	$ 0.98
SAP	SAP HANA Cloud Platform, extension package for SAP SuccessFactors, standard edition	8003952	$ 3.30	$ 2.94
SAP	SAP HANA Cloud Platform, extension package for SAP SuccessFactors, enterprise edition	8003953	$ 11.00	$ 9.79
SAP	SAP SuccessFactors Disaster Recovery, enhanced option	8003778	$ 0.24	$ 0.24
SAP	SAP Jam Collaboration, advanced edition	8004154-1	$ 2.35	$ 2.09
SAP	SAP Jam Collaboration, advanced edition	8004154-2	$ 2.11	$ 1.88
SAP	SAP Jam Collaboration, advanced edition	8004154-3	$ 1.88	$ 1.67
SAP	SAP Jam Collaboration, advanced edition	8004154-4	$ 1.66	$ 1.48
SAP	SAP Jam Collaboration, advanced edition	8004154-5	$ 1.42	$ 1.26
SAP	SAP Jam Collaboration, advanced edition	8004154-6	$ 1.24	$ 1.10
SAP	SAP Jam Collaboration, advanced edition	8004154-7	$ 1.17	$ 1.04
SAP	SAP Jam Collaboration, advanced edition	8004154-8	$ 1.10	$ 0.98
SAP	SAP Jam Collaboration, advanced edition	8004154-9	$ 1.00	$ 0.89
SAP	SAP Jam Collaboration, advanced edition	8004154-10	$ 0.94	$ 0.84
SAP	SAP Jam Collaboration, advanced plus edition	8004155-1	$ 5.64	$ 5.02
SAP	SAP Jam Collaboration, advanced plus edition	8004155-2	$ 4.51	$ 4.01
SAP	SAP Jam Collaboration, advanced plus edition	8004155-3	$ 3.95	$ 3.52
SAP	SAP Jam Collaboration, advanced plus edition	8004155-4	$ 3.38	$ 3.01
SAP	SAP Jam Collaboration, advanced plus edition	8004155-5	$ 2.82	$ 2.51
SAP	SAP Jam Collaboration, advanced plus edition	8004155-6	$ 2.26	$ 2.01
SAP	SAP Jam Collaboration, advanced plus edition	8004155-7	$ 1.69	$ 1.50
SAP	SAP Jam Collaboration, advanced plus edition	8004155-8	$ 1.41	$ 1.25
SAP	SAP Jam Collaboration, enterprise edition	8004156-1	$ 14.00	$ 12.46
SAP	SAP Jam Collaboration, enterprise edition	8004156-2	$ 11.00	$ 9.79
SAP	SAP Jam Collaboration, enterprise edition	8004156-3	$ 9.87	$ 8.78
SAP	SAP Jam Collaboration, enterprise edition	8004156-4	$ 8.46	$ 7.53
SAP	SAP Jam Collaboration, enterprise edition	8004156-5	$ 7.05	$ 6.27

SAP	SAP Jam Collaboration, enterprise edition	8004156-6	$ 5.64	$ 5.02
SAP	SAP Jam Collaboration, enterprise edition	8004156-7	$ 4.23	$ 3.76
SAP	SAP Jam Collaboration, enterprise edition	8004156-8	$ 3.53	$ 3.14
SAP	SAP Jam Collaboration, external user	8000653-1	$ 3.76	$ 3.35
SAP	SAP Jam Collaboration, external user	8000653-2	$ 3.01	$ 2.68
SAP	SAP Jam Collaboration, external user	8000653-3	$ 2.63	$ 2.34
SAP	SAP Jam Collaboration, external user	8000653-4	$ 2.26	$ 2.01
SAP	SAP Jam Collaboration, external user	8000653-5	$ 1.88	$ 1.67
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-1	$ 4.45	$ 3.96
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-2	$ 3.56	$ 3.17
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-3	$ 3.11	$ 2.77
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-4	$ 2.67	$ 2.38
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-5	$ 2.22	$ 1.98
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-6	$ 1.78	$ 1.58
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-7	$ 1.33	$ 1.18
SAP	SAP Jam Collaboration, work pattern builder add-on	8003088-8	$ 1.12	$ 1.00
SAP	SAP Jam Collaboration, data storage add-on	8000654	$ 235.00	$ 209.15
SAP	SAP SuccessFactors Learning, content storage add-on	8003445	$ 1,400.00	$ 1,246.00
SAP	SAP SuccessFactors Learning, content bandwidth add-on	8003446	$ 570.00	$ 507.30
SAP	SF-Addit'l ATS To Extract For Analytics	8000381	$ 6,000.00	$ 5,340.00
SAP	SF-Site Scrape for Addit'l ATS Instances	8000382	$ 6,000.00	$ 5,340.00
SAP	SF-BOOMI: Add On Prod Use Connection	8000768	$ 3,000.00	$ 2,670.00
SAP	SF-BOOMI: Add On Test Use Connection	8000769	$ 1,500.00	$ 1,335.00
SAP	SAP US Benefits Eligible User	8003532-1	$ 152.00	$ 135.28
SAP	SAP US Benefits Eligible User	8003532-2	$ 138.00	$ 122.82
SAP	SAP US Benefits Eligible User	8003532-3	$ 132.00	$ 117.48
SAP	SAP US Benefits Eligible User	8003532-4	$ 126.00	$ 112.14
SAP	SAP US Benefits Eligible User	8003532-5	$ 113.00	$ 100.57
SAP	SAP US Benefits Eligible User	8003532-6	$ 99.00	$ 88.11
SAP	SAP US Benefits Non-Eligible User	8003533	$ 41.00	$ 36.49
SAP	SAP US Benefits Non-Std Interface User	8003534	$ 27.00	$ 24.03
SAP	SAP Time & Attendance Management by WFS	8003956-1	$ 115.50	$ 102.80
SAP	SAP Time & Attendance Management by WFS	8003956-2	$ 99.00	$ 88.11
SAP	SAP Time & Attendance Management by WFS	8003956-3	$ 88.00	$ 78.32
SAP	SAP Time & Attendance Management by WFS	8003956-4	$ 82.50	$ 73.43
SAP	SAP Time & Attendance Management by WFS	8003956-5	$ 77.00	$ 68.53
SAP	SAP Time & Attendance Management by WFS	8003956-6	$ 55.00	$ 48.95
SAP	SAP Time & Attendance Mgmt. for SME by WFS	8003956-7	$ 121,000.00	$ 107,690.00
SAP	SAP Time & Attendance by WFS Adnl Instance	8003958	$ 22.00	$ 19.58
SAP	SAP Product Stewardship Network - product compliance	8003360-1	$ 2,750.00	$ 2,447.50
SAP	SAP Product Stewardship Network - product compliance	8003360-2	$ 2,200.00	$ 1,958.00
SAP	SAP Product Stewardship Network - product compliance	8003360-3	$ 1,760.00	$ 1,566.40
SAP	SAP Product Stewardship Network - product compliance	8003360-4	$ 1,375.00	$ 1,223.75
SAP	SAP Product Stewardship Network - sustainability assessment	8003362-1	$ 2,750.00	$ 2,447.50
SAP	SAP Product Stewardship Network - sustainability assessment	8003362-2	$ 2,200.00	$ 1,958.00
SAP	SAP Product Stewardship Network - sustainability assessment	8003362-3	$ 1,760.00	$ 1,566.40
SAP	SAP Product Stewardship Network - sustainability assessment	8003362-4	$ 1,375.00	$ 1,223.75
SAP	SAP Product Stewardship Network - conflict minerals	8003361-1	$ 2,750.00	$ 2,447.50
SAP	SAP Product Stewardship Network - conflict minerals	8003361-2	$ 2,200.00	$ 1,958.00

SAP	SAP Product Stewardship Network - conflict minerals	8003361-3	$ 1,760.00	$ 1,566.40
SAP	SAP Product Stewardship Network - conflict minerals	8003361-4	$ 1,375.00	$ 1,223.75
SAP	Ariba Sourcing Professional	8000641-1	$ 630.00	$ 560.70
SAP	Ariba Sourcing Professional	8000641-2	$ 430.00	$ 382.70
SAP	Ariba Sourcing Professional	8000641-3	$ 270.00	$ 240.30
SAP	Ariba Sourcing Professional	8000641-4	$ 250.00	$ 222.50
SAP	Ariba Sourcing Professional	8000641-5	$ 230.00	$ 204.70
SAP	Ariba Contract Management Professional	8000625-1	$ 520.00	$ 462.80
SAP	Ariba Contract Management Professional	8000625-2	$ 400.00	$ 356.00
SAP	Ariba Contract Management Professional	8000625-3	$ 270.00	$ 240.30
SAP	Ariba Contract Management Professional	8000625-4	$ 200.00	$ 178.00
SAP	Ariba Contract Management Professional	8000625-5	$ 170.00	$ 151.30
SAP	Ariba Open Invoice Conversion Services	8002538	$ 0.30	$ 0.27
SAP	Ariba Additional Storage	8003324	$ 100.00	$ 89.00
SAP	SAP Predictive Maintenance and Service, measurements	8003165-1	$ 275.00	$ 244.75
SAP	SAP Predictive Maintenance and Service, measurements	8003165-2	$ 165.00	$ 146.85
SAP	SAP Predictive Maintenance and Service, measurements	8003165-3	$ 132.00	$ 117.48
SAP	SAP Predictive Maintenance and Service, measurements	8003165-4	$ 99.00	$ 88.11
SAP	SAP Predictive Maintenance and Service, measurements	8003165-5	$ 77.00	$ 68.53
SAP	SAP Predictive Maintenance and Service, devices	8003166	$ 33.00	$ 29.37
SAP	SAP Predictive Maintenance and Service, historic storage provisioning	8003167	$ 6,160.00	$ 5,482.40
SAP	SAP Predictive Maintenance and Service, additional historic measurements	8003168	$ 5.50	$ 4.90
SAP	SAP Predictive Maintenance and Service, Vibration Analysis add-on	8004025	$ 1.65	$ 1.47
SAP	SAP Innovation Management, cloud edition - Base Package	8003962	$ 55,000.00	$ 48,950.00
SAP	SAP Innovation Management, cloud edition	8003960-1	$ 39.00	$ 34.71
SAP	SAP Innovation Management, cloud edition	8003960-2	$ 28.00	$ 24.92
SAP	SAP Innovation Management, cloud edition	8003960-3	$ 11.00	$ 9.79
SAP	SAP Innovation Management, cloud edition - Additional Storage	8003963	$ 11.00	$ 9.79
SAP	Cloud for Product Stewardship: Basic Layer	8003959-1	$ 9,900.00	$ 8,811.00
SAP	Cloud for Product Stewardship: Basic Layer	8003959-2	$ 44,000.00	$ 39,160.00
SAP	Cloud for Product Stewardship: Basic Layer	8003959-3	$ 82,500.00	$ 73,425.00
SAP	Cloud for Product Stewardship: Basic Layer	8003959-4	$ 132,000.00	$ 117,480.00
SAP	Cloud for Product Stewardship: Basic Layer	8003959-5	$ 275,000.00	$ 244,750.00
SAP	SAP Cloud for Sales, User	8001003	$ 105.00	$ 93.45
SAP	SAP Cloud for Sales, service option	8003187	$ 55.00	$ 48.95
SAP	SAP Cloud for Service, User	8001004	$ 105.00	$ 93.45
SAP	SAP Cloud for Service, sales option	8003188	$ 55.00	$ 48.95
SAP	SAP Cloud for Social Engagement, User	8001005	$ 165.00	$ 146.85
SAP	SAP Cloud for Customer, Advanced User Option	8001006	$ 17.00	$ 15.13
SAP	SAP Cloud for Customer, B2B Industry User Option	8001007	$ 17.00	$ 15.13
SAP	SAP Cloud for Customer, Test Tenant	8000567	$ 11,000.00	$ 9,790.00
SAP	SAP Cloud for Customer, Additional Storage	8000568	$ 5.50	$ 4.90
SAP	SAP Cloud for Customer, Private Edition	8000981	$ 16,500.00	$ 14,685.00
SAP	SAP Cloud for Customer, enhanced package	8003185	$ 176.00	$ 156.64
SAP	SAP Cloud for Customer, limited package	8003186	$ 55.00	$ 48.95
SAP	SAP Cloud for Customer, Edge edition	8003938	$ 32.00	$ 28.48
SAP	SAP Cloud for Customer, enterprise edition	8003948	$ 219.00	$ 194.91
SAP	SAP Contact Center, e-channel, cloud ed.	8001016	$ 66.00	$ 58.74
SAP	SAP Contact Center, voice, cloud ed.	8001017	$ 121.00	$ 107.69

SAP	SAP Knowledge Central by Mindtouch-User	8003084	$ 17.00	$ 15.13
SAP	SAP Knowledge Central by Mindtouch-Ext Srv	8003085	$ 16,500.00	$ 14,685.00
SAP	SAP Knowledge Central by Mindtouch-Base	8003086	$ 4,400.00	$ 3,916.00
SAP	SAP Real-Time Communicator by GENBAND	8004033	$ 6.60	$ 5.87
SAP	SAP HANA Cloud Portal, Cloud for Customer Edition	8000793	$ 0.20	$ 0.20
SAP	SAP HANA Cloud Platform, extension package for SAP Cloud for Customer, standard edition	8003949	$ 17.00	$ 15.13
SAP	SAP HANA Cloud Platform, extension package for SAP Cloud for Customer, premium edition	8003950	$ 28.00	$ 24.92
SAP	SAP Workforce Performance Builder, Cloud	8003509-1	$ 109.00	$ 97.01
SAP	SAP Workforce Performance Builder, Cloud	8003509-2	$ 76.00	$ 67.64
SAP	SAP Workforce Performance Builder, Cloud	8003509-3	$ 64.00	$ 56.96
SAP	SAP Workforce Performance Builder, Cloud	8003509-4	$ 52.00	$ 46.28
SAP	SAP Workforce Performance Builder, Cloud	8003509-5	$ 43.00	$ 38.27
SAP	SAP Workforce Performance Builder, Cloud	8003509-6	$ 35.00	$ 31.15
SAP	SAP Workforce Performance Builder, Cloud	8003509-7	$ 29.00	$ 25.81
SAP	SAP Anywhere, starter bundle	8004078	$ 549.00	$ 488.61
SAP	SAP Anywhere, plus bundle	8004079	$ 934.00	$ 831.26
SAP	SAP Anywhere, premium bundle	8004080	$ 1,869.00	$ 1,663.41
SAP	SAP Anywhere, incremental user	8004084	$ 54.00	$ 48.06
SAP	SAP Anywhere, incremental channel	8004085	$ 109.00	$ 97.01
SAP	SAP HANA AppServices Compute Unit - Pro	8000348	$ 142.00	$ 126.38
SAP	SAP HANA AppServices Compute Unit - Prem	8000349	$ 208.00	$ 185.12
SAP	SAP HANA AppServices, Unstructured Storage	8000571	$ 11.00	$ 9.79
SAP	SAP HANA AppServices, Bandwidth	8000351	$ 4.40	$ 3.92
SAP	SAP HANA AppServices, 3rd Party Connect	8000573	$ 110.00	$ 97.90
SAP	SAP HANA AppServices, Administrator	8004159	$ 39.00	$ 34.71
SAP	SAP HANA AppServices, Cloud Portal	8004158	$ 193.00	$ 171.77
SAP	SAP HCP Starter Edition 32 GB	8001020	$ 439.00	$ 390.71
SAP	SAP HCP Starter Edition 64 GB	8001021	$ 549.00	$ 488.61
SAP	SAP HANA AppServices Custom Domains	8001022	$ 110.00	$ 97.90
SAP	SAP HANA Infrastructure Services 64 GB	8003366	$ 952.00	$ 847.28
SAP	SAP HANA Infrastructure Services 128 GB	8003367	$ 1,472.00	$ 1,310.08
SAP	SAP HANA Infrastructure Services 256 GB	8003368	$ 2,338.00	$ 2,080.82
SAP	SAP HANA Infrastructure Services 512 GB	8003369	$ 4,503.00	$ 4,007.67
SAP	SAP HANA Infrastructure Services 1024 GB	8003370	$ 6,668.00	$ 5,934.52
SAP	SAP HANA DBServices, base edition 32 GB	8003545	$ 1,375.00	$ 1,223.75
SAP	SAP HANA DBServices, base edition 64 GB	8003371	$ 2,602.00	$ 2,315.78
SAP	SAP HANA DBServices, base edition 128 GB	8003372	$ 4,772.00	$ 4,247.08
SAP	SAP HANA DBServices, base edition 256 GB	8003374	$ 8,938.00	$ 7,954.82
SAP	SAP HANA DBServices, base edition 512 GB	8003375	$ 17,703.00	$ 15,755.67
SAP	SAP HANA DBServices, base edition 1024 GB	8003376	$ 31,418.00	$ 27,962.02
SAP	SAP HANA DBServices, non-prod. base ed. 32 GB	8003547	$ 1,375.00	$ 1,223.75
SAP	SAP HANA DBServices, non-prod. base ed. 64 GB	8003377	$ 2,602.00	$ 2,315.78
SAP	SAP HANA DBServices, non-prod. base ed. 128 GB	8003378	$ 4,772.00	$ 4,247.08
SAP	SAP HANA DBServices, non-prod. base ed. 256 GB	8003379	$ 8,938.00	$ 7,954.82
SAP	SAP HANA DBServices, non-prod. base ed. 512 GB	8003380	$ 17,703.00	$ 15,755.67
SAP	SAP HANA DBServices, non-prod. base ed. 1024 GB	8003381	$ 31,418.00	$ 27,962.02
SAP	SAP HANA DBServices, platform edition 32 GB	8003546	$ 3,300.00	$ 2,937.00
SAP	SAP HANA DBServices, platform edition 64 GB	8003382	$ 6,232.00	$ 5,546.48
SAP	SAP HANA DBServices, platform edition 128 GB	8003383	$ 12,032.00	$ 10,708.48

SAP	SAP HANA DBServices, platform edition 256 GB	8003384	$ 23,458.00	$ 20,877.62
SAP	SAP HANA DBServices, platform edition 512 GB	8003385	$ 46,743.00	$ 41,601.27
SAP	SAP HANA DBServices, platform edition 1024 GB	8003386	$ 85,868.00	$ 76,422.52
SAP	SAP HANA DBServices, non-prod platform ed 32 GB	8003548	$ 3,300.00	$ 2,937.00
SAP	SAP HANA DBServices, non-prod platform ed 64 GB	8003387	$ 6,232.00	$ 5,546.48
SAP	SAP HANA DBServices, non-prod platform ed 128 GB	8003388	$ 12,032.00	$ 10,708.48
SAP	SAP HANA DBServices, non-prod. platform ed. 256 GB	8003389	$ 23,458.00	$ 20,877.62
SAP	SAP HANA DBServices, non-prod platform ed 512 GB	8003390	$ 46,743.00	$ 41,601.27
SAP	SAP HANA DBServices, non-prod platform ed 1024 GB	8003391	$ 85,868.00	$ 76,422.52
SAP	SAP HANA DBServices, ASE x-small	8003540	$ 550.00	$ 489.50
SAP	SAP HANA DBServices, ASE small	8003541	$ 770.00	$ 685.30
SAP	SAP HANA DBServices, ASE medium	8003542	$ 1,100.00	$ 979.00
SAP	SAP HANA DBServices, ASE large	8003543	$ 2,090.00	$ 1,860.10
SAP	SAP HANA DBServices, ASE x-large	8003544	$ 3,850.00	$ 3,426.50
SAP	SAP HANA DBServices, ASE non-production x-small	8003535	$ 550.00	$ 489.50
SAP	SAP HANA DBServices, ASE non-production small	8003536	$ 770.00	$ 685.30
SAP	SAP HANA DBServices, ASE non-production medium	8003537	$ 1,100.00	$ 979.00
SAP	SAP HANA DBServices, ASE non-production large	8003538	$ 2,090.00	$ 1,860.10
SAP	SAP HANA DBServices, ASE non-production x-large	8003539	$ 3,850.00	$ 3,426.50
SAP	SAP HANA Cloud Platform, professional edition	8003513	$ 22.00	$ 19.58
SAP	SAP HANA Cloud Platform, single application edition	8003514	$ 43.00	$ 38.27
SAP	SAP HANA Cloud Platform, multiple application edition	8003515	$ 130.00	$ 115.70
SAP	SAP HANA Cloud Platform gamification service	8004046	$ 1,100.00	$ 979.00
SAP	SAP HANA AppServices, standard edition	8003516	$ 1,089.00	$ 969.21
SAP	SAP HANA AppServices, premium edition	8003517	$ 3,619.00	$ 3,220.91
SAP	HANA Cloud Integration - Application Ed	8000800	$ 0.08	$ 0.08
SAP	HANA Cloud Integration Standard Edition	8002949	$ 2,200.00	$ 1,958.00
SAP	HANA Cloud Integration Professional Edition	8002951	$ 5,500.00	$ 4,895.00
SAP	HANA Cloud Integration, add'l connection	8002952	$ 385.00	$ 342.65
SAP	SAP HANA AppServices, Cloud Identity	8003511	$ 5.50	$ 4.90
SAP	SAP HANA AppServices, Web IDE Edition	8003103	$ 54.00	$ 48.06
SAP	SAP HCP, Remote Data Sync Service, standard edition	8003943	$ 587.00	$ 522.43
SAP	SAP HCP, Remote Data Sync Service, premium edition	8003944	$ 1,099.00	$ 978.11
SAP	SAP HCP Internet of Things Services	8003929	$ 2.20	$ 1.96
SAP	SAP TwoGo Location	8000776	$ 11.00	$ 9.79
SAP	SAP Mobile Documents Cloud, User	8000761	$ 4.40	$ 3.92
SAP	SAP Mobile Docs Cloud, Storage	8003298	$ 2.20	$ 1.96
SAP	SAP Mobile Secure, cloud edition	8004160	$ 1.65	$ 1.47
SAP	SAP Mobile App Protection by Mocana, cloud	8004161	$ 2.20	$ 1.96
SAP	SAP HCP Mobile Services, user	8003145	$ 5.50	$ 4.90
SAP	SAP HCP Mobile Services, consumer edition	8004024	$ 8,250.00	$ 7,342.50
SAP	SAP Forms as a Service	8003528	$ 4,400.00	$ 3,916.00
SAP	SAP Lumira Cloud, Professional Ed (GB)	8000782-1	$ 147.00	$ 130.83
SAP	SAP Lumira Cloud, Professional Ed (GB)	8000782-2	$ 246.00	$ 218.94
SAP	SAP Lumira Cloud, Professional Ed (GB)	8000782-3	$ 494.00	$ 439.66
SAP	SAP Lumira Cloud, Enterprise Ed, User	8000783	$ 24.00	$ 21.36
SAP	SAP Lumira Cloud,Ent Ed,Storage (per GB)	8000784	$ 24.00	$ 21.36
SAP	SAP Cloud for Analytics, Analytics Std User Public Ed.	8004104	$ 127.00	$ 113.03
SAP	SAP Cloud for Analytics, Planning Prof User Public Ed.	8004105	$ 1,733.00	$ 1,542.37

SAP	SAP Cloud for Analytics, Planning Std User Public Ed.	8004106	$ 121.00	$ 107.69
SAP	SAP Cloud for Analytics, BI User Public Ed.	8004107	$ 22.00	$ 19.58
SAP	SAP Digital Boardroom, Public Ed.	8004108	$ 11,000.00	$ 9,790.00
SAP	SAP Cloud for Analytics, Analytics Std User Private Ed.	8004099	$ 198.00	$ 176.22
SAP	SAP Cloud for Analytics, Planning Prof User Private Ed.	8004100	$ 2,200.00	$ 1,958.00
SAP	SAP Cloud for Analytics, Planning Std User Private Ed.	8004101	$ 165.00	$ 146.85
SAP	SAP Cloud for Analytics, BI User Private Ed.	8004102	$ 66.00	$ 58.74
SAP	SAP Digital Boardroom, Private Ed.	8004103	$ 16,500.00	$ 14,685.00
SAP	SAP Cloud for Analytics, BI Extension Public Ed.	8004110	$ 22.00	$ 19.58
SAP	SAP Cloud for Analytics, storage add-on (per 10 GB)	8003359	$ 11.00	$ 9.79
SAP	SAP Cloud for Analytics test tenant 32 GB Private Ed.	8003351	$ 2,567.00	$ 2,284.63
SAP	SAP Cloud for Analytics test tenant 64 GB Private Ed.	8003352	$ 2,842.00	$ 2,529.38
SAP	SAP Cloud for Analytics test tenant 128 GB Private Ed.	8003353	$ 3,392.00	$ 3,018.88
SAP	SAP Cloud for Analytics test tenant 256 GB Private Ed.	8003354	$ 6,783.00	$ 6,036.87
SAP	SAP Cloud for Analytics 64 GB HANA upgrade, Private Ed.	8003614	$ 642.00	$ 571.38
SAP	SAP Cloud for Analytics 128 GB HANA upgrade, Private Ed.	8003355	$ 642.00	$ 571.38
SAP	SAP Cloud for Analytics 256 GB HANA upgrade, Private Ed.	8003356	$ 1,100.00	$ 979.00
SAP	SAP Cloud for Analytics 512 GB HANA upgrade, Private Ed.	8003357	$ 2,200.00	$ 1,958.00
SAP	SAP Cloud for Analytics 1024 GB HANA upgrade, Private Ed.	8003358	$ 2,750.00	$ 2,447.50
SAP	SAP Agile Data Preparation, cloud edition, technology foundation	8004122	$ 35,200.00	$ 31,328.00
SAP	SAP Agile Data Preparation, cloud edition, analyst option	8004123	$ 550.00	$ 489.50
SAP	SAP API Mgmt, standard cloud edition	8003674	$ 8,250.00	$ 7,342.50
SAP	SAP API Mgmt, premier cloud edition	8003676	$ 11,000.00	$ 9,790.00
SAP	SAP API Mgmt, enterprise cloud edition	8003677	$ 16,500.00	$ 14,685.00
SAP	Preferred Care, SuccessFactors	8003322	$ 0.20	
SAP	Preferred Care, SAP	8003430	$ 0.20	
SAP	Expert Care, Ariba	8002441	$ 0.30	
ServiceNow	ServiceNow® Additional Non-Production Instance - US Data Center (Monthly)	VOPADDINSTDC-US	$ 1,250.00	$ 1,240.55
ServiceNow	ServiceNow® Additional Production Environment - US Data Center (Monthly)	ADDPRODENVRNMTUS	$ 3,750.00	$ 3,721.66
ServiceNow	ServiceNow® Approver User (Monthly)	SNCAPPROVER-36	$ 25.00	$ 24.81
ServiceNow	ServiceNow® Cloud Management - Node (250 Node Minimum Quantity)	SNCPROD90874	$ 7.00	$ 6.95
ServiceNow	ServiceNow® Customer Service Management - Fulfiller User (Monthly)	SNCPROD103484	$ 125.00	$ 124.06
ServiceNow	ServiceNow® Discovery - Node (250 Node Minimum Quantity)	SNCPROD90840	$ 6.00	$ 5.95
ServiceNow	ServiceNow® Event Management - Node (250 Node Minimum Quantity)	SNCPROD90854	$ 7.00	$ 6.95
ServiceNow	ServiceNow® Express Discovery (100 Pack) - Devices (Monthly)	SNCPROD01057	$ 20.00	$ 19.85
ServiceNow	ServiceNow® Express Discovery (1000 Pack - 500 Included at No Charge) - Devices (Monthly)	SNCPROD01056	$ 100.00	$ 99.24
ServiceNow	ServiceNow® Express Fulfiller User (Monthly)	SNCEXPRESS	$ 50.00	$ 49.62
ServiceNow	ServiceNow® Facilities Service Automation - Unrestricted User (1000 Unrestricted User Minimum Quantity)	SNFACILITIESSVC	$ 7.00	$ 6.95
ServiceNow	ServiceNow® Financial Management - Fulfiller User (Monthly)	SNCFINMGMT	$ 1,250.00	$ 1,240.55
ServiceNow	ServiceNow® Governance, Risk and Compliance Suite - Fulfiller User	SNCPROD90746	$ 125.00	$ 124.06
ServiceNow	ServiceNow® IT Financial Management - Unrestricted User (1000 Unrestricted User Minimum Quantity) (Monthly)	SNCFINMGMTUN	$ 1.00	$ 0.99
ServiceNow	ServiceNow® IT Service Automation Suite - Unrestricted User (1000 Unrestricted User Minimum Quantity) (Monthly)	SNCSVCSAUTSTEGVT-UR	$ 10.00	$ 9.92
ServiceNow	ServiceNow® ITSA Unlimited - Fulfiller User (Monthly)	SNITSAUNLTD	$ 350.00	$ 347.36
ServiceNow	ServiceNow® ITSA Unlimited (Including Platform Runtime) - Fulfiller User	SNCPROD90795	$ 200.00	$ 198.49
ServiceNow	ServiceNow® Notify (All users) - User (Monthly)	SNCNOTIFYAL	$ 1.25	$ 1.24
ServiceNow	ServiceNow® Orchestration Client Software Distribution Application - Client Node (250 Node Minimum Quantity)	SNCPROD90836	$ 1.00	$ 0.99
ServiceNow	ServiceNow® Orchestration Core (10,000 Password Users and 1000 Client SW Dist. Client Nodes included) - Node (250 Node Minimum Quantity)	SNCPROD90863	$ 6.00	$ 5.95
ServiceNow	ServiceNow® Orchestration Password Reset Application - User (Monthly)	SNCORCHPASSWORD	$ 0.50	$ 0.50
ServiceNow	ServiceNow® Performance Analytics - Application (per $1000 Subscription) (Monthly)	SNCPERFANAUSER	$ 200.00	$ 198.49

ServiceNow	ServiceNow® Performance Analytics For IT Service Automation Suite - Application (per $1000 Subscription) (Monthly)	SNCPERFANAITSA	$ 200.00	$ 198.49
ServiceNow	ServiceNow® Performance Analytics For Service Management Suite - Application (per $1000 Subscription) (Monthly)	SNCPERFANASERVMGMT	$ 200.00	$ 198.49
ServiceNow	ServiceNow® Performance Analytics For Service Management Suite With Platform Runtime - Application (per $1000 Subscription) (Monthly)	SNCPROD90797	$ 200.00	$ 198.49
ServiceNow	ServiceNow® Platform Runtime - Fulfiller User	SNCPROD90781	$ 35.00	$ 34.74
ServiceNow	ServiceNow® Project Portfolio Suite - Fulfiller User (Monthly)	SNCPROJPORTUF	$ 75.00	$ 74.43
ServiceNow	ServiceNow® Project Portfolio Suite - Unrestricted User (1000 Unrestricted User Minimum Quantity) (Monthly)	SNCPROJPORTU-UR	$ 8.00	$ 7.94
ServiceNow	ServiceNow® Public Catalog - Requests (Additonal Requests) (Monthly)	SNCPUBCATADD-36	$ 0.42	$ 0.42
ServiceNow	ServiceNow® Public Catalog - Requests (Tier 1) (Monthly)	SNCPUBCAT1-36	$ 8,333.33	$ 8,270.36
ServiceNow	ServiceNow® Public Catalog - Requests (Tier 2) (Monthly)	SNCPUBCAT2-36	$ 10,416.67	$ 10,337.95
ServiceNow	ServiceNow® Public Catalog - Requests (Tier 3) (Monthly)	SNCPUBCAT3-36	$ 12,500.00	$ 12,405.54
ServiceNow	ServiceNow® Public Catalog - Requests (Tier 4) (Monthly)	SNCPUBCAT4-36	$ 16,666.67	$ 16,540.72
ServiceNow	ServiceNow® Public Catalog - Requests (Tier 5) (Monthly)	SNCPUBCAT5-36	$ 20,833.33	$ 20,675.90
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 1 to Tier 2 (Up to 19999 Requests) (Monthly)	SNCPUBCAT1-2	$ 2,083.34	$ 2,067.60
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 1 to Tier 3 (Up to 99999 Requests) (Monthly)	SNCPUBCAT1-3	$ 4,166.67	$ 4,135.18
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 1 to Tier 4 (Up to 299999 Requests) (Monthly)	SNCPUBCAT1-4	$ 8,333.34	$ 8,270.37
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 1 to Tier 5 (Up to 599999 Requests) (Monthly)	SNCPUBCAT1-5	$ 12,500.00	$ 12,405.54
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 2 to Tier 3 (Up to 99999 Requests) (Monthly)	SNCPUBCAT2-3	$ 2,083.33	$ 2,067.59
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 2 to Tier 4 (Up to 299999 Requests) (Monthly)	SNCPUBCAT2-4	$ 6,250.00	$ 6,202.77
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 2 to Tier 5 (Up to 599999 Requests) (Monthly)	SNCPUBCAT2-5	$ 10,416.66	$ 10,337.94
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 3 to Tier 4 (Up to 299999 Requests) (Monthly)	SNCPUBCAT3-4	$ 4,166.67	$ 4,135.18
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 3 to Tier 5 (Up to 599999 Requests) (Monthly)	SNCPUBCAT3-5	$ 8,333.33	$ 8,270.36
ServiceNow	ServiceNow® Public Catalog - Upgrade From Tier 4 to Tier 5 (Up to 599999 Requests) (Monthly)	SNCPUBCAT4-5	$ 4,166.66	$ 4,135.17
ServiceNow	ServiceNow® Security Operations - Devices (250 Device Minimum Quantity) (Monthly)	SNCPROD104598	$ 0.75	$ 0.74
ServiceNow	ServiceNow® Security Operations (1,000 Devices Included) - Module (Monthly)	SNCPROD104565	$ 6,250.00	$ 6,202.77
ServiceNow	ServiceNow® Service Automation Platform Suite - Process User (Monthly)	SNCSVCSAUTPLT	$ 100.00	$ 99.24
ServiceNow	ServiceNow® Service Catalog With Request Management - Unrestricted Users (1000 Unrestricted User Minimum Quantity) (Monthly)	SNCSERVCATREQMG	$ 3.00	$ 2.98
ServiceNow	ServiceNow® Service Management Suite - Fulfiller User (Monthly)	SNCSERVMGMT	$ 100.00	$ 99.24
ServiceNow	ServiceNow® Service Management Suite - Unrestricted User (1000 Unrestricted User Minimum Quantity) (Monthly)	SNCSERVMGMTUN	$ 20.00	$ 19.85
ServiceNow	ServiceNow® Service Management Suite With Platform Runtime - Fulfiller User	SNCPROD90798	$ 125.00	$ 124.06
ServiceNow	ServiceNow® ServiceWatch (Eureka and Fuji Only) - Nodes (250 Node Minimum Quantity) (Monthly)	SNCPROD125784	$ 17.00	$ 16.87
ServiceNow	ServiceNow® ServiceWatch Insight (Discovery, Service Mapping and Event Management included) - Node (250 Node Minimum Quantity)	SNCPROD90862	$ 17.00	$ 16.87
ServiceNow	ServiceNow® ServiceWatch Mapping (Discovery and Service Mapping included) - Node (250 Node Minimum Quantity)	SNCPROD90845	$ 14.00	$ 13.89
ServiceNow	ServiceNow® ServiceWatch Suite - Node (250 Node Minimum Quantity)	SNCPROD90911	$ 26.00	$ 25.80
ServiceNow	ServiceNow® Time Card User - Time Card User (Monthly)	SNCTIMECARD	$ 15.00	$ 14.89
ServiceNow	ServiceNow® Field Service Automation - Unrestricted User (1000 Unrestricted User Minimum Quantity)	SNFIELDSVCAUTU	$ 7.00	$ 6.95
ServiceNow	ServiceNow® HR Service Automation - Unrestricted User (1000 Unrestricted User Minimum Quantity)	SNCHRSERVICEU	$ 7.00	$ 6.95
ServiceNow	ServiceNow® Edge Encryption - Application (per $1000 Subscription) User (Monthly)	SNCPROD01054	$ 200.00	$ 198.49
ServiceNow	ServiceNow® HR Service Management - Unrestricted User (1000 Unrestricted User Minimum Quantity)	SNCHRSERVICE	$ 5.00	$ 4.96
ServiceNow	ServiceNow® Service Management Suite v2 - Fulfiller User	SNCSERVMGMTV2	$ 100.00	$ 99.24
ServiceNow	ServiceNow® Service Management Suite v2 With Platform Runtime - Fulfiller User	SNCSERVPLATRTV2	$ 125.00	$ 124.06
ServiceNow	ServiceNow® Service Strategy - Worker	SNCSERVSTRAT	$ 30.00	$ 29.77
ServiceNow	ServiceNow® Service Strategy - Planner	SNCSERVSTRAT	$ 75.00	$ 74.43
ServiceNow	ServiceNow® Service Strategy - Analyst	SNCSERVSTRAT	$ 1,250.00	$ 1,240.55
ServiceNow	ServiceNow® Reporting and Performance Analytics (2 days) - Public (per attendee)	PROD00975	$ 1,595.00	$ 1,582.95
ServiceNow	ServiceNow® Reporting and Performance Analytics (2 days) - On-Site Class (per attendee, minimum 5 attendees)	PROD00981	$ 1,595.00	$ 1,582.95
ServiceNow	ServiceNow® Reporting and Performance Analytics (2 days) - On-Site Class (additional attendee)	PROD00982	$ 1,595.00	$ 1,582.95
Virtru	VTRUEMAIL001	Virtru email encryption licen	$ 60.00	$ 58.65
Virtru	VTRUDRIVE002	Virtru Google Drive encryptic	$ 60.00	$ 58.65
Virtru	VTRUHIPAA003	Preconfigured DLP rules that	$ 499.00	$ 487.77

Virtru	VTRUTEMP004	Customer's logo added to th	$ 499.00	$ 487.77
Virtru	VTRUGTWY005	Server-side gateway that sca	$ 30,000.00	$ 29,325.00
Virtru	VTRUSR006	Customer's branding added t	$ 9,999.00	$ 9,774.02
Virtru	VTRUCLI007	Command line interace (CLI)	$ 1,999.00	$ 1,954.02
Virtustream	System Backup Setup	IC-DP-BU-1T	$ 500.00	$ 465.00
Virtustream	vHANA Installation and Setup Charge - Virtual Appliance	HM-HA-VIR-1T	$ 1,000.00	$ 930.00
Virtustream	Policy Auditor Service Setup	CS-VS-PSVC-1T	$ 62.50	$ 58.13
Virtustream	Policy Auditor System Setup	CS-VS-PSYS-1T	$ 1,500.00	$ 1,395.00
Virtustream	1 TB HANA Managed Appliance (Single Node/Scale-Up) - Primary	HM-HA1-SN-1TB	$ 6,924.60	$ 6,439.88
Virtustream	1 TB HANA Managed Appliance (Single Node/Scale-Up) - Secondary	HM-HA2-SN-1TB	$ 6,924.60	$ 6,439.88
Virtustream	1 TB HANA Managed Appliance for BW (Scale-Out) - Primary	HM-HA1-SO-1TB	$ 7,883.96	$ 7,332.08
Virtustream	1 TB HANA Managed Appliance for BW (Scale-Out) - Secondary	HM-HA2-SO-1TB	$ 7,883.96	$ 7,332.08
Virtustream	1 TB HANA Managed Appliance for SoH - Primary	HM-HA1-SOH-1TB	$ 7,049.50	$ 6,556.03
Virtustream	1 TB HANA Managed Appliance for SoH - Secondary	HM-HA2-SOH-1TB	$ 7,049.50	$ 6,556.03
Virtustream	1.5 TB HANA Managed Appliance for SoH - Primary	HM-HA1-SOH-15	$ 7,889.70	$ 7,337.43
Virtustream	1.5 TB HANA Managed Appliance for SoH - Secondary	HM-HA2-SOH-15	$ 7,889.70	$ 7,337.43
Virtustream	2 TB HANA Managed Appliance (Single Node/Scale-Up) - Primary	HM-HA1-SN-2TB	$ 16,353.69	$ 15,208.93
Virtustream	2 TB HANA Managed Appliance (Single Node/Scale-Up) - Secondary	HM-HA2-SN-2TB	$ 16,353.69	$ 15,208.93
Virtustream	2 TB HANA Managed Appliance for BW (Scale-Out) - Primary	HM-HA1-SO-2TB	$ 15,978.11	$ 14,859.65
Virtustream	2 TB HANA Managed Appliance for BW (Scale-Out) - Secondary	HM-HA2-SO-2TB	$ 15,978.11	$ 14,859.65
Virtustream	2 TB HANA Managed Appliance for SoH - Primary	HM-HA1-SOH-2TB	$ 8,438.34	$ 7,847.65
Virtustream	2 TB HANA Managed Appliance for SoH - Secondary	HM-HA2-SOH-2TB	$ 8,438.34	$ 7,847.65
Virtustream	2FA Dedicated Base Fee	CS-2F-D1-SYS	$ 150.00	$ 139.50
Virtustream	2FA Dedicated DR Base Fee	CS-2F-D2-SYS	$ 45.00	$ 41.85
Virtustream	2FA Dedicated Token Fee	CS-2F-DT-MF	$ 9.00	$ 8.37
Virtustream	2FA Shared Token Fee	CS-2F-ST-MF	$ 11.00	$ 10.23
Virtustream	2FA Virtustream Portal Token Fee	CS-2F-VPT-MF	$ 9.00	$ 8.37
Virtustream	3 TB HANA Managed Appliance for SoH - Primary	HM-HA1-SOH-3TB	$ 9,613.54	$ 8,940.59
Virtustream	3 TB HANA Managed Appliance for SoH - Secondary	HM-HA2-SOH-3TB	$ 9,613.54	$ 8,940.59
Virtustream	512 GB HANA Managed Appliance (Single Node/Scale-Up) - Primary	HM-HA1-SN-512	$ 5,472.60	$ 5,089.52
Virtustream	512 GB HANA Managed Appliance (Single Node/Scale-Up) - Secondary	HM-HA2-SN-512	$ 5,472.60	$ 5,089.52
Virtustream	512 GB HANA Managed Appliance for BW (Scale-Out) - Primary	HM-HA1-SO-512	$ 6,533.21	$ 6,075.89
Virtustream	512 GB HANA Managed Appliance for BW (Scale-Out) - Secondary	HM-HA2-SO-512	$ 6,533.21	$ 6,075.89
Virtustream	6 TB HANA Managed Appliance for SoH - Primary	HM-HA1-SOH-6TB	$ 25,124.52	$ 23,365.81
Virtustream	6 TB HANA Managed Appliance for SoH - Secondary	HM-HA2-SOH-6TB	$ 25,124.52	$ 23,365.81
Virtustream	Encryption Non-Production Agent per vCPU Fee	CS-ENC-AGTC-NP	$ 30.00	$ 27.90
Virtustream	Encryption Production Agent per vCPU Fee	CS-ENC-AGTC-PR	$ 60.00	$ 55.80
Virtustream	HANA Encryption Agent Fee (Non-Production)	CS-ENC-AGTH-NP	$ 125.00	$ 116.25
Virtustream	HANA Encryption Agent Fee (Production)	CS-ENC-AGTH-PR	$ 250.00	$ 232.50
Virtustream	Enterprise Basic Plus µVM	IC-UVM-BASP-ENT	$ 66.00	$ 61.38
Virtustream	Enterprise Reserve µVM	IC-UVM-RESV-ENT	$ 10.00	$ 9.30
Virtustream	Encryption Management System Fee	CS-ENC-SYS-SYS	$ 850.00	$ 790.50
Virtustream	Firewall Audit System	CS-FA-FA-SYS	$ 675.00	$ 627.75
Virtustream	Managed Firewall Auditing Service	CS-FA-MFA-SVC	$ 270.00	$ 251.10
Virtustream	Anti-Virus Primary System	CS-TM-AV1-SYS	$ 25.00	$ 23.25
Virtustream	Anti-Virus Secondary System	CS-TM-AV2-SYS	$ 25.00	$ 23.25
Virtustream	Anti-Virus Managed Service	CS-TM-AV-SVC	$ 24.99	$ 23.24
Virtustream	File Integrity Monitoring Primary System	CS-TM-FIM1-SYS	$ 25.00	$ 23.25
Virtustream	File Integrity Monitoring Secondary System	CS-TM-FIM2-SYS	$ 25.00	$ 23.25

Virtustream	High Memory Enterprise Basic Plus µVM	IC-UHV-BASP-ENT	$ 24.00	$ 22.32
Virtustream	High Memory Enterprise Basic Plus VM Fee	IC-HVM-BASP-ENT	$ 1,275.00	$ 1,185.75
Virtustream	High Memory Enterprise Reserve µVM	IC-UHV-RESV-ENT	$ 6.50	$ 6.05
Virtustream	Intrusion Detection and Firewall Primary System	CS-TM-IDFW1-SYS	$ 203.57	$ 189.32
Virtustream	Intrusion Detection and Firewall Secondary System	CS-TM-IDFW2-SYS	$ 25.00	$ 23.25
Virtustream	IPSec VPN Bandwidth Fee - USDC1	CS-VPN-U1-NET	$ 31.25	$ 29.06
Virtustream	IPSec VPN Bandwidth Fee - USDC2	CS-VPN-U2-NET	$ 31.25	$ 29.06
Virtustream	IPSec VPN Tunnel Managed Service	CS-VPN-T-SVC	$ 50.00	$ 46.50
Virtustream	Load Balancing Bandwidth Fee (Additional to Network Bandwidth)	IC-NW-LBM-NET	$ 22.50	$ 20.93
Virtustream	Intrusion Detection and Firewall Managed Service	CS-TM-IDFW-SVC	$ 73.74	$ 68.57
Virtustream	VM-Level Security Bundle Primary System fee	CS-TM-VLSB1-SYS	$ 190.18	$ 176.87
Virtustream	Managed Load Balancer Services (Per Server)	IC-NW-LBM-LB	$ 100.00	$ 93.00
Virtustream	VM-Level Security Bundle Secondary System fee	CS-TM-VLSB2-SYS	$ 56.25	$ 52.31
Virtustream	Managed Perimeter Firewall	CS-FW-MPF-SVC	$ 25.00	$ 23.25
Virtustream	Microsoft OS	IC-SW-MSS-WIN	$ 50.00	$ 46.50
Virtustream	Microsoft SQL Enterprise (Per 2 cores)	IC-SW-MQL-ENT	$ 575.00	$ 534.75
Virtustream	Microsoft SQL Standard (Per 2 cores)	IC-SW-MQL-STD	$ 150.00	$ 139.50
Virtustream	Network Bandwidth Fee - USDC1	CS-NW-BWU1-NET	$ 28.75	$ 26.74
Virtustream	Network Bandwidth Fee - USDC2	CS-NW-BWU2-NET	$ 28.75	$ 26.74
Virtustream	Network Based Intrusion Detection System and Managed Service - Secondary	CS-IDS-NB2-SYS	$ 477.00	$ 443.61
Virtustream	Network Based Intrusion Detection System and Managed Service - Primary	CS-IDS-NB1-SYS	$ 957.00	$ 890.01
Virtustream	VM-Level Security Bundle Service Fee (<101 VMs)	CS-TM-VLSBA-SVC	$ 116.14	$ 108.01
Virtustream	VM-Level Security Bundle Service Fee (<1001 VMs)	CS-TM-VLSBB-SVC	$ 105.92	$ 98.50
Virtustream	Public IP Address (IPv4)	IC-NW-IPAD-V4	$ 25.00	$ 23.25
Virtustream	Public IP Address (IPv6)	IC-NW-IPAD-V6	$ 5.00	$ 4.65
Virtustream	Red Hat Enterprise Linux - Enterprise (Per OS)	IC-SW-RHL-ENT	$ 100.00	$ 93.00
Virtustream	Red Hat Enterprise Linux - Standard (Per OS)	IC-SW-RHL-STD	$ 50.00	$ 46.50
Virtustream	Remote Desktop Services (Per User)	IC-SW-RDS-IF	$ 7.50	$ 6.98
Virtustream	SUSE Linux Enterprise <=2 vCPU & <=2GB RAM	IC-SW-SLES-2C	$ 110.00	$ 102.30
Virtustream	SUSE Linux Enterprise <=4 vCPU & <=8GB RAM	IC-SW-SLES-4C	$ 150.00	$ 139.50
Virtustream	SUSE Linux Enterprise <=8 vCPU & >8GB RAM	IC-SW-SLES-8C	$ 250.00	$ 232.50
Virtustream	SUSE Linux Enterprise > 8 vCPU & >8GB RAM	IC-SW-SLES-VCPU	$ 32.00	$ 29.76
Virtustream	SUSE Linux Enterprise for Physical HANA	IC-SW-SLES-PH	$ 200.00	$ 186.00
Virtustream	SUSE Linux Enterprise for SAP <=2 vCPU & <=2GB RAM	IC-SW-SLES-S2C	$ 200.00	$ 186.00
Virtustream	SUSE Linux Enterprise for SAP <=4 vCPU & <=8GB RAM	IC-SW-SLES-S4C	$ 275.00	$ 255.75
Virtustream	SUSE Linux Enterprise for SAP >4 vCPU or >8GB RAM	IC-SW-SLES-SVM	$ 325.00	$ 302.25
Virtustream	SUSE Linux Enterprise for Virtual HANA	IC-SW-SLES-VH	$ 73.00	$ 67.89
Virtustream	STABDARD System Backup (PROTECTED)- Local Only	IC-DP-BUP-LOC	$ 0.30	$ 0.28
Virtustream	STANDARD System Backup (PROTECTED) - Replicated	IC-DP-BUP-REP	$ 0.40	$ 0.37
Virtustream	HANA System Backup (Protected Data) - Local Only	IC-DP-BUPH-LOC	$ 1.35	$ 1.26
Virtustream	HANA System Backup (Protected Data) - Replicated	IC-DP-BUPH-REP	$ 1.80	$ 1.67
Virtustream	Tier 0 Block Storage - Local Only	IC-STO-T0A-LOC	$ 0.99	$ 0.92
Virtustream	Tier 0 Block Storage - Replicated	IC-STO-T0A-REP	$ 2.23	$ 2.07
Virtustream	Tier I Block Storage - Local Only	IC-STO-T1A-LOC	$ 0.53	$ 0.49
Virtustream	Tier I Block Storage - Replicated	IC-STO-T1A-REP	$ 1.16	$ 1.07
Virtustream	Tier II Block Storage - Local Only	IC-STO-T2A-LOC	$ 0.37	$ 0.34
Virtustream	Tier II Block Storage - Replicated	IC-STO-T2A-REP	$ 0.84	$ 0.78
Virtustream	Tier III Block Storage - Local Only	IC-STO-T3A-LOC	$ 0.16	$ 0.15
Virtustream	Tier III Block Storage – Replicated	IC-STO-T3A-REP	$ 0.42	$ 0.39

Virtustream	VM-Level Security Bundle Service Fee (<10,001 VMs)	CS-TM-VLSBC-SVC	$ 99.00	$ 92.07
Virtustream	VM-Level Security Bundle Service Fee (10,000+ VMs)	CS-TM-VLSBD-SVC	$ 88.72	$ 82.51
Virtustream	Log Management System Fee	CS-VS-LM-SYS	$ 2,000.00	$ 1,860.00
Virtustream	Managed Log Management Service	CS-VS-MLM-SVC	$ 60.00	$ 55.80
Virtustream	Policy Auditor Service Fee	CS-VS-PA-SVC	$ 73.00	$ 67.89
Virtustream	Policy Auditor System Fee	CS-VS-PA-SYS	$ 125.00	$ 116.25
Virtustream	Vulnerability Scanning Managed Service - non Public IP	CS-VS-NPIP-SVC	$ 100.00	$ 93.00
Virtustream	Vulnerability Scanning Remedial Ad Hoc Scan	CS-VS-NPIP-AH	$ 450.00	$ 418.50
Virtustream	Vulnerability Scanning Managed Service - Public IP	CS-VS-PIP-SVC	$ 500.00	$ 465.00
Virtustream	Co-Innovation Roundtables - Ad Hoc (6 months)	CC-TAM-CIR-AH	$ 5,850.00	$ 5,440.50
Virtustream	Demand Management Meetings - Ad Hoc (3 months)	CC-TAM-DMM-AH	$ 3,217.50	$ 2,992.28
Virtustream	Executive Scorecards - Ad Hoc (3 months)	CC-TAM-ES-AH	$ 3,510.00	$ 3,264.30
Virtustream	IT Resource Forecast - Ad Hoc (3 months)	CC-TAM-ITRF-AH	$ 7,020.00	$ 6,528.60
Virtustream	Reporting and Business Review - Ad Hoc (1 month)	CC-TAM-RBR-AH	$ 4,638.75	$ 4,314.04
Virtustream	Resource and Performance - Ad Hoc (1 month)	CC-TAM-RP-AH	$ 4,203.75	$ 3,909.49
Virtustream	SLA Review - Ad Hoc (1 month)	CC-TAM-SLAR-AH	$ 1,755.00	$ 1,632.15
Virtustream	Weekly Status and Incident Reporting - Ad Hoc (1 month)	CC-TAM-WSIR-AH	$ 3,330.00	$ 3,096.90
Virtustream	Cloud Cover Setup	CC-SVC-ONCC-1T	$ 155.00	$ 144.15
Virtustream	Onshore SAP User, Security, and Change Management Process Setup	CC-SAP-ONUS-1T	$ 2,750.00	$ 2,557.50
Virtustream	Onshore Business Operating System & Database Support	CC-NS-ONDB-BUS	$ 550.00	$ 511.50
Virtustream	Onshore Business Operating System Support	CC-NS-ONOS-BUS	$ 312.50	$ 290.63
Virtustream	Onshore Business SAP Technical Support (Non-Prod/Basis)	CC-SAP-ONNH-BUS	$ 1,031.25	$ 959.06
Virtustream	Onshore Business SAP Technical Support (Prod/Basis)	CC-SAP-ONPH-BUS	$ 2,625.00	$ 2,441.25
Virtustream	Onshore Enterprise Operating System & Database Support	CC-NS-ONDB-ENT	$ 675.00	$ 627.75
Virtustream	Onshore Enterprise Operating System Support	CC-NS-ONOS-ENT	$ 406.25	$ 377.81
Virtustream	Onshore Enterprise SAP Technical Support (Non-Prod/Basis)	CC-SAP-ONNH-ENT	$ 2,625.00	$ 2,441.25
Virtustream	Onshore Enterprise SAP Technical Support (Prod/Basis)	CC-SAP-ONPH-ENT	$ 3,625.00	$ 3,371.25
Virtustream	Onshore Standard Operating System & Database Support	CC-NS-ONDB-STD	$ 168.75	$ 156.94
Virtustream	Onshore Standard Operating System Support	CC-NS-ONOS-STD	$ 93.75	$ 87.19
Virtustream	Onshore Standard SAP Technical Support (Non-Prod)	CC-SAP-ONNH-STD	$ 406.25	$ 377.81
Virtustream	Onshore Standard SAP Technical Support (Prod)	CC-SAP-ONPH-STD	$ 687.50	$ 639.38
Virtustream	Operational Integration - 1 Year	CC-TAM-OPIN-1Y	$ 1,950.00	$ 1,813.50
Virtustream	Reporting and Business Review - 1 Year	CC-TAM-RBR-1Y	$ 3,092.50	$ 2,876.03
Virtustream	Resource and Performance - 1 Year	CC-TAM-RP-1Y	$ 2,802.50	$ 2,606.33
Virtustream	SLA Review - 1 Year	CC-TAM-SLAR-1Y	$ 1,170.00	$ 1,088.10
Virtustream	Technical Account Management (TAM) - Gold	CC-TAM-TAM-GOLD	$ 12,000.00	$ 11,160.00
Virtustream	Technical Account Management (TAM) - Silver	CC-TAM-TAM-SILV	$ 6,000.00	$ 5,580.00
Virtustream	Technical Account Manager (TAM) - Platinum	CC-TAM-TAM-PLAT	$ 24,000.00	$ 22,320.00
Virtustream	Technical Account Management (TAM) - Per Instance	CC-TAM-TAM-INST	$ 400.00	$ 372.00
Virtustream	Weekly Status and Incident Reporting - 1 Year	CC-TAM-WSIR-1Y	$ 2,220.00	$ 2,064.60
Virtustream	Rack & Stack (Full Cab) - USDC2	DC-RKU2-RS-1T	$ 1,562.50	$ 1,453.13
Virtustream	Rack & Stack (Full Cab) - USDC1	DC-RKU1-RS-1T	$ 1,562.50	$ 1,453.13
Virtustream	Remote Eyes & Hands (US) - Bronze/Silver Ad Hoc (1 Hour)	DC-SVC-REU-SAH1	$ 150.00	$ 139.50
Virtustream	Remote Eyes & Hands (US) - Bronze/Silver Ad Hoc (15 Minutes)	DC-SVC-REU-SAHQ	$ 37.50	$ 34.88
Virtustream	Remote Eyes & Hands (US) - Gold Ad Hoc (1 Hour)	DC-SVC-REU-GAH1	$ 175.00	$ 162.75
Virtustream	Remote Eyes & Hands (US) - Gold Ad Hoc (15 Minutes)	DC-SVC-REU-GAHQ	$ 43.75	$ 40.69
Virtustream	Cloud Connect - HA (48 ports available) - Setup - USDC1	DC-NWU1-XCH-1T	$ 650.00	$ 604.50
Virtustream	Cloud Connect - HA (48 ports available) - Setup - USDC2	DC-NWU2-XCH-1T	$ 650.00	$ 604.50
Virtustream	Cloud Connect - Standard (24 Ports Available) - Setup - USDC1	DC-NWU1-XCS-1T	$ 450.00	$ 418.50

Virtustream	Cloud Connect - Standard (24 Ports Available) - Setup - USDC2	DC-NWU2-XCS-1T	$ 450.00	$ 418.50
Virtustream	Coax Cross Connect - USDC1 - Installation	DC-NWU1-XCCX-1T	$ 200.00	$ 186.00
Virtustream	Coax Cross Connect - USDC2 - Installation	DC-NWU2-XCCX-1T	$ 200.00	$ 186.00
Virtustream	Copper Cross Connect - USDC1 - Installation	DC-NWU1-XCC-1T	$ 250.00	$ 232.50
Virtustream	Copper Cross Connect - USDC2 - Installation	DC-NWU2-XCC-1T	$ 250.00	$ 232.50
Virtustream	Fiber Cross Connect - USDC1 - Installation	DC-NWU1-XCF-1T	$ 500.00	$ 465.00
Virtustream	Fiber Cross Connect - USDC2 - Installation	DC-NWU2-XCF-1T	$ 500.00	$ 465.00
Virtustream	20 A / 120 V Power Strip - USDC1	DC-PWU1-21S-1T	$ 1,125.00	$ 1,046.25
Virtustream	20 A / 120 V Power Strip - USDC2	DC-PWU2-21S-1T	$ 1,125.00	$ 1,046.25
Virtustream	20 A / 120 V Primary / Redundant Power - USDC1 - Installation	DC-PWU1-21R-1T	$ 3,020.84	$ 2,809.38
Virtustream	20 A / 120 V Primary / Redundant Power - USDC2 - Installation	DC-PWU2-21R-1T	$ 4,479.16	$ 4,165.62
Virtustream	20 A / 120 V Primary Power - USDC1 - Installation	DC-PWU1-21P-1T	$ 1,979.16	$ 1,840.62
Virtustream	20 A / 120 V Primary Power - USDC2 - Installation	DC-PWU2-21P-1T	$ 2,916.66	$ 2,712.49
Virtustream	20 A / 208 V Power Strip - USDC1	DC-PWU1-22S-1T	$ 1,375.00	$ 1,278.75
Virtustream	20 A / 208 V Power Strip - USDC2	DC-PWU2-22S-1T	$ 1,375.00	$ 1,278.75
Virtustream	20 A / 208 V Primary / Redundant Power - USDC1 - Installation	DC-PWU1-22R-1T	$ 3,125.00	$ 2,906.25
Virtustream	20 A / 208 V Primary / Redundant Power - USDC2 - Installation	DC-PWU2-22R-1T	$ 4,687.50	$ 4,359.38
Virtustream	20 A / 208 V Primary Power - USDC1 - Installation	DC-PWU1-22P-1T	$ 2,083.34	$ 1,937.51
Virtustream	20 A / 208 V Primary Power - USDC2 - Installation	DC-PWU2-22P-1T	$ 3,229.16	$ 3,003.12
Virtustream	30 A / 120 V Power Strip - USDC1	DC-PWU1-31S-1T	$ 1,375.00	$ 1,278.75
Virtustream	30 A / 120 V Power Strip - USDC2	DC-PWU2-31S-1T	$ 1,375.00	$ 1,278.75
Virtustream	30 A / 120 V Primary / Redundant Power - USDC1 - Installation	DC-PWU1-31R-1T	$ 4,583.34	$ 4,262.51
Virtustream	30 A / 120 V Primary / Redundant Power - USDC2 - Installation	DC-PWU2-31R-1T	$ 7,291.66	$ 6,781.24
Virtustream	30 A / 120 V Primary Power - USDC1 - Installation	DC-PWU1-31P-1T	$ 3,125.00	$ 2,906.25
Virtustream	30 A / 120 V Primary Power - USDC2 - Installation	DC-PWU2-31P-1T	$ 5,000.00	$ 4,650.00
Virtustream	30 A / 208 V Power Strip - USDC1	DC-PWU1-32S-1T	$ 1,375.00	$ 1,278.75
Virtustream	30 A / 208 V Power Strip - USDC2	DC-PWU2-32S-1T	$ 1,375.00	$ 1,278.75
Virtustream	30 A / 208 V Primary / Redundant Power - USDC1 - Installation	DC-PWU1-32R-1T	$ 4,583.34	$ 4,262.51
Virtustream	30 A / 208 V Primary / Redundant Power - USDC2 - Installation	DC-PWU2-32R-1T	$ 7,708.34	$ 7,168.76
Virtustream	30 A / 208 V Primary Power - USDC1 - Installation	DC-PWU1-32P-1T	$ 3,333.34	$ 3,100.01
Virtustream	30 A / 208 V Primary Power - USDC2 - Installation	DC-PWU2-32P-1T	$ 5,625.00	$ 5,231.25
Virtustream	Rack Installation - USDC1	DC-RKU1-RK-1T	$ 5,000.00	$ 4,650.00
Virtustream	Rack Installation - USDC2	DC-RKU2-RK-1T	$ 5,000.00	$ 4,650.00
Virtustream	20 A / 120 V Primary / Redundant Power - USDC1	DC-PWU1-21R-PF	$ 534.06	$ 496.68
Virtustream	20 A / 120 V Primary / Redundant Power - USDC2	DC-PWU2-21R-PF	$ 576.89	$ 536.51
Virtustream	20 A / 120 V Primary Power - USDC1	DC-PWU1-21P-PF	$ 418.43	$ 389.14
Virtustream	20 A / 120 V Primary Power - USDC2	DC-PWU2-21P-PF	$ 463.76	$ 431.30
Virtustream	20 A / 208 V Primary / Redundant Power - USDC1	DC-PWU1-22R-PF	$ 823.85	$ 766.18
Virtustream	20 A / 208 V Primary / Redundant Power - USDC2	DC-PWU2-22R-PF	$ 898.09	$ 835.22
Virtustream	20 A / 208 V Primary Power - USDC1	DC-PWU1-22P-PF	$ 684.96	$ 637.01
Virtustream	20 A / 208 V Primary Power - USDC2	DC-PWU2-22P-PF	$ 759.20	$ 706.06
Virtustream	30 A / 120 V Primary / Redundant Power - USDC1	DC-PWU1-31R-PF	$ 731.65	$ 680.43
Virtustream	30 A / 120 V Primary / Redundant Power - USDC2	DC-PWU2-31R-PF	$ 795.89	$ 740.18
Virtustream	30 A / 120 V Primary Power - USDC1	DC-PWU1-31P-PF	$ 627.63	$ 583.70
Virtustream	30 A / 120 V Primary Power - USDC2	DC-PWU2-31P-PF	$ 695.65	$ 646.95
Virtustream	30 A / 208 V Primary / Redundant Power - USDC1	DC-PWU1-32R-PF	$ 1,166.34	$ 1,084.70
Virtustream	30 A / 208 V Primary / Redundant Power - USDC2	DC-PWU2-32R-PF	$ 1,277.69	$ 1,188.25
Virtustream	30 A / 208 V Primary Power - USDC1	DC-PWU1-32P-PF	$ 1,027.45	$ 955.53
Virtustream	30 A / 208 V Primary Power - USDC2	DC-PWU2-32P-PF	$ 1,138.80	$ 1,059.08

Virtustream	Cloud Connect - HA (48 ports available)	DC-NWU3-XCH-HA	$ 531.25	$ 494.06
Virtustream	Cloud Connect - HA (48 ports available) - USDC1	DC-NWU1-XCH-HA	$ 531.25	$ 494.06
Virtustream	Cloud Connect - HA (48 ports available) - USDC2	DC-NWU2-XCH-HA	$ 531.25	$ 494.06
Virtustream	Cloud Connect - Standard (24 ports available)	DC-NWU3-XCS-STD	$ 250.00	$ 232.50
Virtustream	Cloud Connect - Standard (24 ports available) - USDC1	DC-NWU1-XCS-STD	$ 250.00	$ 232.50
Virtustream	Cloud Connect - Standard (24 ports available) - USDC2	DC-NWU2-XCS-STD	$ 250.00	$ 232.50
Virtustream	Coax DS-3 Cross Connect - USDC1	DC-NWU1-XCCX-MF	$ 175.00	$ 162.75
Virtustream	Coax DS-3 Cross Connect - USDC2	DC-NWU2-XCCX-MF	$ 175.00	$ 162.75
Virtustream	Copper Cross Connect - USDC1	DC-NWU1-XCC-MF	$ 187.50	$ 174.38
Virtustream	Copper Cross Connect - USDC2	DC-NWU2-XCC-MF	$ 187.50	$ 174.38
Virtustream	Fiber Cross Connect - USDC1	DC-NWU1-XCF-MF	$ 343.75	$ 319.69
Virtustream	Fiber Cross Connect - USDC2	DC-NWU2-XCF-MF	$ 343.75	$ 319.69
Virtustream	Hotel Rack (1U) - Managed Colo - USDC1	DC-RKU1-RK-HR	$ 125.00	$ 116.25
Virtustream	Hotel Rack (1U) - Managed Colo - USDC2	DC-RKU2-RK-HR	$ 125.00	$ 116.25
Virtustream	kW Primary Power Charge - USDC1	DC-PWU1-P-PF	$ 217.93	$ 202.67
Virtustream	kW Primary Power Charge - USDC2	DC-PWU2-P-PF	$ 217.93	$ 202.67
Virtustream	Remote Eyes & Hands (US) - Bronze	DC-SVC-REU-B	$ 300.00	$ 279.00
Virtustream	Remote Eyes & Hands (US) - Gold	DC-SVC-REU-G	$ 1,500.00	$ 1,395.00
Virtustream	Co-Innovation Roundtables - Ad Hoc (6 months)	CC-TAM-CIR-AH	$ 5,850.00	$ 5,265.00
Virtustream	Demand Management Meetings - Ad Hoc (3 months)	CC-TAM-DMM-AH	$ 3,217.50	$ 2,895.75
Virtustream	Executive Scorecards - Ad Hoc (3 months)	CC-TAM-ES-AH	$ 3,510.00	$ 3,159.00
Virtustream	IT Resource Forecast - Ad Hoc (3 months)	CC-TAM-ITRF-AH	$ 7,020.00	$ 6,318.00
Virtustream	Reporting and Business Review - Ad Hoc (1 month)	CC-TAM-RBR-AH	$ 4,638.75	$ 4,174.88
Virtustream	Resource and Performance - Ad Hoc (1 month)	CC-TAM-RP-AH	$ 4,203.75	$ 3,783.38
Virtustream	SLA Review - Ad Hoc (1 month)	CC-TAM-SLAR-AH	$ 1,755.00	$ 1,579.50
Virtustream	Weekly Status and Incident Reporting - Ad Hoc (1 month)	CC-TAM-WSIR-AH	$ 3,330.00	$ 2,997.00
Virtustream	Cloud Cover Setup	CC-SVC-ONCC-1T	$ 155.00	$ 139.50
Virtustream	Onshore SAP User, Security, and Change Management Process Setup	CC-SAP-ONUS-1T	$ 2,750.00	$ 2,475.00
Virtustream	Onshore Business Operating System & Database Support	CC-NS-ONDB-BUS	$ 550.00	$ 495.00
Virtustream	Onshore Business Operating System Support	CC-NS-ONOS-BUS	$ 312.50	$ 281.25
Virtustream	Onshore Business SAP Technical Support (Non-Prod/Basis)	CC-SAP-ONNH-BUS	$ 1,031.25	$ 928.13
Virtustream	Onshore Business SAP Technical Support (Prod/Basis)	CC-SAP-ONPH-BUS	$ 2,625.00	$ 2,362.50
Virtustream	Onshore Enterprise Operating System & Database Support	CC-NS-ONDB-ENT	$ 675.00	$ 607.50
Virtustream	Onshore Enterprise Operating System Support	CC-NS-ONOS-ENT	$ 406.25	$ 365.63
Virtustream	Onshore Enterprise SAP Technical Support (Non-Prod/Basis)	CC-SAP-ONNH-ENT	$ 2,625.00	$ 2,362.50
Virtustream	Onshore Enterprise SAP Technical Support (Prod/Basis)	CC-SAP-ONPH-ENT	$ 3,625.00	$ 3,262.50
Virtustream	Onshore Standard Operating System & Database Support	CC-NS-ONDB-STD	$ 168.75	$ 151.88
Virtustream	Onshore Standard Operating System Support	CC-NS-ONOS-STD	$ 93.75	$ 84.38
Virtustream	Onshore Standard SAP Technical Support (Non-Prod)	CC-SAP-ONNH-STD	$ 406.25	$ 365.63
Virtustream	Onshore Standard SAP Technical Support (Prod)	CC-SAP-ONPH-STD	$ 687.50	$ 618.75
Virtustream	Operational Integration - 1 Year	CC-TAM-OPIN-1Y	$ 1,950.00	$ 1,755.00
Virtustream	Reporting and Business Review - 1 Year	CC-TAM-RBR-1Y	$ 3,092.50	$ 2,783.25
Virtustream	Resource and Performance - 1 Year	CC-TAM-RP-1Y	$ 2,802.50	$ 2,522.25
Virtustream	SLA Review - 1 Year	CC-TAM-SLAR-1Y	$ 1,170.00	$ 1,053.00
Virtustream	Technical Account Management (TAM) - Gold	CC-TAM-TAM-GOLD	$ 12,000.00	$ 10,800.00
Virtustream	Technical Account Management (TAM) - Silver	CC-TAM-TAM-SILV	$ 6,000.00	$ 5,400.00
Virtustream	Technical Account Manager (TAM) - Platinum	CC-TAM-TAM-PLAT	$ 24,000.00	$ 21,600.00
Virtustream	Technical Account Management (TAM) - Per Instance	CC-TAM-TAM-INST	$ 400.00	$ 360.00
Virtustream	Weekly Status and Incident Reporting - 1 Year	CC-TAM-WSIR-1Y	$ 2,220.00	$ 1,998.00

VMware	U.S. Federal Socialcast Configuration and Integration Design - On Premise Platform	CON-HZ-SC-CIDOP-FF	$ 7,500.00	$ 7,329.97
VMware	U.S. Federal Socialcast Assigned Client Account Representative	CON-HZ-SC-ACAR-FF	$ 30,000.00	$ 29,319.90
VMware	U.S. Federal Socialcast Reach System Integration	CON-HZ-SC-RSI-FF	$ 3,500.00	$ 3,420.65
VMware	U.S. Federal Socialcast Single Sign On Configuration	CON-HZ-SC-SSOC-FF	$ 5,000.00	$ 4,886.65
VMware	U.S. Federal Socialcast Custom Theme Integration	CON-HZ-SC-CTI-FF	$ 3,500.00	$ 3,420.65
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.8] - Open Enrollment	EDU-SRMICM58-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.8] - Onsite	EDU-SRMICM58-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.8] - Extra Person	EDU-SRMICM58-XP-F	$ 1,376.00	$ 1,344.81
VMware	U.S. Federal VMware vSphere: Design Workshop [V5.5] - Open Enrollment	EDU-VSDW55-OE-F	$ 2,695.00	$ 2,633.90
VMware	U.S. Federal VMware vSphere: Design Workshop [V5.5] - On Site	EDU-VSDW55-OS-F	$ 22,650.00	$ 22,136.52
VMware	U.S. Federal VMware vSphere: Design Workshop [V5.5] - Extra Person	EDU-VSDW55-XP-F	$ 2,265.00	$ 2,213.65
VMware	U.S. Federal VMware SDDC Intensive Workshop [V3.0] - Open Enrollment	EDU-SDDC3-OE-F	$ 6,265.00	$ 6,122.97
VMware	U.S. Federal VMware SDDC Intensive Workshop [V3.0] - On Site	EDU-SDDC3-OS-F	$ 52,850.00	$ 51,651.89
VMware	U.S. Federal VMware SDDC Intensive Workshop [V3.0] - Extra Person	EDU-SDDC3-XP-F	$ 5,285.00	$ 5,165.19
VMware	VMware NSX for Internetworking Experts Fast Track [V6.0] - Open Enrollment	EDU-NSXFT6-OE-F	$ 6,265.00	$ 6,122.97
VMware	VMware NSX for Internetworking Experts Fast Track [V6.0] - On Site	EDU-NSXFT6-OS-F	$ 52,850.00	$ 51,651.89
VMware	VMware NSX for Internetworking Experts Fast Track [V6.0] - Extra Person	EDU-NSXFT6-XP-F	$ 5,285.00	$ 5,165.19
VMware	VMware Mirage: Install Configure Manage [V5.0] - Open Enrollment	EDU-MICM5-OE-F	$ 2,250.00	$ 2,198.99
VMware	VMware Mirage: Install Configure Manage [V5.0] - Onsite	EDU-MICM5-OS-F	$ 18,750.00	$ 18,324.94
VMware	VMware Mirage: Install Configure Manage [V5.0] - Extra Person	EDU-MICM5-XP-F	$ 1,875.00	$ 1,832.49
VMware	U.S. Federal VMware vSphere: Optimize and Scale [V6.0] - Open Enrollment	EDU-VSOS6-OE-F	$ 4,475.00	$ 4,373.55
VMware	U.S. Federal VMware vSphere: Optimize and Scale [V6.0] - On Site	EDU-VSOS6-OS-F	$ 37,750.00	$ 36,894.21
VMware	U.S. Federal VMware vSphere: Install Configure Manage [V6.0] - Open Enrollment	EDU-VSICM6-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware vSphere: Install Configure Manage [V6.0] - On Site	EDU-VSICM6-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware vSphere: Install Configure Manage [V 6.0] - Extra Person	EDU-VSICM6-XP-F	$ 3,440.00	$ 3,362.02
VMware	U.S. Federal VMware vFabric tcServer Jumpstart	CON-S2-TCSERVER-JS-F	$ 5,495.00	$ 5,370.43
VMware	U.S. Federal VMware vFabric Hyperic Jumpstart	CON-S2-HYPERIC-JS-F	$ 8,195.00	$ 8,009.22
VMware	U.S. Federal VMware vFabric Hyperic and tcServer Jumpstart	CON-S2-HYPR-TCS-JS-F	$ 12,795.00	$ 12,504.94
VMware	U.S. Federal VMware vFabric PaaS Planning Service	CON-S2-PAAS-PLN-F	$ 25,595.00	$ 25,014.76
VMware	U.S. Federal GemFire Architectural Accelerator Service	CON-S2-GEMFIRE-ACL-F	$ 25,595.00	$ 25,014.76
VMware	U.S. Federal VMware Hyperic and vCenter Operations Enterprise Standalone Jumpstart	CON-S2-HYPR-VCO-JS-F	$ 18,995.00	$ 18,564.38
VMware	U.S. Federal VMware Advanced Technical Account Manager for NSX	TAM-NSX-ADV-F	$ 174,995.00	$ 171,027.86
VMware	U.S. Federal VMware Basic Technical Account Manager for NSX	TAM-NSX-BSC-F	$ 89,995.00	$ 87,954.81
VMware	U.S. Federal VMware Dedicated Technical Account Manager for NSX	TAM-NSX-DED-F	$ 324,995.00	$ 317,627.36
VMware	U.S. Federal VMware Infrastructure Health Check	CON-ESX-HC-AW-F	$ 9,000.00	$ 8,795.97
VMware	U.S. Federal VMware Physical to Virtual Migration Jumpstart	CON-ESX-P2V-F	$ 6,000.00	$ 5,863.98
VMware	U.S. Federal VMware Infrastructure with vCenter Lab Manager Jumpstart	CON-ESXVC-LM-JS-F	$ 13,500.00	$ 13,193.95
VMware	U.S. Federal VMware Infrastructure with Physical to Virtual Migration Jumpstart	CON-ESXVCP2V-JS-F	$ 13,500.00	$ 13,193.95
VMware	U.S. Federal VMware Infrastructure Jumpstart with vCenter Stage Manager	CON-ESXVCSM-JS-F	$ 13,500.00	$ 13,193.95
VMware	U.S. Federal Consulting Expense Reimbursement (T&E)	CON-EXP-F	$ 2,200.00	$ 2,150.13
VMware	U.S. Federal Vmware 1-day Jumpstart Add-on	CON-GC-JSAO-F	$ 3,000.00	$ 2,931.99
VMware	U.S. Federal VMware vCenter Lab Manager Jumpstart	CON-LM-JS-F	$ 6,000.00	$ 5,863.98
VMware	U.S. Federal VMware ThinApp Application Virtualization Jumpstart	CON-THIN-JS-F	$ 6,000.00	$ 5,863.98
VMware	U.S. Federal VMware View Manager Jumpstart	CON-VIEW-JS-F	$ 9,000.00	$ 8,795.97
VMware	U.S. Federal UPGRADE: VMware Technical Account Manager Tier 1 to Tier 2 per Month	TAM-UG-TIER-1-2-F	$ 7,500.00	$ 7,329.97
VMware	U.S. Federal UPGRADE: VMware Technical Account Manager Tier 1 to Tier 3 per Month	TAM-UG-TIER-1-3-F	$ 19,583.33	$ 19,139.38
VMware	U.S. Federal UPGRADE: VMware Technical Account Manager Tier 2 to Tier 3 per Month	TAM-UG-TIER-2-3-F	$ 12,083.33	$ 11,809.40
VMware	U.S. Federal VMware View 4: Install Configure Manage - Open Enrollment	EDU-VMVICM-OE-F	$ 2,475.00	$ 2,418.89
VMware	U.S. Federal VMware View 4: Install Configure Manage - Onsite	EDU-VMVICM-OS-F	$ 20,625.00	$ 20,157.43

VMware	U.S. Federal VMware View 4: Install Configure Manage - Extra Person	EDU-VMVICM-XP-F	$ 2,063.00	$ 2,016.23
VMware	U.S. Federal VMware vSphere 4: Manage for Performance - Extra Person	EDU-VS4DMP-XP-F	$ 2,265.00	$ 2,213.65
VMware	U.S. Federal VMware vSphere 4: Design Workshop - Open Enrollment	EDU-VS4DW-OE-F	$ 2,475.00	$ 2,418.89
VMware	U.S. Federal VMware vSphere 4: Design Workshop - On Site	EDU-VS4DW-OS-F	$ 20,625.00	$ 20,157.43
VMware	U.S. Federal VMware vSphere 4: Design Workshop - Extra Person	EDU-VS4DW-XP-F	$ 2,063.00	$ 2,016.23
VMware	U.S. Federal VMware vSphere 4: Manage Availability - Open Enrollment	EDU-VS4MA-OE-F	$ 825.00	$ 806.30
VMware	U.S. Federal VMware vSphere 4: Manage Availability - On Site	EDU-VS4MA-OS-F	$ 6,875.00	$ 6,719.14
VMware	U.S. Federal VMware vSphere 4: Manage Availability - Extra Person	EDU-VS4MA-XP-F	$ 688.00	$ 672.40
VMware	U.S. Federal VMware vSphere 4: Manage and Design for Security - Open Enrollment	EDU-VS4MDS-OE-F	$ 2,695.00	$ 2,633.90
VMware	U.S. Federal VMware vSphere 4: Manage and Design for Security - On Site	EDU-VS4MDS-OS-F	$ 22,650.00	$ 22,136.52
VMware	U.S. Federal VMware vSphere 4: Manage and Design for Security - Extra Person	EDU-VS4MDS-XP-F	$ 2,265.00	$ 2,213.65
VMware	U.S. Federal VMware vSphere 4: Manage for Performance - Open Enrollment	EDU-VS4MP-OE-F	$ 2,695.00	$ 2,633.90
VMware	U.S. Federal VMware vSphere 4: Manage for Performance - On Site	EDU-VS4MP-OS-F	$ 22,650.00	$ 22,136.52
VMware	U.S. Federal VMware vSphere 4: Manage Scalability - Open Enrollment	EDU-VS4MS-OE-F	$ 825.00	$ 806.30
VMware	U.S. Federal VMware vSphere 4: Manage Scalability - On Site	EDU-VS4MS-OS-F	$ 6,875.00	$ 6,719.14
VMware	U.S. Federal VMware vSphere 4: Manage Scalability - Extra Person	EDU-VS4MS-XP-F	$ 688.00	$ 672.40
VMware	U.S. Federal VMware vSphere 4: Skills for Operators - Open Enrollment	EDU-VS4SO-OE-F	$ 1,645.00	$ 1,607.71
VMware	U.S. Federal VMware vSphere 4: Skills for Operators - Onsite	EDU-VS4SO-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vSphere 4: Skills for Operators- Extra Person	EDU-VS4SO-XP-F	$ 1,375.00	$ 1,343.83
VMware	U.S. Federal VMware vSphere 4: Troubleshooting - Open Enrollment	EDU-VS4TR-OE-F	$ 3,595.00	$ 3,513.50
VMware	U.S. Federal VMware vSphere 4: Troubleshooting - On Site	EDU-VS4TR-OS-F	$ 30,200.00	$ 29,515.37
VMware	U.S. Federal VMware vSphere 4: Troubleshooting - Extra Person	EDU-VS4TR-XP-F	$ 3,020.00	$ 2,951.54
VMware	U.S. Federal VMware vSphere 4: What's New - Open Enrollment	EDU-VS4WN-OE-F	$ 1,645.00	$ 1,607.71
VMware	U.S. Federal VMware vSphere 4: What's New-On Site	EDU-VS4WN-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vSphere 4: What's New-Extra Person	EDU-VS4WN-XP-F	$ 1,375.00	$ 1,343.83
VMware	U.S. Federal Vmware VS4: Install Configure Manage V40b - Extra Person	EDU-VS41ICM-XP-F	$ 3,438.00	$ 3,360.06
VMware	U.S. Federal VMware View: Desktop Fast Track [V4.5] - Open Enrollment	EDU-VDFT45-OE-F	$ 4,945.00	$ 4,832.90
VMware	U.S. Federal VMware View: Desktop Fast Track [V4.5] - Onsite	EDU-VDFT45-OS-F	$ 41,580.00	$ 40,637.38
VMware	U.S. Federal VMware View: Desktop Fast Track [V4.5] - Extra Person	EDU-VDFT45-XP-F	$ 4,158.00	$ 4,063.74
VMware	U.S. Federal VMware vSphere: Advanced Fast Track [V4.x] - Open Enrollment	EDU-VS4AFT-OE-F	$ 5,600.00	$ 5,473.05
VMware	U.S. Federal VMware vSphere: Advanced Fast Track [V4.x] - Onsite	EDU-VS4AFT-OS-F	$ 47,190.00	$ 46,120.20
VMware	U.S. Federal VMware vSphere: Advanced Fast Track [V4.x] - Extra Person	EDU-VS4AFT-XP-F	$ 4,719.00	$ 4,612.02
VMware	U.S. Federal VMware vSphere: Automation Fast Track [V4.1] - Open Enrollment	EDU-VS41AUFT-OE-F	$ 5,165.00	$ 5,047.91
VMware	U.S. Federal VMware vSphere: Automation Fast Track [V4.1] - Onsite	EDU-VS41AUFT-OS-F	$ 43,450.00	$ 42,464.99
VMware	U.S. Federal VMware vSphere: Automation Fast Track [V4.1] - Extra Person	EDU-VS41AUFT-XP-F	$ 4,345.00	$ 4,246.50
VMware	U.S. Federal VMware vSphere: Install Configure Manage [V5.0] - On Site	EDU-VSICM5-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware vSphere: Install Configure Manage [V5.0] - Extra Person	EDU-VSICM5-XP-F	$ 3,438.00	$ 3,360.06
VMware	U.S. Federal VMware vSphere: What's New [V5.0] - Open Enrollment	EDU-VSWN5-OE-F	$ 1,645.00	$ 1,607.71
VMware	U.S. Federal VMware vSphere: What's New [V5.0] - On Site	EDU-VSWN5-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vSphere: What's New [V5.0] - Extra Person	EDU-VSWN5-XP-F	$ 1,375.00	$ 1,343.83
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.0] - Open Enrollment	EDU-VCSRM5-OE-F	$ 1,795.00	$ 1,754.31
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.0] - On Site	EDU-VCSRM5-OS-F	$ 15,100.00	$ 14,757.68
VMware	U.S. Federal VMware vCenter Site Recovery Manager: Install Configure Manage [V5.0] - Extra Person	EDU-VCSRM5-XP-F	$ 1,510.00	$ 1,475.77
VMware	U.S. Federal VMware vSphere: Fast Track [V5.0] - On Site	EDU-VSFT5-OS-F	$ 55,000.00	$ 53,753.15
VMware	U.S. Federal VMware vSphere: Fast Track [V5.0] - Extra Person	EDU-VSFT5-XP-F	$ 5,500.00	$ 5,375.31
VMware	U.S. Federal VMware vCloud: Deploy and Manage the VMware Cloud [V1.5] - Open Enrollment	EDU-VC15DM-OE-F	$ 3,595.00	$ 3,513.50
VMware	U.S. Federal VMware vCloud: Deploy and Manage the VMware Cloud [V1.5] - On Site	EDU-VC15DM-OS-F	$ 30,200.00	$ 29,515.37
VMware	U.S. Federal VMware vCloud: Deploy and Manage the VMware Cloud [V1.5] - Extra Person	EDU-VC15DM-XP-F	$ 3,020.00	$ 2,951.54
VMware	U.S. Federal VMware vSphere: Optimize and Scale [V5.0] - Open Enrollment	EDU-VSOS5-OE-F	$ 4,495.00	$ 4,393.10

VMware	U.S. Federal VMware vSphere: Optimize and Scale [V5.0] - On Site	EDU-VSOS5-OS-F	$ 37,750.00	$ 36,894.21
VMware	U.S. Federal VMware vSphere: Optimize and Scale [V5.0] - Extra Person	EDU-VSOS5-XP-F	$ 3,775.00	$ 3,689.42
VMware	U.S. Federal VMware vCenter Operations Manager:Analyze and Predict [V5.0] - Open Enrollment	EDU-VCOAP5-OE-F	$ 1,645.00	$ 1,607.71
VMware	U.S. Federal VMware vCenter Operations Manager:Analyze and Predict [V5.0] - On Site	EDU-VCOAP5-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vCenter Operations Manager:Analyze and Predict [V5.0] - Extra Person	EDU-VCOAP5-XP-F	$ 1,375.00	$ 1,343.83
VMware	VMware View: Design Best Practices [V5.1] - Open Enrollment	EDU-VDBP51-OE-F	$ 2,695.00	$ 2,633.90
VMware	VMware View: Design Best Practices [V5.1] - On Site	EDU-VDBP51-OS-F	$ 22,650.00	$ 22,136.52
VMware	VMware View: Design Best Practices [V5.1] - Extra Person	EDU-VDBP51-XP-F	$ 2,265.00	$ 2,213.65
VMware	U.S. Federal VMware View: Desktop Fast Track [V5.0] - On Site	EDU-VDFT5-OS-F	$ 37,818.00	$ 36,960.66
VMware	U.S. Federal VMware View: Desktop Fast Track [V5.0] - Extra Person	EDU-VDFT5-XP-F	$ 3,782.00	$ 3,696.26
VMware	VMware vCloud: Design Best Practices [V1.5] - Open Enrollment	EDU-VCDBP15-OE-F	$ 2,695.00	$ 2,633.90
VMware	VMware vCloud: Design Best Practices [V1.5] - On Site	EDU-VCDBP15-OS-F	$ 22,650.00	$ 22,136.52
VMware	VMware vCloud: Design Best Practices [V1.5] - Extra Person	EDU-VCDBP15-XP-F	$ 2,265.00	$ 2,213.65
VMware	U.S. Federal VMware vFabric TAM	CON-S2-TAM-TIER-1-F	$ 64,995.00	$ 63,521.56
VMware	U.S. Federal VMware vFabric Strategic TAM	CON-S2-TAM-TIER-2-F	$ 154,995.00	$ 151,481.26
VMware	U.S. Federal VMware vFabric Dedicated Strategic TAM	CON-S2-TAM-TIER-3-F	$ 299,995.00	$ 293,194.11
VMware	U.S. Federal Spring Web [V3.1] - Onsite	EDU-S2-PRIV-SW31-OS-F	$ 2,025.00	$ 2,025.00
VMware	Groovy and Grails [V2.0] - Open Enrollment	EDU-S2-GG20-OE-F	$ 2,700.00	$ 2,638.79
VMware	Groovy and Grails [V2.0] - Onsite	EDU-S2-PRIV-GG20-OS-F	$ 2,025.00	$ 1,979.09
VMware	VMware vCloud Networking and Security for vSphere Professionals [V5.1] - Open Enrollment	EDU-VCNS51-OE-F	$ 2,695.00	$ 2,633.90
VMware	VMware vCloud Networking and Security for vSphere Professionals [V5.1] - On Site	EDU-VCNS51-OS-F	$ 22,650.00	$ 22,136.52
VMware	VMware vCloud Networking and Security for vSphere Professionals [V5.1] - Extra Person	EDU-VCNS51-XP-F	$ 2,265.00	$ 2,213.65
VMware	VMware vCloud Director: Organization Administration [V5.5] - Open Enrollment	EDU-VCOA55-OE-F	$ 1,645.00	$ 1,607.71
VMware	VMware vCloud Director: Organization Administration [V5.5] - On Site	EDU-VCOA55-OS-F	$ 13,750.00	$ 13,438.29
VMware	VMware vCloud Director: Organization Administration [V5.5] - Extra Person	EDU-VCOA55-XP-F	$ 1,375.00	$ 1,343.83
VMware	VMware vCloud Director: Install Configure Manage [V5.5] - Open Enrollment	EDU-VCICM55-OE-F	$ 2,475.00	$ 2,418.89
VMware	VMware vCloud Director: Install Configure Manage [V5.5] - On Site	EDU-VCICM55-OS-F	$ 20,625.00	$ 20,157.43
VMware	VMware vCloud Director: Install Configure Manage [V5.5] - Extra Person	EDU-VCICM55-XP-F	$ 2,063.00	$ 2,016.23
VMware	U.S. Federal VMware View: Install Configure Manage [V5.0] - Open Enrollment	EDU-VICM5-OE-F	$ 3,295.00	$ 3,220.30
VMware	U.S. Federal VMware View: Install Configure Manage [V5.0] - On Site	EDU-VICM5-OS-F	$ 27,500.00	$ 26,876.57
VMware	U.S. Federal VMware vSphere: What's New [V5.x to V6.0] - Open Enrollment	EDU-VSWN6-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal VMware vSphere: What's New [V5.x to V6.0] - On Site	EDU-VSWN6-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vSphere: What's New [V5.x to V6.0] - Extra Person	EDU-VSWN6-XP-F	$ 1,376.00	$ 1,344.81
VMware	U.S. Federal VMware Mirage [V5.0] and Horizon with View [V6.0]: Fast Track - Open Enrollment	EDU-M5H6FT-OE-F	$ 6,265.00	$ 6,122.97
VMware	U.S. Federal VMware Mirage [V5.0] and Horizon with View [V6.0]: Fast Track - On Site	EDU-M5H6FT-OS-F	$ 52,850.00	$ 51,651.89
VMware	U.S. Federal VMware Mirage [V5.0] and Horizon with View [V6.0]: Fast Track - Extra Person	EDU-M5H6FT-XP-F	$ 5,285.00	$ 5,165.19
VMware	U.S. Federal VMware IT Business Management: Costing and Implementation [V8.0] - Open Enrollment	EDU-ITBM8-OE-F	$ 3,300.00	$ 3,225.19
VMware	U.S. Federal VMware IT Business Management: Costing and Implementation [V8.0] - On Site	EDU-ITBM8-OS-F	$ 27,500.00	$ 26,876.57
VMware	U.S. Federal VMware IT Business Management: Costing and Implementation [V8.0] - Extra Person	EDU-ITBM8-XP-F	$ 2,752.00	$ 2,689.61
VMware	U.S. Federal VMware vRealize Operations Manager: Install Configure Manage [V6.0] - On Site	EDU-VCOPICM6-OS-F	$ 37,750.00	$ 36,894.21
VMware	U.S. Federal VMware vRealize Operations Manager: Install Configure Manage [V6.0] - Open Enrollment	EDU-VCOPICM6-OE-F	$ 4,495.00	$ 4,393.10
VMware	U.S. Federal VMware vRealize Operations Manager: Install Configure Manage [V6.0] - Extra Person	EDU-VCOPICM6-XP-F	$ 3,775.00	$ 3,689.42
VMware	U.S. Federal VMware Horizon 6 Production Pilot	CON-HZN-PILOT-F	$ 74,380.00	$ 72,693.80
VMware	U.S. Federal AirWatch Enterprise Mobility: Bootcamp - Open Enrollment	EDU-AW-BTCMP-OE-F	$ 2,800.00	$ 2,736.52
VMware	U.S. Federal AirWatch Enterprise Mobility: Bootcamp - On Site	EDU-AW-BTCMP-OS-F	$ 16,800.00	$ 16,419.14
VMware	U.S. Federal AirWatch Enterprise Mobility: Bootcamp - Extra Person	EDU-AW-BTCMP-XP-F	$ 2,240.00	$ 2,189.22
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Deploy Integrated Solutions - Open Enrollment	EDU-AW-INTEG-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Deploy Integrated Solutions - On Site	EDU-AW-INTEG-OS-F	$ 9,900.00	$ 9,675.57
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Deploy Integrated Solutions - Extra Person	EDU-AW-INTEG-XP-F	$ 1,320.00	$ 1,290.08

VMware	U.S. Federal AirWatch Enterprise Mobility: K12 Education - Open Enrollment	EDU-AW-K12-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal AirWatch Enterprise Mobility: K12 Education - On Site	EDU-AW-K12-OS-F	$ 9,900.00	$ 9,675.57
VMware	U.S. Federal AirWatch Enterprise Mobility: K12 Education - Extra Person*	EDU-AW-K12-XP-F	$ 1,320.00	$ 1,290.08
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Manage - Open Enrollment	EDU-AW-MANAGE-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Manage - On Site	EDU-AW-MANAGE-OS-F	$ 9,900.00	$ 9,675.57
VMware	U.S. Federal AirWatch Enterprise Mobility: Configure and Manage - Extra Person	EDU-AW-MANAGE-XP-F	$ 1,320.00	$ 1,290.08
VMware	U.S. Federal AirWatch by VMware Enterprise Mobility: Install and Deploy On-Premise Solutions - Open Enrollment	EDU-AW-ONPREM-OE-F	$ 895.00	$ 874.71
VMware	U.S. Federal AirWatch by VMware Enterprise Mobility: Install and Deploy On-Premise Solutions - On Site Dedicated	EDU-AW-ONPREM-OS-F	$ 5,370.00	$ 5,248.26
VMware	U.S. Federal AirWatch by VMware Enterprise Mobility: Install and Deploy On-Premise Solutionsy - Extra Person	EDU-AW-ONPREM-XP-F	$ 716.00	$ 699.77
VMware	U.S. Federal VMware vSphere: Bootcamp [V6] - Open Enrollment	EDU-BOOT6-OE-F	$ 7,145.00	$ 6,983.02
VMware	U.S. Federal VMware Horizon: Design and Deploy [v6.0] - Open Enrollment	EDU-HDD6-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware Horizon: Design and Deploy [v6.0] - On Site	EDU-HDD6-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware Horizon: Design and Deploy [v6.0] - Extra Person	EDU-HDD6-XP-F	$ 3,440.00	$ 3,362.02
VMware	U.S. Federal Horizon (with View): Install Configure Manage [V6.2] - Open Enrollment	EDU-HICM62-OE-F	$ 3,300.00	$ 3,225.19
VMware	U.S. Federal Horizon (with View): Install Configure Manage [V6.2] - On Site	EDU-HICM62-OS-F	$ 27,500.00	$ 26,876.57
VMware	U.S. Federal Horizon (with View): Install Configure Manage [V6.2] - Extra Person	EDU-HICM62-XP-F	$ 2,752.00	$ 2,689.61
VMware	U.S. Federal VMware NSX for Internetworking Experts Fast Track [V6.1] - Open Enrollment	EDU-NSXFT61-OE-F	$ 6,265.00	$ 6,122.97
VMware	U.S. Federal VMware NSX for Internetworking Experts Fast Track [V6.1] - On Site	EDU-NSXFT61-OS-F	$ 52,850.00	$ 51,651.89
VMware	U.S. Federal VMware NSX for Internetworking Experts Fast Track [V6.1] - Extra Person	EDU-NSXFT61-XP-F	$ 5,285.00	$ 5,165.19
VMware	U.S. Federal VMware NSX: Install Configure Manage [V6.2] - Open Enrollment	EDU-NSXICM62-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware NSX: Install Configure Manage [V6.2] - On Site	EDU-NSXICM62-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware NSX: Install Configure Manage [V6.2] - Extra Person	EDU-NSXICM62-XP-F	$ 3,440.00	$ 3,362.02
VMware	U.S. Federal VMware Site Recovery Manager: Install Configure Manage [V6.1] - Open Enrollment	EDU-SRMICM61-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. FederalVMware Site Recovery Manager: Install Configure Manage [V6.1] - On Site	EDU-SRMICM61-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware Site Recovery Manager: Install Configure Manage [V6.1] - Extra Person	EDU-SRMICM61-XP-F	$ 1,376.00	$ 1,344.81
VMware	U.S. Federal VMware Cloud Automation: Design and Deploy Fast Track [v6.0] - Open Enrollment	EDU-VCADDFT6-OE-F	$ 6,265.00	$ 6,122.97
VMware	U.S. Federal VMware Cloud Automation: Design and Deploy Fast Track [v6.0] - On Site	EDU-VCADDFT6-OS-F	$ 52,850.00	$ 51,651.89
VMware	U.S. Federal VMware Cloud Automation: Design and Deploy Fast Track [v6.0] - Extra Person	EDU-VCADDFT6-XP-F	$ 5,285.00	$ 5,165.19
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - On Premise (Includes Production Sup	EDU-VOSTFT6-OE-F	$ 6,265.00	$ 5,996.73
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - Shared Cloud (Includes SaaS Producti	EDU-VOSTFT6-OS-F	$ 52,850.00	$ 50,586.90
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - Shared Cloud (Includes SaaS Produ	EDU-VOSTFT6-XP-F	$ 5,285.00	$ 5,058.69
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V6.2] - Open Enrollment	EDU-VRAICM62-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V6.2] - On Site	EDU-VRAICM62-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V6.2] - Extra Person	EDU-VRAICM62-XP-F	$ 3,440.00	$ 3,362.02
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V7.x] - Open Enrollment	EDU-VRAICM7-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V7.x] - On Site	EDU-VRAICM7-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware vRealize Automation: Install Configure Manage [V7.x] - Extra Person	EDU-VRAICM7-XP-F	$ 3,440.00	$ 3,362.02
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Product	EDU-VROPSOP60-OE-F	$ 1,650.00	$ 1,579.35
VMware	U.S. Federal VMware Virtual SAN: Deploy and Manage [V6] - Open Enrollment	EDU-VSANDM6-OE-F	$ 2,475.00	$ 2,418.89
VMware	U.S. Federal VMware Virtual SAN: Deploy and Manage [V6] - On Site	EDU-VSANDM6-OS-F	$ 20,625.00	$ 20,157.43
VMware	U.S. Federal VMware Virtual SAN: Deploy and Manage [V6] - Extra Person	EDU-VSANDM6-XP-F	$ 2,064.00	$ 2,017.21
VMware	U.S. Federal VMware vSphere Bootcamp - Onsite	EDU-VSBC-OS-F	$ 54,600.00	$ 53,362.22
VMware	U.S. Federal VMware vSphere Bootcamp - Extra Student	EDU-VSBC-XP-F	$ 5,460.00	$ 5,336.22
VMware	U.S. Federal VMware vSphere: Design and Deploy Fast Track [V6] - Open Enrollment	EDU-VSDDFT6-OE-F	$ 6,265.00	$ 6,122.97
VMware	U.S. Federal VMware vSphere: Design and Deploy Fast Track [V6] - On Site	EDU-VSDDFT6-OS-F	$ 52,850.00	$ 51,651.89
VMware	U.S. Federal VMware vSphere: Design and Deploy Fast Track [V6] - Extra Person	EDU-VSDDFT6-XP-F	$ 5,285.00	$ 5,165.19
VMware	U.S. Federal VMware vSphere: Skills for Operators - Open Enrollment	EDU-VSO6-OE-F	$ 1,650.00	$ 1,612.59
VMware	U.S. Federal VMware vSphere: Skills for Operators - On Site	EDU-VSO6-OS-F	$ 13,750.00	$ 13,438.29
VMware	U.S. Federal VMware vSphere: Skills for Operators - Extra Person	EDU-VSO6-XP-F	$ 1,376.00	$ 1,344.81

VMware	U.S. Federal VMware vSphere: Troubleshooting Workshop [V6] - Open Enrollment	EDU-VTSW6-OE-F	$ 4,125.00	$ 4,031.49
VMware	U.S. Federal VMware vSphere: Troubleshooting Workshop [V6] - On Site	EDU-VTSW6-OS-F	$ 34,375.00	$ 33,595.72
VMware	U.S. Federal VMware vSphere: Troubleshooting Workshop [V6] - Extra Person	EDU-VTSW6-XP-F	$ 755.00	$ 737.88
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-CLD-D-2G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-CLD-D-2P-F	$ 38.00	$ 36.37
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-CLD-D-3G-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-CLD-D-3P-F	$ 53.00	$ 50.73
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-CLD-D-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-CLD-D-P-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-DLD-D-2G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-DLD-D-2P-F	$ 38.00	$ 36.37
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-DLD-D-3G-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-APP-DLD-D-3P-F	$ 53.00	$ 50.73
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-DLD-D-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-APP-DLD-D-P-F	$ 20.00	$ 19.14
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Teacher Tools: 1 Device for 1 year	V-APP-PLL-D-F	$ 25.00	$ 23.93
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Teacher Tools: 1 Device for 3 years	V-APP-SSS-D-3G-F	$ 13.20	$ 12.63
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-APP-SSS-D-3P-F	$ 15.84	$ 15.16
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Teacher Tools: 1 Device for 1 year	V-APP-SSS-D-G-F	$ 5.00	$ 4.79
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Teacher Tools: 1 Device for 3 years	V-APP-SSS-D-P-F	$ 6.00	$ 5.74
VMware	TPP L3 U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extensi	V-BMS-CLD-D-2G-F	$ 143.00	$ 136.88
VMware	U.S. Federal VMware AirWatch Blue Management Suite On-Premise - Includes 3 days On-Site	V-BMS-CLD-D-2P-F	$ 151.00	$ 144.53
VMware	TPP L4 U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extensi	V-BMS-CLD-D-3G-F	$ 201.00	$ 192.39
VMware	U.S. Federal VMware AirWatch Blue Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-BMS-CLD-D-3P-F	$ 212.00	$ 202.92
VMware	TPP L2 U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extensi	V-BMS-CLD-D-G-F	$ 76.00	$ 72.75
VMware	TPP L5 U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extensi	V-BMS-CLD-D-P-F	$ 80.00	$ 76.57
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-CLD-U-2G-F	$ 286.00	$ 273.75
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-BMS-CLD-U-2P-F	$ 299.00	$ 286.20
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-BMS-CLD-U-3G-F	$ 402.00	$ 384.79
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-CLD-U-3P-F	$ 420.00	$ 402.02
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-CLD-U-G-F	$ 152.00	$ 145.49
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-BMS-CLD-U-P-F	$ 159.00	$ 152.19
VMware	U.S. Federal VMware AirWatch Green Management Suite On-Premise - Includes 2 days On-Site	V-BMS-DLD-D-2G-F	$ 166.00	$ 158.89
VMware	U.S. Federal VMware AirWatch Orange Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-BMS-DLD-D-2P-F	$ 173.00	$ 165.59
VMware	U.S. Federal VMware AirWatch Green Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-BMS-DLD-D-3G-F	$ 233.00	$ 223.02
VMware	U.S. Federal VMware AirWatch On-Premise Weekend Upgrades and Off-Hours Requiring Same Region One Time Fee	V-BMS-DLD-D-3P-F	$ 243.00	$ 232.59
VMware	U.S. Federal VMware AirWatch End User On-Boarding Video	V-BMS-DLD-D-G-F	$ 88.00	$ 84.23
VMware	U.S. Federal VMware AirWatch Orange Management Suite On-Premise - Includes 2 days On-Site	V-BMS-DLD-D-P-F	$ 92.00	$ 88.06
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-DLD-U-2G-F	$ 331.00	$ 316.83
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscrip	V-BMS-DLD-U-2P-F	$ 345.00	$ 330.23
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscrip	V-BMS-DLD-U-3G-F	$ 465.00	$ 445.09
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-BMS-DLD-U-3P-F	$ 484.00	$ 463.27
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-DLD-U-G-F	$ 176.00	$ 168.46
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscrip	V-BMS-DLD-U-P-F	$ 183.00	$ 175.16
VMware	U.S. Federal VMware AirWatch SaaS SEG and MAG Upgrade	V-BMS-OPL-D-2G-F	$ 121.00	$ 115.82
VMware	U.S. Federal VMware AirWatch Yellow Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-BMS-OPL-D-2P-F	$ 128.00	$ 122.52
VMware	U.S. Federal VMware AirWatch SaaS SEG and MAG Weekend and Same Region Off-Hours Upgrade	V-BMS-OPL-D-3G-F	$ 169.00	$ 161.76
VMware	U.S. Federal VMware AirWatch Green Management Suite Perpetual: 1 Device	V-BMS-OPL-D-3P-F	$ 180.00	$ 172.29
VMware	U.S. Federal VMware AirWatch SocialCast Dedicated SaaS Setup Fee One Time Fee	V-BMS-OPL-D-G-F	$ 64.00	$ 61.26

VMware	U.S. Federal VMware AirWatch Yellow Management Suite On-Premise - Includes 3 days On-Site	V-BMS-OPL-D-P-F	$ 68.00	$ 65.09
VMware	TPP L3 Upgrade: U S. Federal VMware vRealize Automation 7 Advanced to U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-BMS-PLL-D-F	$ 90.00	$ 86.15
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Green Management Suite: 1 Device for 1 year	V-BMS-PLL-U-F	$ 180.00	$ 172.29
VMware	U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extension (25	V-BMS-SSS-D-3G-F	$ 50.16	$ 48.01
VMware	TPP L1 U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced Public Cloud Extension to vRealize Automation 7 Enterprise Public Cloud Extensi	V-BMS-SSS-D-3P-F	$ 60.72	$ 58.12
VMware	TPP L4 Upgrade: U S. Federal VMware vRealize Automation 7 Advanced to U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-BMS-SSS-D-G-F	$ 19.00	$ 18.19
VMware	TPP L5 Upgrade: U S. Federal VMware vRealize Automation 7 Advanced to U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-BMS-SSS-D-P-F	$ 23.00	$ 22.02
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Green Management Suite: 1 Device for 3 years	V-BMS-SSS-U-3G-F	$ 100.32	$ 96.02
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-BMS-SSS-U-3P-F	$ 118.80	$ 113.71
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Green Management Suite: 1 Device for 1 year	V-BMS-SSS-U-G-F	$ 38.00	$ 36.37
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Green Management Suite: 1 Device for 3 years	V-BMS-SSS-U-P-F	$ 45.00	$ 43.07
VMware	U.S. Federal VMware AirWatch App Catalog 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-CLD-D-2G-F	$ 93.00	$ 89.02
VMware	U.S. Federal VMware AirWatch App Catalog 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-CLD-D-2P-F	$ 96.00	$ 91.89
VMware	U.S. Federal VMware AirWatch App Catalog 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-CLD-D-3G-F	$ 130.00	$ 124.43
VMware	U.S. Federal VMware AirWatch App Catalog 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-CLD-D-3P-F	$ 135.00	$ 129.22
VMware	U.S. Federal VMware AirWatch App Catalog 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-CLD-D-G-F	$ 49.00	$ 46.90
VMware	U.S. Federal VMware AirWatch App Catalog 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-CLD-D-P-F	$ 51.00	$ 48.82
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Video: 1 Device for 1 year	V-CLC-DLD-D-2G-F	$ 115.00	$ 110.08
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Video: 1 Device for 3 years	V-CLC-DLD-D-2P-F	$ 119.00	$ 113.90
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Video: 1 Device for 1 year	V-CLC-DLD-D-3G-F	$ 162.00	$ 155.06
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-DLD-D-3P-F	$ 167.00	$ 159.85
VMware	U.S. Federal VMware AirWatch Video Perpetual: 1 Device	V-CLC-DLD-D-G-F	$ 61.00	$ 58.39
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Video: 1 Device for 3 years	V-CLC-DLD-D-P-F	$ 63.00	$ 60.30
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-OPL-D-2G-F	$ 76.00	$ 72.75
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-OPL-D-2P-F	$ 79.00	$ 75.62
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-OPL-D-3G-F	$ 106.00	$ 101.46
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-OPL-D-3P-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-OPL-D-G-F	$ 40.00	$ 38.29
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-OPL-D-P-F	$ 42.00	$ 40.20
VMware	U.S. Federal VMware AirWatch App Catalog 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-PLL-D-F	$ 50.00	$ 47.86
VMware	U.S. Federal VMware AirWatch App Catalog 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-SSS-D-3G-F	$ 29.04	$ 27.80
VMware	U.S. Federal VMware AirWatch App Catalog 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-SSS-D-3P-F	$ 34.32	$ 32.85
VMware	U.S. Federal VMware AirWatch App Catalog 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLC-SSS-D-G-F	$ 11.00	$ 10.53
VMware	U.S. Federal VMware AirWatch App Catalog 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLC-SSS-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Telecom: 1 Device for 1 year	V-CLV-CLD-D-2G-F	$ 57.00	$ 54.56
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Telecom: 1 Device for 3 years	V-CLV-CLD-D-2P-F	$ 59.00	$ 56.47
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Telecom: 1 Device for 1 year	V-CLV-CLD-D-3G-F	$ 80.00	$ 76.57
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-CLD-D-3P-F	$ 82.00	$ 78.49
VMware	U.S. Federal VMware AirWatch Telecom Perpetual: 1 Device	V-CLV-CLD-D-G-F	$ 30.00	$ 28.72
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Telecom: 1 Device for 3 years	V-CLV-CLD-D-P-F	$ 31.00	$ 29.67
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-DLD-D-2G-F	$ 79.00	$ 75.62
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-DLD-D-2P-F	$ 81.00	$ 77.53
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-DLD-D-3G-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-DLD-D-3P-F	$ 114.00	$ 109.12
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-DLD-D-G-F	$ 42.00	$ 40.20
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-DLD-D-P-F	$ 43.00	$ 41.16
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-OPL-D-2G-F	$ 34.00	$ 32.54
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-OPL-D-2P-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-OPL-D-3G-F	$ 48.00	$ 45.94

VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-CLV-OPL-D-3P-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-CLV-OPL-D-G-F	$ 18.00	$ 17.23
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-CLV-OPL-D-P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-CLV-PLL-D-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-CLV-SSS-D-3G-F	$ 10.56	$ 10.11
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-CLV-SSS-D-3P-F	$ 13.20	$ 12.63
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-CLV-SSS-D-G-F	$ 4.00	$ 3.83
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-CLV-SSS-D-P-F	$ 5.00	$ 4.79
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-CLD-U-2G-F	$ 173.00	$ 165.59
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription	V-COL-CLD-U-2P-F	$ 188.00	$ 179.95
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription	V-COL-CLD-U-3G-F	$ 243.00	$ 232.59
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-CLD-U-3P-F	$ 264.00	$ 252.70
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-CLD-U-G-F	$ 92.00	$ 88.06
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription	V-COL-CLD-U-P-F	$ 100.00	$ 95.72
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-DLD-U-2G-F	$ 230.00	$ 220.15
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-COL-DLD-U-2P-F	$ 245.00	$ 234.51
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-COL-DLD-U-3G-F	$ 323.00	$ 309.17
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-COL-DLD-U-3P-F	$ 344.00	$ 329.27
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-DLD-U-G-F	$ 122.00	$ 116.78
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-COL-DLD-U-P-F	$ 130.00	$ 124.43
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Blue Management Suite: 1 Device for 1 year	V-COL-PLL-U-F	$ 200.00	$ 191.44
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Blue Management Suite: 1 Device for 3 years	V-COL-SSS-U-3G-F	$ 110.88	$ 106.13
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-COL-SSS-U-3P-F	$ 132.00	$ 126.35
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Blue Management Suite: 1 Device for 1 year	V-COL-SSS-U-G-F	$ 42.00	$ 40.20
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Blue Management Suite: 1 Device for 3 years	V-COL-SSS-U-P-F	$ 50.00	$ 47.86
VMware	TPP L5 U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-CLD-D-2G-F	$ 98.00	$ 90.84
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Business 7 Standard (25 OSI Pack) for 3 years	V-GMS-CLD-D-2P-F	$ 102.00	$ 94.55
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Business 7 Standard (25 OSI Pack) for 1 year	V-GMS-CLD-D-3G-F	$ 138.00	$ 127.92
VMware	U.S. Federal Production Support/Subscription VMware vRealize Business 7 Standard (25 OSI Pack) for 3 years	V-GMS-CLD-D-3P-F	$ 143.00	$ 132.55
VMware	TPP L4 U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-CLD-D-G-F	$ 52.00	$ 48.20
VMware	U.S. Federal Production Support/Subscription VMware vRealize Business 7 Standard (25 OSI Pack) for 1 year	V-GMS-CLD-D-P-F	$ 54.00	$ 50.06
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Advanced (25 OSI Pack) for 3 years	V-GMS-CLD-U-2G-F	$ 194.00	$ 179.83
VMware	TPP L1 U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-CLD-U-2P-F	$ 202.00	$ 187.24
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Advanced (25 OSI Pack) for 3 years	V-GMS-CLD-U-3G-F	$ 272.00	$ 252.13
VMware	TPP L2 U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-CLD-U-3P-F	$ 283.00	$ 262.33
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Advanced (25 OSI Pack) for 1 year	V-GMS-CLD-U-G-F	$ 103.00	$ 95.48
VMware	U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-CLD-U-P-F	$ 107.00	$ 99.18
VMware	TPP L1 U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-2G-F	$ 121.00	$ 112.16
VMware	TPP L4 U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-2P-F	$ 125.00	$ 115.87
VMware	TPP L2 U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-3G-F	$ 169.00	$ 156.65
VMware	TPP L5 U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-3P-F	$ 175.00	$ 162.22
VMware	U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-G-F	$ 64.00	$ 59.32
VMware	TPP L3 U.S. Federal VMware vRealize Business 7 Standard (Per CPU)	V-GMS-DLD-D-P-F	$ 66.00	$ 61.18
VMware	TPP L4 U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-DLD-U-2G-F	$ 239.00	$ 221.54
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 1 year	V-GMS-DLD-U-2P-F	$ 247.00	$ 228.96
VMware	TPP L5 U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-DLD-U-3G-F	$ 336.00	$ 311.46
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 2 Months	V-GMS-DLD-U-3P-F	$ 346.00	$ 320.73
VMware	TPP L3 U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-GMS-DLD-U-G-F	$ 127.00	$ 117.72
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 1 year	V-GMS-DLD-U-P-F	$ 131.00	$ 121.43

VMware	U.S. Federal Production Support/Subscription VMware vRealize Business 7 Standard (Per CPU) for 1 year	V-GMS-OPL-D-2G-F	$ 76.00	$ 72.75
VMware	U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-OPL-D-2P-F	$ 79.00	$ 75.62
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Business 7 Standard (Per CPU) for 3 year	V-GMS-OPL-D-3G-F	$ 106.00	$ 101.46
VMware	TPP L1 U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-OPL-D-3P-F	$ 111.00	$ 106.25
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Business 7 Standard (Per CPU) for 1 year	V-GMS-OPL-D-G-F	$ 40.00	$ 38.29
VMware	U.S. Federal Production Support/Subscription VMware vRealize Business 7 Standard (Per CPU) for 3 year	V-GMS-OPL-D-P-F	$ 42.00	$ 40.20
VMware	TPP L5 U.S. Federal VMware Horizon FLEX Add-On 10 pack (Per Device)	V-GMS-PLL-D-F	$ 50.00	$ 48.87
VMware	TPP L2 U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-PLL-U-F	$ 100.00	$ 97.73
VMware	TPP L2 U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-SSS-D-3G-F	$ 29.04	$ 28.38
VMware	TPP L3 U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-SSS-D-3P-F	$ 34.32	$ 33.54
VMware	U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-SSS-D-G-F	$ 11.00	$ 10.75
VMware	TPP L1 U.S. Federal VMware vRealize Business 7 Standard (25 OSI Pack)	V-GMS-SSS-D-P-F	$ 13.00	$ 12.71
VMware	TPP L5 U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-SSS-U-3G-F	$ 55.44	$ 54.18
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Advanced (25 OSI Pack) for 1 year	V-GMS-SSS-U-3P-F	$ 66.00	$ 64.50
VMware	TPP L3 U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-SSS-U-G-F	$ 21.00	$ 20.52
VMware	TPP L4 U.S. Federal VMware vRealize Automation 7 Advanced (25 OSI Pack)	V-GMS-SSS-U-P-F	$ 25.00	$ 24.43
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-HOS-CLD-D-F	$ 24.00	$ 22.97
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-HOS-DLD-D-F	$ 24.00	$ 22.97
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch App Catalog: 1 Device for 1 year	V-IDM-CLD-U-2G-F	$ 185.00	$ 177.08
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch App Catalog: 1 Device for 3 years	V-IDM-CLD-U-2P-F	$ 190.00	$ 181.86
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch App Catalog: 1 Device for 1 year	V-IDM-CLD-U-3G-F	$ 259.00	$ 247.91
VMware	U.S. Federal VMware AirWatch App Catalog 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-IDM-CLD-U-3P-F	$ 267.00	$ 255.57
VMware	U.S. Federal VMware AirWatch App Catalog Perpetual: 1 Device	V-IDM-CLD-U-G-F	$ 98.00	$ 93.80
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch App Catalog: 1 Device for 3 years	V-IDM-CLD-U-P-F	$ 101.00	$ 96.68
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-IDM-PLL-U-F	$ 96.00	$ 91.89
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-IDM-SSS-U-3G-F	$ 52.80	$ 50.54
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-IDM-SSS-U-3P-F	$ 63.36	$ 60.65
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-IDM-SSS-U-G-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-IDM-SSS-U-P-F	$ 24.00	$ 22.97
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Blue Management Suite: 1 User for 1 year	V-INB-CLD-D-2G-F	$ 46.00	$ 44.03
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Blue Management Suite: 1 User for 3 years	V-INB-CLD-D-2P-F	$ 47.00	$ 44.99
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Blue Management Suite: 1 User for 1 year	V-INB-CLD-D-3G-F	$ 64.00	$ 61.26
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-CLD-D-3P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Blue Management Suite Perpetual: 1 User	V-INB-CLD-D-G-F	$ 24.00	$ 22.97
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Blue Management Suite: 1 User for 3 years	V-INB-CLD-D-P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-DLD-D-2G-F	$ 68.00	$ 65.09
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-INB-DLD-D-2P-F	$ 70.00	$ 67.00
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-INB-DLD-D-3G-F	$ 96.00	$ 91.89
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-DLD-D-3P-F	$ 98.00	$ 93.80
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-DLD-D-G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-INB-DLD-D-P-F	$ 37.00	$ 35.42
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-OPL-D-2G-F	$ 23.00	$ 22.02
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscriptior	V-INB-OPL-D-2P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscriptior	V-INB-OPL-D-3G-F	$ 32.00	$ 30.63
VMware	U.S. Federal VMware AirWatch Yellow Management Suite Perpetual: 1 Device	V-INB-OPL-D-3P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-INB-OPL-D-G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscriptior	V-INB-OPL-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-INB-PLL-D-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Blue Management Suite 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-INB-SSS-D-3G-F	$ 10.56	$ 10.11

VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-INB-SSS-D-3P-F	$ 13.20	$ 12.63
VMware	U.S. Federal VMware AirWatch Blue Management Suite 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-INB-SSS-D-G-F	$ 4.00	$ 3.83
VMware	U.S. Federal VMware AirWatch Blue Management Suite 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-INB-SSS-D-P-F	$ 5.00	$ 4.79
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-CLD-D-2G-F	$ 98.00	$ 93.80
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-CLD-D-2P-F	$ 102.00	$ 97.63
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-CLD-D-3G-F	$ 138.00	$ 132.09
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-CLD-D-3P-F	$ 143.00	$ 136.88
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-CLD-D-G-F	$ 52.00	$ 49.77
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-CLD-D-P-F	$ 54.00	$ 51.69
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-DLD-D-2G-F	$ 121.00	$ 115.82
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-DLD-D-2P-F	$ 125.00	$ 119.65
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-DLD-D-3G-F	$ 169.00	$ 161.76
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-LTP-DLD-D-3P-F	$ 175.00	$ 167.51
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-DLD-D-G-F	$ 64.00	$ 61.26
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-LTP-DLD-D-P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-LTP-OPL-D-2G-F	$ 76.00	$ 72.75
VMware	U.S. Federal VMware AirWatch Inbox 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-LTP-OPL-D-2P-F	$ 79.00	$ 75.62
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-LTP-OPL-D-3G-F	$ 106.00	$ 101.46
VMware	U.S. Federal VMware AirWatch Teacher Tools Perpetual: 1 Device	V-LTP-OPL-D-3P-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-LTP-OPL-D-G-F	$ 40.00	$ 38.29
VMware	U.S. Federal VMware AirWatch Inbox 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-LTP-OPL-D-P-F	$ 42.00	$ 40.20
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Inbox: 1 Device for 1 year	V-LTP-PLL-D-F	$ 50.00	$ 47.86
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Inbox: 1 Device for 3 years	V-LTP-SSS-D-3G-F	$ 29.04	$ 27.80
VMware	U.S. Federal VMware AirWatch Inbox 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-LTP-SSS-D-3P-F	$ 34.32	$ 32.85
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Inbox: 1 Device for 1 year	V-LTP-SSS-D-G-F	$ 11.00	$ 10.53
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Inbox: 1 Device for 3 years	V-LTP-SSS-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Telecom: 1 User for 1 year	V-MAW-CLD-D-2G-F	$ 12.00	$ 11.49
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Telecom: 1 User for 3 years	V-MAW-CLD-D-2P-F	$ 14.00	$ 13.40
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Telecom: 1 User for 1 year	V-MAW-CLD-D-3G-F	$ 16.00	$ 15.31
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MAW-CLD-D-3P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Telecom Perpetual: 1 User	V-MAW-CLD-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Telecom: 1 User for 3 years	V-MAW-CLD-D-P-F	$ 7.00	$ 6.70
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MAW-DLD-D-2G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MAW-DLD-D-2P-F	$ 14.00	$ 13.40
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MAW-DLD-D-3G-F	$ 16.00	$ 15.31
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MAW-DLD-D-3P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MAW-DLD-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MAW-DLD-D-P-F	$ 7.00	$ 6.70
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MAW-PLL-D-F	$ 10.00	$ 9.57
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MAW-SSS-D-3G-F	$ 5.28	$ 5.05
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MAW-SSS-D-3P-F	$ 7.92	$ 7.58
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MAW-SSS-D-G-F	$ 2.00	$ 1.91
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MAW-SSS-D-P-F	$ 3.00	$ 2.87
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Orange Management Suite: 1 User for 1 year	V-MBM-CLD-D-2G-F	$ 46.00	$ 44.03
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Orange Management Suite: 1 User for 3 years	V-MBM-CLD-D-2P-F	$ 47.00	$ 44.99
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Orange Management Suite: 1 User for 1 year	V-MBM-CLD-D-3G-F	$ 64.00	$ 61.26
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-CLD-D-3P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Orange Management Suite Perpetual: 1 User	V-MBM-CLD-D-G-F	$ 24.00	$ 22.97
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Orange Management Suite: 1 User for 3 years	V-MBM-CLD-D-P-F	$ 25.00	$ 23.93

VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-DLD-D-2G-F	$ 68.00	$ 65.09
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-MBM-DLD-D-2P-F	$ 70.00	$ 67.00
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-MBM-DLD-D-3G-F	$ 96.00	$ 91.89
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-DLD-D-3P-F	$ 98.00	$ 93.80
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-DLD-D-G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-MBM-DLD-D-P-F	$ 37.00	$ 35.42
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-OPL-D-2G-F	$ 23.00	$ 22.02
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-MBM-OPL-D-2P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-MBM-OPL-D-3G-F	$ 32.00	$ 30.63
VMware	U.S. Federal VMware AirWatch Blue Management Suite Perpetual: 1 Device	V-MBM-OPL-D-3P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MBM-OPL-D-G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-MBM-OPL-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MBM-PLL-D-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MBM-SSS-D-3G-F	$ 10.56	$ 10.11
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MBM-SSS-D-3P-F	$ 13.20	$ 12.63
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MBM-SSS-D-G-F	$ 4.00	$ 3.83
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MBM-SSS-D-P-F	$ 5.00	$ 4.79
VMware	U.S. Federal Basic Support/Subscription for VMware Collaboration Bundle: 1 User for 1 year	V-MDM-CLD-D-2G-F	$ 98.00	$ 93.80
VMware	U.S. Federal Production Support/Subscription for VMware Collaboration Bundle: 1 User for 3 years	V-MDM-CLD-D-2P-F	$ 102.00	$ 97.63
VMware	U.S. Federal Production Support/Subscription for VMware Collaboration Bundle: 1 User for 1 year	V-MDM-CLD-D-3G-F	$ 138.00	$ 132.09
VMware	U.S. Federal VMware Collaboration Bundle 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-CLD-D-3P-F	$ 143.00	$ 136.88
VMware	U.S. Federal VMware Collaboration Bundle Perpetual: 1 User	V-MDM-CLD-D-G-F	$ 52.00	$ 49.77
VMware	U.S. Federal Basic Support/Subscription for VMware Collaboration Bundle: 1 User for 3 years	V-MDM-CLD-D-P-F	$ 54.00	$ 51.69
VMware	U.S. Federal VMware Collaboration Bundle 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-DLD-D-2G-F	$ 121.00	$ 115.82
VMware	U.S. Federal VMware Collaboration Bundle 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-DLD-D-2P-F	$ 125.00	$ 119.65
VMware	U.S. Federal VMware Collaboration Bundle 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-DLD-D-3G-F	$ 169.00	$ 161.76
VMware	U.S. Federal VMware Collaboration Bundle 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-DLD-D-3P-F	$ 175.00	$ 167.51
VMware	U.S. Federal VMware Collaboration Bundle 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-DLD-D-G-F	$ 64.00	$ 61.26
VMware	U.S. Federal VMware Collaboration Bundle 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-DLD-D-P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware Collaboration Bundle 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-OPL-D-2G-F	$ 76.00	$ 72.75
VMware	U.S. Federal VMware Collaboration Bundle 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-OPL-D-2P-F	$ 79.00	$ 75.62
VMware	U.S. Federal VMware Collaboration Bundle 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-OPL-D-3G-F	$ 106.00	$ 101.46
VMware	U.S. Federal VMware AirWatch Inbox Perpetual: 1 Device	V-MDM-OPL-D-3P-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware Collaboration Bundle 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-MDM-OPL-D-G-F	$ 40.00	$ 38.29
VMware	U.S. Federal VMware Collaboration Bundle 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-MDM-OPL-D-P-F	$ 42.00	$ 40.20
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MDM-PLL-D-F	$ 50.00	$ 47.86
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MDM-SSS-D-3G-F	$ 29.04	$ 27.80
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MDM-SSS-D-3P-F	$ 34.32	$ 32.85
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-MDM-SSS-D-G-F	$ 11.00	$ 10.53
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-MDM-SSS-D-P-F	$ 13.00	$ 12.44
VMware	TPP L3 U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-CLD-D-2G-F	$ 115.00	$ 106.60
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack) for 1 year	V-OMS-CLD-D-2P-F	$ 121.00	$ 112.16
VMware	TPP L4 U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-CLD-D-3G-F	$ 162.00	$ 150.17
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack) for 1 year	V-OMS-CLD-D-3P-F	$ 169.00	$ 156.65
VMware	TPP L2 U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-CLD-D-G-F	$ 61.00	$ 56.54
VMware	TPP L5 U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-CLD-D-P-F	$ 64.00	$ 59.32
VMware	TPP L4 U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-CLD-U-2G-F	$ 230.00	$ 220.15
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 for Desktop per CCU (25 Pack) for 1 year	V-OMS-CLD-U-2P-F	$ 239.00	$ 228.77
VMware	TPP L5 U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-CLD-U-3G-F	$ 323.00	$ 309.17

VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 (10 Pack) for 1 year	V-OMS-CLD-U-3P-F	$ 336.00	$ 321.61
VMware	TPP L3 U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-CLD-U-G-F	$ 122.00	$ 116.78
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 for Desktop per CCU (25 Pack) for 1 year	V-OMS-CLD-U-P-F	$ 127.00	$ 121.56
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack) for 3 years	V-OMS-DLD-D-2G-F	$ 138.00	$ 127.92
VMware	TPP L2 U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-DLD-D-2P-F	$ 143.00	$ 132.55
VMware	U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-DLD-D-3G-F	$ 193.00	$ 178.90
VMware	TPP L3 U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-DLD-D-3P-F	$ 201.00	$ 186.32
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack) for 3 years	V-OMS-DLD-D-G-F	$ 73.00	$ 67.67
VMware	TPP L1 U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-DLD-D-P-F	$ 76.00	$ 70.45
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 for Desktop per CCU (25 Pack) for 3 years	V-OMS-DLD-U-2G-F	$ 275.00	$ 263.22
VMware	TPP L1 Upgrade: U S. Federal VMware vRealize Automation 7 Advanced to U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-OMS-DLD-U-2P-F	$ 284.00	$ 271.84
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 for Desktop per CCU (25 Pack) for 3 years	V-OMS-DLD-U-3G-F	$ 386.00	$ 369.47
VMware	TPP L2 Upgrade: U S. Federal VMware vRealize Automation 7 Advanced to U.S. Federal VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-OMS-DLD-U-3P-F	$ 399.00	$ 381.91
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 (10 Pack) for 1 year	V-OMS-DLD-U-G-F	$ 146.00	$ 139.75
VMware	U.S. Federal Upgrade: VMware vRealize Automation 7 Advanced to VMware vRealize Automation 7 Enterprise (25 OSI Pack)	V-OMS-DLD-U-P-F	$ 151.00	$ 144.53
VMware	TPP L5 U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-OPL-D-2G-F	$ 93.00	$ 89.02
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 2 Months	V-OMS-OPL-D-2P-F	$ 98.00	$ 93.80
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 1 year	V-OMS-OPL-D-3G-F	$ 130.00	$ 124.43
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 2 Months	V-OMS-OPL-D-3P-F	$ 138.00	$ 132.09
VMware	TPP L4 U.S. Federal VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack)	V-OMS-OPL-D-G-F	$ 49.00	$ 46.90
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 1 year	V-OMS-OPL-D-P-F	$ 52.00	$ 49.77
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 2 Months	V-OMS-PLL-D-F	$ 70.00	$ 68.41
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 3 years	V-OMS-PLL-U-F	$ 140.00	$ 134.01
VMware	U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-SSS-D-3G-F	$ 39.60	$ 38.70
VMware	TPP L1 U.S. Federal VMware vRealize Automation 7 Advanced Public Cloud Extension (25 OSI Pack)	V-OMS-SSS-D-3P-F	$ 47.52	$ 46.44
VMware	U.S. Federal Basic Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 3 years	V-OMS-SSS-D-G-F	$ 15.00	$ 14.66
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise (25 OSI Pack) for 3 years	V-OMS-SSS-D-P-F	$ 18.00	$ 17.59
VMware	TPP L1 U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-SSS-U-3G-F	$ 76.56	$ 73.28
VMware	TPP L2 U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-SSS-U-3P-F	$ 92.40	$ 88.44
VMware	U.S. Federal Production Support/Subscription VMware vRealize Automation 7 Enterprise Public Cloud Extension (25 OSI Pack) for 3 years	V-OMS-SSS-U-G-F	$ 29.00	$ 27.76
VMware	U.S. Federal VMware vRealize Automation 7 for Desktop per CCU (25 Pack)	V-OMS-SSS-U-P-F	$ 35.00	$ 33.50
VMware	U.S. Federal AirWatch by VMware Accelerated Deployment Add-On One Time Fee	V-PS-ACCELERATE-F	$ 5,500.00	$ 5,375.31
VMware	U.S. Federal VMware AirWatch Per App Tunneling Configuration One Time Fee	V-PS-APP-VPN-SP-F	$ 750.00	$ 733.00
VMware	U.S. Federal VMware AirWatch Application Server Migration	V-PS-APSV-MG-SP-F	$ 1,000.00	$ 977.33
VMware	U.S. Federal VMware AirWatch Reports Server Configuration and Deployment One Time Fee	V-PS-AW-RPT-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Telecom Module Deployment One Time Fee	V-PS-AWT-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Video Deployment One Time Fee	V-PS-AWV-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Blue Management Suite Cloud Deployment Fee One Time Fee	V-PS-BMS-CLD-SP-F	$ 4,500.00	$ 4,397.98
VMware	U.S. Federal VMware AirWatch Blue Management Suite On Premise Deployment Fee One Time Fee	V-PS-BMS-OP-SP-F	$ 5,500.00	$ 5,375.31
VMware	U.S. Federal AirWatch by VMware Blue Management Suite On-Premise - Includes 3 days On-Site	V-PS-BMS-OPL-3OS-F	$ 9,800.00	$ 9,577.83
VMware	U.S. Federal AirWatch by VMware Blue Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-PS-BMS-OPL-RSS-F	$ 7,250.00	$ 7,085.64
VMware	U.S. Federal VMware AirWatch Database Server Migration	V-PS-DBSV-MG-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Device Enrollment Program (DEP) Configuration and Deployment One Time Fee	V-PS-DEP-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Cloud - Dedicated Environment Setup One Time Fee / Environment	V-PS-DHE-SET-F	$ 10,000.00	$ 9,773.30
VMware	U.S. Federal VMware AirWatch Cloud - Dedicated UAT Environment 1 Year Fee / Device	V-PS-DHE-UAT-F	$ 10,000.00	$ 9,773.30
VMware	U.S. Federal VMware AirWatch Disaster Recovery Set-up Fee	V-PS-DR-SP-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware AirWatch Cloud Connector (ACC) Configuration and Deployment - Enterprise Integration One Time Fee	V-PS-ENT-ACC-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Telecom 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-PS-ENT-SUP-GEO-F	$ 25,000.00	$ 23,929.47
VMware	U.S. Federal AirWatch by VMware End User On-Boarding Video	V-PS-EU-OBV-F	$ 1,200.00	$ 1,172.80

VMware	U.S. Federal VMware AirWatch Enterprise Gold SaaS Cloud Deployment up to 100000 devices One Time Fee	V-PS-GLD-CLD-SP-F	$ 37,500.00	$ 36,649.87
VMware	U.S. Federal VMware AirWatch Enterprise Gold On Premise Deployment up to 100000 devices One Time Fee	V-PS-GLD-OP-SP-F	$ 50,000.00	$ 48,866.50
VMware	U.S. Federal VMware AirWatch Green Management Suite Lite Cloud Deployment Fee One Time Fee	V-PS-GMCL-LITE-F	$ 750.00	$ 733.00
VMware	U.S. Federal VMware AirWatch Green Management Suite Lite On Premise Deployment Fee One Time Fee	V-PS-GMOP-LITE-F	$ 1,750.00	$ 1,710.33
VMware	U.S. Federal VMware AirWatch Green Management Suite Cloud Deployment Fee One Time Fee	V-PS-GMS-CLD-SP-F	$ 1,500.00	$ 1,465.99
VMware	U.S. Federal VMware AirWatch Green Management Suite On Premise Deployment Fee One Time Fee	V-PS-GMS-OP-SP-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal AirWatch by VMware Green Management Suite On-Premise - Includes 2 days On-Site	V-PS-GMS-OPL-2OS-F	$ 5,450.00	$ 5,326.45
VMware	U.S. Federal AirWatch by VMware Green Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-PS-GMS-OPL-RSS-F	$ 3,250.00	$ 3,176.32
VMware	U.S. Federal VMware AirWatch High Availability Set-up One Time Fee	V-PS-HA-SP-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware AirWatch Health Check One Time Fee	V-PS-HC-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal VMware AirWatch Professional Services - 1 hour of support services One Time Fee	V-PS-HR-PS-F	$ 150.00	$ 146.60
VMware	U.S. Federal AirWatch by VMware Browser Deployment Fee One Time Fee	V-PS-MBM-SP-F	$ 750.00	$ 733.00
VMware	U.S. Federal AirWatch by VMware AirWatch Content Locker Collaborate Add-On for K12+MAG Management Suite Deployment One Time Fee	V-PS-MCC-BMS-SP-F	$ 1,000.00	$ 977.33
VMware	U.S. Federal AirWatch by VMware AirWatch Content Collaborate Add-On for Green/Orange Deployment Fee One Time Fee	V-PS-MCC-SP-F	$ 1,500.00	$ 1,465.99
VMware	U.S. Federal VMware AirWatch Mobile Content Management Only Cloud Deployment One Time Fee	V-PS-MCM-CLD-SP-F	$ 2,000.00	$ 1,954.66
VMware	U.S. Federal VMware AirWatch Mobile Content Management Only On Premise Deployment One Time Fee	V-PS-MCM-OP-SP-F	$ 3,000.00	$ 2,931.99
VMware	U.S. Federal VMware AirWatch Content View Cloud Deployment Fee One Time Fee	V-PS-MCV-SP-F	$ 750.00	$ 733.00
VMware	U.S. Federal VMware AirWatch Advanced Migration Configuration and Deployment On Premise Deployment Fee One Time Fee	V-PS-MIG-ADV-OP-F	$ 4,000.00	$ 3,909.32
VMware	U.S. Federal AirWatch by VMware Advanced Migration Configuration and Deployment Cloud One Time Fee	V-PS-MIG-ADV-SP-F	$ 3,000.00	$ 2,931.99
VMware	U.S. Federal VMware AirWatch Basic Migration Configuration and Deployment On Premise Deployment Fee One Time Fee	V-PS-MIG-BASIC-OP-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal AirWatch by VMware Basic Migration Configuration and Deployment Cloud Deployment One Time Fee	V-PS-MIG-BASIC-SP-F	$ 1,500.00	$ 1,465.99
VMware	U.S. Federal VMware AirWatch Rugged Device Configuration and Deployment Add-On One Time Fee	V-PS-MS-ADDONRG-SP-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware AirWatch Rugged Device Cloud Configuration and Deployment One Time Fee	V-PS-MS-CLDSPRG-SP-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal VMware AirWatch Rugged Device On Premise Configuration and Deployment One Time Fee	V-PS-MS-OP-SPRG-SP-F	$ 3,500.00	$ 3,420.65
VMware	U.S. Federal VMware AirWatch Orange Management Suite Cloud Deployment Fee One Time Fee	V-PS-OMS-CLD-SP-F	$ 2,000.00	$ 1,954.66
VMware	U.S. Federal VMware AirWatch Orange Management Suite On Premise Deployment Fee One Time Fee	V-PS-OMS-OP-SP-F	$ 3,000.00	$ 2,931.99
VMware	U.S. Federal AirWatch by VMware Orange Management Suite On-Premise - Includes 2 days On-Site	V-PS-OMS-OPL-2OS-F	$ 6,200.00	$ 6,059.45
VMware	U.S. Federal AirWatch by VMware Orange Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-PS-OMS-OPL-RSS-F	$ 4,000.00	$ 3,909.32
VMware	U.S. Federal VMware AirWatch On Premise to Dedicated Deployment One Time Fee	V-PS-OP2-DHS-F	$ 10,000.00	$ 9,773.30
VMware	U.S. Federal AirWatch by VMware On-Premise Weekend Upgrades and Off-Hours Requiring Same Region One Time Fee	V-PS-OPL-WUOH-F	$ 3,700.00	$ 3,616.12
VMware	U.S. Federal VMware AirWatch PKI Certificate Advanced Configuration and Deployment One Time Fee	V-PS-PKI-ADV-SP-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal VMware AirWatch PKI Certificate Basic Configuration and Deployment One Time Fee	V-PS-PKI-BASIC-SP-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware AirWatch PowerShell Configuration and Deployment One Time Fee	V-PS-PWR-SHELL-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal AirWatch Socialcast Cloud Deployment One Time Fee	V-PS-SC-CLD-SP-F	$ 1,800.00	$ 1,759.19
VMware	U.S. Federal AirWatch by VMware SocialCast Dedicated SaaS Setup Fee One Time Fee	V-PS-SC-DSAAS-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal AirWatch Socialcast On Premise Deployment One Time Fee	V-PS-SC-OP-SP-F	$ 4,200.00	$ 4,104.79
VMware	U.S. Federal AirWatch by VMware SaaS SEG and MAG Upgrade	V-PS-SEG-MAG-UG-F	$ 800.00	$ 781.86
VMware	U.S. Federal AirWatch by VMware SaaS SEG and MAG Weekend and Same Region Off-Hours Upgrade	V-PS-SEG-MAG-WR-F	$ 3,300.00	$ 3,225.19
VMware	U.S. Federal VMware AirWatch Secure Email Gateway (SEG) Configuration and Deployment One Time Fee	V-PS-SEG-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Enterprise Silver SaaS Cloud Deployment up to 50000 devices One Time Fee	V-PS-SLV-CLD-SP-F	$ 20,000.00	$ 19,546.60
VMware	U.S. Federal VMware AirWatch Enterprise Silver On Premise Deployment up to 50000 devices One Time Fee	V-PS-SLV-OP-SP-F	$ 25,000.00	$ 24,433.25
VMware	U.S. Federal VMware AirWatch Professional Services - 8 hours of support services One Time Fee	V-PS-SP-DAY-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware AirWatch Standby Support (Monday - Friday) One Time Fee	V-PS-STBS-WD-PS-F	$ 5,000.00	$ 4,886.65
VMware	U.S. Federal VMware AirWatch Standby Support (Weekend) One Time Fee	V-PS-STBS-WE-PS-F	$ 10,000.00	$ 9,773.30
VMware	U.S. Federal VMware AirWatch Incident Support Package 5 pack	V-PS-SUPP-INC-F	$ 1,000.00	$ 977.33
VMware	U.S. Federal VMware AirWatch Telecom 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-PS-TAM-F	$ 69,995.00	$ 66,997.73
VMware	U.S. Federal VMware AirWatch Professional Services Travel and Expense - daily One Time Fee	V-PS-TE-AW-F	$ 610.00	$ 596.17
VMware	U.S. Federal VMware AirWatch Teacher Tools Deployment One Time Fee	V-PS-TT-SP-F	$ 500.00	$ 488.66
VMware	U.S. Federal VMware AirWatch Upgrade from Green Management Suite to Orange Management Suite Deployment (Cloud or On Premise) One Time Fee	V-PS-UPG-GM-OM-SP-F	$ 500.00	$ 488.66

VMware	U.S. Federal VMware AirWatch Dedicated Cloud Upgrade off-hours One Time Fee	V-PS-UPGR-OFFHOURS-F	$ 2,500.00	$ 2,443.32
VMware	U.S. Federal VMware AirWatch Upgrade Services for On Premise Deployments Fee One Time Fee	V-PS-UPGR-STD-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware Collaborate Bundle Cloud Deployment One Time Fee	V-PS-VCB-CLD-SP-F	$ 4,000.00	$ 3,909.32
VMware	U.S. Federal VMware Collaborate Bundle On Premise Deployment One time Fee	V-PS-VCB-OP-SP-F	$ 7,500.00	$ 7,329.97
VMware	U.S. Federal VMware Identity Manager Shared Cloud Deployment One Time Fee	V-PS-VIDM-CLD-SP-F	$ 1,200.00	$ 1,172.80
VMware	U.S. Federal VMware Identity Manager On Premise Deployment One Time Fee	V-PS-VIDM-OP-SP-F	$ 1,800.00	$ 1,759.19
VMware	U.S. Federal VMware AirWatch Yellow Management Suite Cloud Deployment Fee One Time Fee	V-PS-YMS-CLD-SP-F	$ 5,500.00	$ 5,375.31
VMware	U.S. Federal VMware AirWatch Yellow Management Suite On Premise Deployment Fee One Time Fee	V-PS-YMS-OP-SP-F	$ 6,500.00	$ 6,352.64
VMware	U.S. Federal AirWatch by VMware Yellow Management Suite On-Premise - Includes 3 days On-Site	V-PS-YMS-OPL-3OS-F	$ 11,050.00	$ 10,799.50
VMware	U.S. Federal AirWatch by VMware Yellow Management Suite On-Premise with ability to Remote Screen Share No On-Site Included	V-PS-YMS-OPL-RSS-F	$ 8,500.00	$ 8,307.30
VMware	U.S. Federal VMware Identity Manager Advanced Edition SaaS Deployment One Time Fee	V-PSVIDM-ADVCLD-SP-F	$ 3,000.00	$ 2,931.99
VMware	U.S. Federal VMware Identity Manager Advanced Edition On-Premises Deployment One Time Fee	V-PSVIDM-ADVOP-SP-F	$ 4,000.00	$ 3,909.32
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-CLD-D-2G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-CLD-D-2P-F	$ 38.00	$ 36.37
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-CLD-D-3G-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-CLD-D-3P-F	$ 53.00	$ 50.73
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-CLD-D-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-CLD-D-P-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-DLD-D-2G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware AirWatch Mobile Browser 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-DLD-D-2P-F	$ 38.00	$ 36.37
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-DLD-D-3G-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-PTR-DLD-D-3P-F	$ 53.00	$ 50.73
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-DLD-D-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Mobile Browser 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-PTR-DLD-D-P-F	$ 20.00	$ 19.14
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Browser: 1 Device for 1 year	V-PTR-PLL-D-F	$ 25.00	$ 23.93
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Browser: 1 Device for 3 years	V-PTR-SSS-D-3G-F	$ 13.20	$ 12.63
VMware	U.S. Federal VMware AirWatch Mobile Browser 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-PTR-SSS-D-3P-F	$ 15.84	$ 15.16
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Browser: 1 Device for 1 year	V-PTR-SSS-D-G-F	$ 5.00	$ 4.79
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Browser: 1 Device for 3 years	V-PTR-SSS-D-P-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-RUG-CLD-D-2G-F	$ 98.00	$ 93.80
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-RUG-CLD-D-2P-F	$ 102.00	$ 97.63
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-RUG-CLD-D-3G-F	$ 138.00	$ 132.09
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-RUG-CLD-D-3P-F	$ 143.00	$ 136.88
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-RUG-CLD-D-G-F	$ 52.00	$ 49.77
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-RUG-CLD-D-P-F	$ 54.00	$ 51.69
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Video: 1 User for 1 year	V-RUG-DLD-D-2G-F	$ 121.00	$ 115.82
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Video: 1 User for 3 years	V-RUG-DLD-D-2P-F	$ 125.00	$ 119.65
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Video: 1 User for 1 year	V-RUG-DLD-D-3G-F	$ 169.00	$ 161.76
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-RUG-DLD-D-3P-F	$ 175.00	$ 167.51
VMware	U.S. Federal VMware AirWatch Video Perpetual: 1 User	V-RUG-DLD-D-G-F	$ 64.00	$ 61.26
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Video: 1 User for 3 years	V-RUG-DLD-D-P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-RUG-OPL-D-2G-F	$ 76.00	$ 72.75
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-RUG-OPL-D-2P-F	$ 79.00	$ 75.62
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-RUG-OPL-D-3G-F	$ 106.00	$ 101.46
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-RUG-OPL-D-3P-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-RUG-OPL-D-G-F	$ 40.00	$ 38.29
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-RUG-OPL-D-P-F	$ 42.00	$ 40.20
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-RUG-PLL-D-F	$ 50.00	$ 47.86
VMware	U.S. Federal VMware AirWatch Video 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-RUG-SSS-D-3G-F	$ 29.04	$ 27.80

VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-RUG-SSS-D-3P-F	$ 34.32	$ 32.85
VMware	U.S. Federal VMware AirWatch Video 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-RUG-SSS-D-G-F	$ 11.00	$ 10.53
VMware	U.S. Federal VMware AirWatch Video 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-RUG-SSS-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-CLD-U-2G-F	$ 59.00	$ 56.47
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-SCT-CLD-U-2P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-SCT-CLD-U-3G-F	$ 82.00	$ 78.49
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-CLD-U-3P-F	$ 93.00	$ 89.02
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-CLD-U-G-F	$ 31.00	$ 29.67
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription	V-SCT-CLD-U-P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-DLD-U-2G-F	$ 81.00	$ 77.53
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-SCT-DLD-U-2P-F	$ 89.00	$ 85.19
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-SCT-DLD-U-3G-F	$ 114.00	$ 109.12
VMware	U.S. Federal VMware AirWatch Mobile Browser Perpetual: 1 Device	V-SCT-DLD-U-3P-F	$ 125.00	$ 119.65
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-DLD-U-G-F	$ 43.00	$ 41.16
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscript	V-SCT-DLD-U-P-F	$ 47.00	$ 44.99
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Yellow Management Suite: 1 User for 1 year	V-SCT-PLL-U-F	$ 90.00	$ 86.15
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Yellow Management Suite: 1 User for 3 years	V-SCT-SSS-U-3G-F	$ 50.16	$ 48.01
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-SCT-SSS-U-3P-F	$ 60.72	$ 58.12
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Yellow Management Suite: 1 User for 1 year	V-SCT-SSS-U-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Yellow Management Suite: 1 User for 3 years	V-SCT-SSS-U-P-F	$ 23.00	$ 22.02
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-CLD-D-2G-F	$ 23.00	$ 22.02
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-CLD-D-2P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-CLD-D-3G-F	$ 32.00	$ 30.63
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-CLD-D-3P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-CLD-D-G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-CLD-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-TEL-CLD-U-2G-F	$ 47.00	$ 44.99
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-TEL-CLD-U-2P-F	$ 49.00	$ 46.90
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-TEL-CLD-U-3G-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscript	V-TEL-CLD-U-3P-F	$ 69.00	$ 66.05
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-TEL-CLD-U-G-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-TEL-CLD-U-P-F	$ 26.00	$ 24.89
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-DLD-D-2G-F	$ 46.00	$ 44.03
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-DLD-D-2P-F	$ 47.00	$ 44.99
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-DLD-D-3G-F	$ 64.00	$ 61.26
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TEL-DLD-D-3P-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-DLD-D-G-F	$ 24.00	$ 22.97
VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-TEL-DLD-D-P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscript	V-TEL-DLD-U-2G-F	$ 93.00	$ 89.02
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Sub	V-TEL-DLD-U-2P-F	$ 94.00	$ 89.97
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Sub	V-TEL-DLD-U-3G-F	$ 130.00	$ 124.43
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TEL-DLD-U-3P-F	$ 132.00	$ 126.35
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscript	V-TEL-DLD-U-G-F	$ 49.00	$ 46.90
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Sub	V-TEL-DLD-U-P-F	$ 50.00	$ 47.86
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TEL-OPL-D-2G-F	$ 23.00	$ 22.02
VMware	U.S. Federal VMware AirWatch Mobile Device 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TEL-OPL-D-2P-F	$ 25.00	$ 23.93
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TEL-OPL-D-3G-F	$ 32.00	$ 30.63
VMware	U.S. Federal VMware AirWatch Laptop Management Suite Perpetual: 1 Device	V-TEL-OPL-D-3P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TEL-OPL-D-G-F	$ 12.00	$ 11.49

VMware	U.S. Federal VMware AirWatch Mobile Device 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TEL-OPL-D-P-F	$ 13.00	$ 12.44
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Device: 1 Device for 1 year	V-TEL-PLL-D-F	$ 20.00	$ 19.14
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch for Laptop Management Suite: 1 Device for 1 year	V-TEL-PLL-U-F	$ 40.00	$ 38.29
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Device: 1 Device for 3 years	V-TEL-SSS-D-3G-F	$ 10.56	$ 10.11
VMware	U.S. Federal VMware AirWatch Mobile Device 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TEL-SSS-D-3P-F	$ 13.20	$ 12.63
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Device: 1 Device for 1 year	V-TEL-SSS-D-G-F	$ 4.00	$ 3.83
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Device: 1 Device for 3 years	V-TEL-SSS-D-P-F	$ 5.00	$ 4.79
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch for Laptop Management Suite: 1 Device for 3 years	V-TEL-SSS-U-3G-F	$ 21.12	$ 20.22
VMware	U.S. Federal VMware AirWatch for Laptop Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-TEL-SSS-U-3P-F	$ 26.40	$ 25.27
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch for Laptop Management Suite: 1 Device for 1 year	V-TEL-SSS-U-G-F	$ 8.00	$ 7.66
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch for Laptop Management Suite: 1 Device for 3 years	V-TEL-SSS-U-P-F	$ 10.00	$ 9.57
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-CLD-D-2G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-TTS-CLD-D-2P-F	$ 14.00	$ 13.40
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-TTS-CLD-D-3G-F	$ 16.00	$ 15.31
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-CLD-D-3P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-CLD-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscriptio	V-TTS-CLD-D-P-F	$ 7.00	$ 6.70
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-DLD-D-2G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-TTS-DLD-D-2P-F	$ 14.00	$ 13.40
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-TTS-DLD-D-3G-F	$ 16.00	$ 15.31
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TTS-DLD-D-3P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-DLD-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-TTS-DLD-D-P-F	$ 7.00	$ 6.70
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TTS-OPL-D-2G-F	$ 12.00	$ 11.49
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TTS-OPL-D-2P-F	$ 14.00	$ 13.40
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TTS-OPL-D-3G-F	$ 16.00	$ 15.31
VMware	U.S. Federal VMware AirWatch Yellow Management Suite Perpetual: 1 User	V-TTS-OPL-D-3P-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-TTS-OPL-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-TTS-OPL-D-P-F	$ 7.00	$ 6.70
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Yellow Management Suite: 1 Device for 1 year	V-TTS-PLL-D-F	$ 20.00	$ 19.14
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Yellow Management Suite: 1 Device for 3 years	V-TTS-SSS-D-3G-F	$ 10.56	$ 10.11
VMware	U.S. Federal VMware AirWatch Yellow Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-TTS-SSS-D-3P-F	$ 13.20	$ 12.63
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Yellow Management Suite: 1 Device for 1 year	V-TTS-SSS-D-G-F	$ 4.00	$ 3.83
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Yellow Management Suite: 1 Device for 3 years	V-TTS-SSS-D-P-F	$ 5.00	$ 4.79
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-BU-CLD-U-G-F	$ 83.50	$ 77.40
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Application Wrapping: 1 Device for 3 years	V-UG-BU-CLD-U-P-F	$ 87.00	$ 80.64
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-BU-DLD-U-G-F	$ 97.00	$ 89.91
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Application Wrapping: 1 Device for 3 years	V-UG-BU-DLD-U-P-F	$ 100.00	$ 92.70
VMware	U.S. Federal VMware AirWatch Enterprise Support 1 Year Fee per Geography or Business Unit	V-UG-BU-PLL-U-F	$ 99.00	$ 96.76
VMware	U.S. Federal VMware AirWatch Technical Account Manager can be purchased by AirWatch Production or Enterprise Customers	V-UG-BU-SSS-U-G-F	$ 21.00	$ 20.52
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic Su	V-UG-BU-SSS-U-P-F	$ 25.00	$ 24.43
VMware	U.S. Federal VMware Identity Manager Advanced Edition Perpetual: 1 User	V-UG-BY-CLD-D-G-F	$ 39.50	$ 37.81
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-BY-CLD-D-P-F	$ 40.50	$ 38.77
VMware	U.S. Federal VMware AirWatch Telecom 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-UG-BY-CLD-U-G-F	$ 78.00	$ 74.66
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-BY-CLD-U-P-F	$ 81.50	$ 78.01
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-UG-BY-DLD-D-G-F	$ 39.50	$ 37.81
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscriptio	V-UG-BY-DLD-D-P-F	$ 40.50	$ 37.54
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-UG-BY-DLD-U-G-F	$ 78.00	$ 74.66
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscriptio	V-UG-BY-DLD-U-P-F	$ 81.50	$ 75.55

VMware	U.S. Federal Basic Support/Subscription for VMware Identity Manager Advanced Edition: 1 User for 1 year	V-UG-BY-OPL-D-G-F	$ 39.50	$ 37.81
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices Perpetual: 1 Device	V-UG-BY-OPL-D-P-F	$ 40.50	$ 38.77
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic	V-UG-BY-PLL-D-F	$ 44.00	$ 43.00
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Blue Management Suite Subscription - On Premise (Includes Basic Support/	V-UG-BY-SSS-D-G-F	$ 9.00	$ 8.80
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Yellow Management Suite Subscription - On Premise (Includes Basic Suppo	V-UG-BY-SSS-D-P-F	$ 11.00	$ 10.75
VMware	U.S. Federal Production Support/Subscription for VMware Identity Manager Advanced Edition: 1 User for 1 year	V-UG-GB-CLD-D-G-F	$ 26.50	$ 25.37
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Management Suite for Rugged Devices: 1 Device for 1 year	V-UG-GB-CLD-D-P-F	$ 28.50	$ 27.28
VMware	U.S. Federal VMware Identity Manager Advanced Edition 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-UG-GB-CLD-U-G-F	$ 54.00	$ 51.69
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subs	V-UG-GB-CLD-U-P-F	$ 57.00	$ 54.56
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-UG-GB-DLD-D-G-F	$ 26.50	$ 25.37
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subsc	V-UG-GB-DLD-D-P-F	$ 28.50	$ 26.42
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-UG-GB-DLD-U-G-F	$ 54.00	$ 51.69
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subsc	V-UG-GB-DLD-U-P-F	$ 57.00	$ 52.84
VMware	U.S. Federal VMware Identity Manager Advanced Edition 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-UG-GB-OPL-D-G-F	$ 26.50	$ 25.37
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Management Suite for Rugged Devices: 1 Device for 3 years	V-UG-GB-OPL-D-P-F	$ 28.50	$ 27.28
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Blue Management Suite Subscription - Shared Cloud (Includes SaaS Basic Su	V-UG-GB-PLL-D-F	$ 44.00	$ 43.00
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic	V-UG-GB-SSS-D-G-F	$ 9.00	$ 8.80
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic	V-UG-GB-SSS-D-P-F	$ 11.00	$ 10.75
VMware	U.S. Federal Basic Support/Subscription for VMware Identity Manager Advanced Edition: 1 User for 3 years	V-UG-GO-CLD-D-G-F	$ 10.00	$ 9.57
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Management Suite for Rugged Devices: 1 Device for 1 year	V-UG-GO-CLD-D-P-F	$ 11.00	$ 10.53
VMware	U.S. Federal VMware Identity Manager Advanced Edition 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-UG-GO-CLD-U-G-F	$ 21.00	$ 20.10
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Suppor	V-UG-GO-CLD-U-P-F	$ 22.00	$ 21.06
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-UG-GO-DLD-D-G-F	$ 10.00	$ 9.57
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subsc	V-UG-GO-DLD-D-P-F	$ 11.00	$ 10.20
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-UG-GO-DLD-U-G-F	$ 21.00	$ 20.10
VMware	U.S. Federal VMware AirWatch Content Locker View Perpetual: 1 Device	V-UG-GO-DLD-U-P-F	$ 22.00	$ 20.39
VMware	U.S. Federal VMware Identity Manager Advanced Edition 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-UG-GO-OPL-D-G-F	$ 10.00	$ 9.57
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subs	V-UG-GO-OPL-D-P-F	$ 11.00	$ 10.53
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic	V-UG-GO-PLL-D-F	$ 22.00	$ 21.50
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic	V-UG-GO-SSS-D-G-F	$ 5.00	$ 4.89
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic	V-UG-GO-SSS-D-P-F	$ 6.00	$ 5.86
VMware	U.S. Federal Production Support/Subscription for VMware Identity Manager Advanced Edition: 1 User for 3 years	V-UG-GY-CLD-D-G-F	$ 66.00	$ 63.17
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Management Suite for Rugged Devices: 1 Device for 3 years	V-UG-GY-CLD-D-P-F	$ 69.50	$ 66.52
VMware	U.S. Federal VMware Identity Manager Advanced Edition 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-UG-GY-CLD-U-G-F	$ 132.00	$ 126.35
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Suppor	V-UG-GY-CLD-U-P-F	$ 138.50	$ 132.57
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-GY-DLD-D-G-F	$ 64.00	$ 59.32
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-GY-DLD-D-P-F	$ 69.50	$ 64.42
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-GY-DLD-U-G-F	$ 132.00	$ 122.36
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-GY-DLD-U-P-F	$ 138.50	$ 128.38
VMware	U.S. Federal VMware Identity Manager Advanced Edition 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-UG-GY-OPL-D-G-F	$ 66.00	$ 63.17
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subs	V-UG-GY-OPL-D-P-F	$ 69.50	$ 66.52
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - Dedicated Cloud (Includes SaaS Ba	V-UG-GY-PLL-D-F	$ 88.00	$ 86.01
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - Dedicated Cloud (Includes SaaS Ba	V-UG-GY-SSS-D-G-F	$ 18.00	$ 17.59
VMware	U.S. Federal Upgrade: VMware AirWatch from Mobile Device & Airwatch Content Locker View to Yellow Management Suite Subscription - Dedicated Clo	V-UG-GY-SSS-D-P-F	$ 22.00	$ 21.50
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-MU-CLD-U-G-F	$ 56.00	$ 51.91
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-MU-CLD-U-P-F	$ 58.50	$ 54.23
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-MU-DLD-U-G-F	$ 69.50	$ 64.42
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-MU-DLD-U-P-F	$ 71.50	$ 66.28
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic Su	V-UG-MU-PLL-U-F	$ 55.00	$ 53.75

VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - On Premise (Includes Basic Support/S	V-UG-MU-SSS-U-G-F	$ 12.00	$ 11.73
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - Shared Cloud (Includes SaaS Basic Sup	V-UG-MU-SSS-U-P-F	$ 14.00	$ 13.68
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Content Locker Collaborate: 1 Device for 1 year	V-UG-MY-CLD-D-G-F	$ 33.00	$ 31.59
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/S	V-UG-MY-CLD-D-P-F	$ 35.00	$ 33.50
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-UG-MY-DLD-D-G-F	$ 20.00	$ 19.14
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Content Locker View: 1 Device for 1 year	V-UG-MY-DLD-D-P-F	$ 22.00	$ 20.39
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Content Locker Collaborate: 1 Device for 1 year	V-UG-MY-OPL-D-G-F	$ 46.00	$ 44.03
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/S	V-UG-MY-OPL-D-P-F	$ 48.50	$ 46.42
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - On Premise (Includes Basic Suppor	V-UG-MY-PLL-D-F	$ 66.00	$ 64.50
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Yellow Management Suite Subscription - On Premise (Includes Basic Support	V-UG-MY-SSS-D-G-F	$ 14.00	$ 13.68
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - Shared Cloud (Includes SaaS Basic Sup	V-UG-MY-SSS-D-P-F	$ 17.00	$ 16.61
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Content Locker Collaborate: 1 Device for 3 years	V-UG-OB-CLD-D-G-F	$ 16.50	$ 15.79
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/S	V-UG-OB-CLD-D-P-F	$ 17.50	$ 16.75
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OB-CLD-U-G-F	$ 33.00	$ 31.59
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Sup	V-UG-OB-CLD-U-P-F	$ 35.00	$ 32.44
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-UG-OB-DLD-D-G-F	$ 16.50	$ 15.79
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Content Locker View: 1 Device for 1 year	V-UG-OB-DLD-D-P-F	$ 17.50	$ 16.22
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-OB-DLD-U-G-F	$ 33.00	$ 31.59
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Content Locker View: 1 Device for 3 years	V-UG-OB-DLD-U-P-F	$ 35.00	$ 32.44
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OB-OPL-D-G-F	$ 16.50	$ 15.79
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Sup	V-UG-OB-OPL-D-P-F	$ 17.50	$ 16.75
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Blue Management Suite Subscription - Dedicated Cloud (Includes SaaS Basi	V-UG-OB-PLL-D-F	$ 22.00	$ 21.50
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Blue Management Suite Subscription - Dedicated Cloud (Includes SaaS Basi	V-UG-OB-SSS-D-G-F	$ 5.00	$ 4.89
VMware	U.S. Federal Upgrade: VMware AirWatch Orange Management Suite to Yellow Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic Su	V-UG-OB-SSS-D-P-F	$ 6.00	$ 5.86
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-OU-CLD-U-G-F	$ 67.00	$ 62.11
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-UG-OU-CLD-U-P-F	$ 69.50	$ 64.42
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-OU-DLD-U-G-F	$ 80.50	$ 74.62
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OU-DLD-U-P-F	$ 82.50	$ 76.47
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - Shared Cloud (Includes SaaS Basic	V-UG-OU-PLL-U-F	$ 77.00	$ 75.25
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic S	V-UG-OU-SSS-U-G-F	$ 16.00	$ 15.64
VMware	U.S. Federal Upgrade: VMware AirWatch from Airwatch Content Locker View to Airwatch Content Locker Collaborate - Shared Cloud (Includes SaaS Basi	V-UG-OU-SSS-U-P-F	$ 19.00	$ 18.57
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Content Locker Collaborate: 1 Device for 3 years	V-UG-OY-CLD-D-G-F	$ 56.00	$ 53.60
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OY-CLD-D-P-F	$ 56.00	$ 51.91
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscript	V-UG-OY-CLD-U-G-F	$ 111.00	$ 106.25
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscriptio	V-UG-OY-CLD-U-P-F	$ 116.50	$ 107.99
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-OY-DLD-D-G-F	$ 56.00	$ 53.60
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OY-DLD-D-P-F	$ 58.50	$ 54.23
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-OY-DLD-U-G-F	$ 111.00	$ 106.25
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Content Locker View: 1 Device for 3 years	V-UG-OY-DLD-U-P-F	$ 116.50	$ 107.99
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-OY-OPL-D-G-F	$ 56.00	$ 53.60
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Sup	V-UG-OY-OPL-D-P-F	$ 58.50	$ 55.99
VMware	U.S. Federal Upgrade: VMware AirWatch from Airwatch Content Locker View to Airwatch Content Locker Collaborate - Dedicated Cloud (Includes SaaS B	V-UG-OY-PLL-D-F	$ 66.00	$ 64.50
VMware	U.S. Federal Upgrade: VMware AirWatch Orange Management Suite to Yellow Management Suite Subscription - Dedicated Cloud (Includes SaaS Basic Su	V-UG-OY-SSS-D-G-F	$ 14.00	$ 13.68
VMware	U.S. Federal Upgrade: VMware AirWatch from Blue Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Product	V-UG-OY-SSS-D-P-F	$ 17.00	$ 16.61
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-TU-CLD-U-G-F	$ 14.50	$ 13.44
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping Perpetual: 1 Device	V-UG-TU-CLD-U-P-F	$ 14.50	$ 13.44
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscriptic	V-UG-TU-DLD-U-G-F	$ 27.50	$ 25.49
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-TU-DLD-U-P-F	$ 27.50	$ 25.49
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscriptic	V-UG-TU-PLL-U-F	$ 22.00	$ 21.50

VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subs	V-UG-TU-SSS-U-G-F	$ 5.00	$ 4.89
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subs	V-UG-TU-SSS-U-P-F	$ 6.00	$ 5.86
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate Perpetual: 1 Device	V-UG-VC-CLD-D-G-F	$ 21.00	$ 20.10
VMware	U.S. Federal VMware AirWatch Management Suite for Rugged Devices 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Suppor	V-UG-VC-CLD-D-P-F	$ 22.00	$ 21.06
VMware	U.S. Federal VMware AirWatch Content Locker Collaborate 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-UG-VC-DLD-D-G-F	$ 21.00	$ 20.10
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-VC-DLD-D-P-F	$ 22.00	$ 20.39
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Orange Management Suite Subscription - Shared Cloud (Includes SaaS Basic	V-UG-VC-PLL-D-F	$ 33.00	$ 32.25
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Yellow Management Suite Subscription - Shared Cloud (Includes SaaS Basic S	V-UG-VC-SSS-D-G-F	$ 7.00	$ 6.84
VMware	U.S. Federal Upgrade: VMware AirWatch from Green Management Suite to Blue Management Suite Subscription - On Premise (Includes Basic Support/S	V-UG-VC-SSS-D-P-F	$ 8.00	$ 7.82
VMware	U.S. Federal VMware AirWatch Content Locker View 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscription)	V-UG-VU-CLD-U-G-F	$ 33.00	$ 30.59
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Mobile Application Wrapping: 1 Device for 1 year	V-UG-VU-CLD-U-P-F	$ 34.00	$ 31.52
VMware	U.S. Federal VMware AirWatch Content Locker View 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-UG-VU-DLD-U-G-F	$ 46.00	$ 42.64
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Mobile Application Wrapping: 1 Device for 1 year	V-UG-VU-DLD-U-P-F	$ 47.50	$ 44.03
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subs	V-UG-VU-PLL-U-F	$ 33.00	$ 32.25
VMware	U.S. Federal VMware AirWatch Cloud - Dedicated Environment for Perpetual Licenses: 1 Device for 1 year	V-UG-VU-SSS-U-G-F	$ 7.00	$ 6.84
VMware	U.S. Federal VMware AirWatch Cloud - Shared Environment for Perpetual Licenses: 1 Device for 1 year	V-UG-VU-SSS-U-P-F	$ 8.00	$ 7.82
VMware	U.S. Federal VMware AirWatch Content Locker View 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-UG-YU-CLD-U-G-F	$ 122.00	$ 113.09
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-UG-YU-CLD-U-P-F	$ 127.50	$ 118.19
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscriptic	V-UG-YU-DLD-U-G-F	$ 135.50	$ 125.60
VMware	U.S. Federal VMware AirWatch Mobile Application Wrapping 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscri	V-UG-YU-DLD-U-P-F	$ 141.00	$ 130.70
VMware	U.S. Federal Upgrade: VMware AirWatch from Mobile Device & Airwatch Content Locker View to Yellow Management Suite Subscription - On Premise (I	V-UG-YU-PLL-U-F	$ 143.00	$ 139.76
VMware	U.S. Federal Upgrade: VMware AirWatch from Mobile Device & Airwatch Content Locker View to Yellow Management Suite Subscription - Shared Cloud	V-UG-YU-SSS-U-G-F	$ 30.00	$ 29.32
VMware	U.S. Federal Upgrade: VMware AirWatch from Orange Management Suite to Blue Management Suite. Subscription - Shared Cloud (Includes SaaS Basic S	V-UG-YU-SSS-U-P-F	$ 36.00	$ 35.18
VMware	U.S. Federal Basic Support/Subscription for VMware Socialcast: 1 User for 1 year	V-VID-CLD-D-2G-F	$ 59.00	$ 56.47
VMware	U.S. Federal Production Support/Subscription for VMware Socialcast: 1 User for 3 years	V-VID-CLD-D-2P-F	$ 61.00	$ 58.39
VMware	U.S. Federal Production Support/Subscription for VMware Socialcast: 1 User for 1 year	V-VID-CLD-D-3G-F	$ 82.00	$ 78.49
VMware	U.S. Federal VMware Socialcast 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-CLD-D-3P-F	$ 85.00	$ 81.36
VMware	U.S. Federal VMware Socialcast Perpetual: 1 User	V-VID-CLD-D-G-F	$ 31.00	$ 29.67
VMware	U.S. Federal Basic Support/Subscription for VMware Socialcast: 1 User for 3 years	V-VID-CLD-D-P-F	$ 32.00	$ 30.63
VMware	U.S. Federal VMware AirWatch Printer 3-year Subscription - Shared Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-CLD-U-2G-F	$ 115.00	$ 110.08
VMware	U.S. Federal VMware AirWatch Printer 3-year Subscription - Shared Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-CLD-U-2P-F	$ 119.00	$ 113.90
VMware	U.S. Federal VMware AirWatch Printer 1-year Subscription - Shared Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-CLD-U-3G-F	$ 162.00	$ 155.06
VMware	U.S. Federal VMware AirWatch Printer 1-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-CLD-U-3P-F	$ 167.00	$ 159.85
VMware	U.S. Federal VMware AirWatch Printer 2-year Subscription - Shared Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-CLD-U-G-F	$ 61.00	$ 58.39
VMware	U.S. Federal VMware AirWatch Printer 2-year Subscription - Shared Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-CLD-U-P-F	$ 63.00	$ 60.30
VMware	U.S. Federal VMware Socialcast 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-DLD-D-2G-F	$ 81.00	$ 77.53
VMware	U.S. Federal VMware Socialcast 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-DLD-D-2P-F	$ 83.00	$ 79.45
VMware	U.S. Federal VMware Socialcast 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-DLD-D-3G-F	$ 114.00	$ 109.12
VMware	U.S. Federal VMware Socialcast 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-DLD-D-3P-F	$ 117.00	$ 111.99
VMware	U.S. Federal VMware Socialcast 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-DLD-D-G-F	$ 43.00	$ 41.16
VMware	U.S. Federal VMware Socialcast 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-DLD-D-P-F	$ 44.00	$ 42.12
VMware	U.S. Federal VMware AirWatch Printer 3-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-DLD-U-2G-F	$ 160.00	$ 153.15
VMware	U.S. Federal VMware AirWatch Printer 3-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-DLD-U-2P-F	$ 164.00	$ 156.98
VMware	U.S. Federal VMware AirWatch Printer 1-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-DLD-U-3G-F	$ 225.00	$ 215.37
VMware	U.S. Federal VMware AirWatch Mobile Device Perpetual: 1 Device	V-VID-DLD-U-3P-F	$ 230.00	$ 220.15
VMware	U.S. Federal VMware AirWatch Printer 2-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-DLD-U-G-F	$ 85.00	$ 81.36
VMware	U.S. Federal VMware AirWatch Printer 2-year Subscription - Dedicated Cloud for 1 device (Includes SaaS Production Support/Subscription)	V-VID-DLD-U-P-F	$ 87.00	$ 83.27
VMware	U.S. Federal VMware Socialcast 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-OPL-D-2G-F	$ 36.00	$ 34.46
VMware	U.S. Federal VMware Socialcast 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-OPL-D-2P-F	$ 38.00	$ 36.37

VMware	U.S. Federal VMware Socialcast 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-OPL-D-3G-F	$ 51.00	$ 48.82
VMware	U.S. Federal VMware AirWatch Printer Perpetual: 1 Device	V-VID-OPL-D-3P-F	$ 53.00	$ 50.73
VMware	U.S. Federal VMware Socialcast 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-VID-OPL-D-G-F	$ 19.00	$ 18.19
VMware	U.S. Federal VMware Socialcast 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-VID-OPL-D-P-F	$ 20.00	$ 19.14
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-VID-PLL-D-F	$ 30.00	$ 28.72
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Printer: 1 Device for 1 year	V-VID-PLL-U-F	$ 60.00	$ 57.43
VMware	U.S. Federal VMware AirWatch Teacher Tools 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-VID-SSS-D-3G-F	$ 15.84	$ 15.16
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-VID-SSS-D-3P-F	$ 21.12	$ 20.22
VMware	U.S. Federal VMware AirWatch Teacher Tools 3-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-VID-SSS-D-G-F	$ 6.00	$ 5.74
VMware	U.S. Federal VMware AirWatch Teacher Tools 1-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-VID-SSS-D-P-F	$ 8.00	$ 7.66
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Printer: 1 Device for 3 years	V-VID-SSS-U-3G-F	$ 34.32	$ 32.85
VMware	U.S. Federal VMware AirWatch Printer 1-year Subscription - Shared Cloud for 1 device (Includes SaaS Basic Support/Subscription)	V-VID-SSS-U-3P-F	$ 39.60	$ 37.90
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Printer: 1 Device for 1 year	V-VID-SSS-U-G-F	$ 13.00	$ 12.44
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Printer: 1 Device for 3 years	V-VID-SSS-U-P-F	$ 15.00	$ 14.36
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Green Management Suite: 1 User for 1 year	V-YMS-CLD-D-2G-F	$ 211.00	$ 201.96
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Green Management Suite: 1 User for 3 years	V-YMS-CLD-D-2P-F	$ 220.00	$ 210.58
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Green Management Suite: 1 User for 1 year	V-YMS-CLD-D-3G-F	$ 296.00	$ 283.32
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-CLD-D-3P-F	$ 309.00	$ 295.77
VMware	U.S. Federal VMware AirWatch Green Management Suite Perpetual: 1 User	V-YMS-CLD-D-G-F	$ 112.00	$ 107.20
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Green Management Suite: 1 User for 3 years	V-YMS-CLD-D-P-F	$ 117.00	$ 111.99
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-YMS-CLD-U-2G-F	$ 420.00	$ 402.02
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscripti	V-YMS-CLD-U-2P-F	$ 439.00	$ 420.20
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscripti	V-YMS-CLD-U-3G-F	$ 589.00	$ 563.78
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-YMS-CLD-U-3P-F	$ 616.00	$ 589.62
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-YMS-CLD-U-G-F	$ 223.00	$ 213.45
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Shared Cloud for 1 Device (Includes SaaS Production Support/Subscripti	V-YMS-CLD-U-P-F	$ 233.00	$ 223.02
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-DLD-D-2G-F	$ 234.00	$ 223.98
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-YMS-DLD-D-2P-F	$ 243.00	$ 232.59
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-YMS-DLD-D-3G-F	$ 328.00	$ 313.95
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-DLD-D-3P-F	$ 341.00	$ 326.40
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-DLD-D-G-F	$ 124.00	$ 118.69
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Shared Cloud for 1 User (Includes SaaS Production Support/Subscription)	V-YMS-DLD-D-P-F	$ 129.00	$ 123.48
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-YMS-DLD-U-2G-F	$ 465.00	$ 445.09
VMware	U.S. Federal VMware AirWatch Orange Management Suite 3-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-YMS-DLD-U-2P-F	$ 484.00	$ 463.27
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-YMS-DLD-U-3G-F	$ 653.00	$ 625.04
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-YMS-DLD-U-3P-F	$ 679.00	$ 649.92
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Basic Support/Subscription	V-YMS-DLD-U-G-F	$ 247.00	$ 236.42
VMware	U.S. Federal VMware AirWatch Orange Management Suite 2-year Subscription - Dedicated Cloud for 1 Device (Includes SaaS Production Support/Subscr	V-YMS-DLD-U-P-F	$ 257.00	$ 245.99
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-OPL-D-2G-F	$ 188.00	$ 179.95
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscripti	V-YMS-OPL-D-2P-F	$ 198.00	$ 189.52
VMware	U.S. Federal VMware View: Install Configure Manage [V5.0] - Extra Person	EDU-VICM5-XP-F	$ 2,750.00	$ 2,687.66
VMware	Application Virtualization with VMware ThinApp [V5.0] - Open Enrollment	EDU-THINAPP5-OE-F	$ 825.00	$ 806.30
VMware	Application Virtualization with VMware ThinApp [V5.0] - On Site	EDU-THINAPP5-OS-F	$ 6,875.00	$ 6,719.14
VMware	Application Virtualization with VMware ThinApp [V5.0] - Extra Person	EDU-THINAPP5-XP-F	$ 688.00	$ 672.40
VMware	VMware vCloud Automation Center: Extensibility and Advanced Administration [V5 2] - Open Enrollment	EDU-VCACEXT52-OE-F	$ 1,645.00	$ 1,607.71
VMware	VMware vCloud Automation Center: Extensibility and Advanced Administration [V5 2] - Onsite	EDU-VCACEXT52-OS-F	$ 13,750.00	$ 13,438.29
VMware	VMware vCloud Automation Center: Extensibility and Advanced Administration [V5 2] - Extra Person	EDU-VCACEXT52-XP-F	$ 1,375.00	$ 1,343.83
VMware	U.S. Federal Using VMware vCenter Lab Manager - Open Enrollment	EDU-LM4-OE-F	$ 825.00	$ 806.30
VMware	U.S. Federal Using VMware vCenter Lab Manager - On Site	EDU-LM4-OS-F	$ 6,875.00	$ 6,719.14

VMware	U.S. Federal Using VMware vCenter Lab Manager - Extra Person	EDU-LM4-XP-F	$ 688.00	$ 672.40
VMware	U.S. Federal Consulting & Training Credits - Prepaid Services PSO Credit 1-150	SVC-CR-0-F	$ 100.00	$ 97.73
VMware	U.S. Federal Restricted SKU: Consulting & Training Credits. Prepaid Services. PSO Credit 1-150.	SVC-CR-0-SSS-F	$ 100.00	$ 97.73
VMware	U.S. Federal Consulting & Training Credits - Prepaid Services PSO Credit 151-600	SVC-CR-10-F	$ 90.00	$ 87.96
VMware	U.S. Federal Restricted SKU: Consulting & Training Credits. Prepaid Services. PSO Credit 151-600.	SVC-CR-10-SSS-F	$ 90.00	$ 87.96
VMware	U.S. Federal Consulting & Training Credits - Prepaid Services PSO Credit 601-1200	SVC-CR-15-F	$ 85.00	$ 83.07
VMware	U.S. Federal Restricted SKU: Consulting & Training Credits. Prepaid Services. PSO Credit 601-1200.	SVC-CR-15-SSS-F	$ 85.00	$ 83.07
VMware	U.S. Federal Consulting & Training Credits - Prepaid Services PSO Credit 1201+	SVC-CR-20-F	$ 80.00	$ 78.19
VMware	U.S. Federal Restricted SKU: Consulting & Training Credits. Prepaid Services. PSO Credit 1201+	SVC-CR-20-SSS-F	$ 80.00	$ 78.19
VMware	U.S. Federal Socialcast Configuration and Integration Design - On Premises	CON-SC-CIDOP-FF-F	$ 7,500.00	$ 7,329.97
VMware	U.S. Federal Socialcast Assigned Client Account Representative	CON-SC-ACAR-FF-F	$ 30,000.00	$ 29,319.90
VMware	U.S. Federal Socialcast Reach System Integration	CON-SC-RSI-FF-F	$ 3,500.00	$ 3,420.65
VMware	U.S. Federal Socialcast Single Sign On Configuration	CON-SC-SSOC-FF-F	$ 5,000.00	$ 4,886.65
VMware	U.S. Federal Socialcast Custom Theme Integration	CON-SC-CTI-FF-F	$ 3,500.00	$ 3,420.65
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscripti	V-YMS-OPL-D-3G-F	$ 264.00	$ 252.70
VMware	U.S. Federal VMware AirWatch Orange Management Suite Perpetual: 1 Device	V-YMS-OPL-D-3P-F	$ 278.00	$ 266.10
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Basic Support/Subscription)	V-YMS-OPL-D-G-F	$ 100.00	$ 95.72
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - Dedicated Cloud for 1 User (Includes SaaS Production Support/Subscripti	V-YMS-OPL-D-P-F	$ 105.00	$ 100.50
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-YMS-PLL-D-F	$ 130.00	$ 124.43
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Orange Management Suite: 1 Device for 1 year	V-YMS-PLL-U-F	$ 260.00	$ 248.87
VMware	U.S. Federal VMware AirWatch Green Management Suite 2-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-YMS-SSS-D-3G-F	$ 71.28	$ 68.23
VMware	U.S. Federal VMware AirWatch Green Management Suite 3-year Subscription - On Premise for 1 Device (Includes Production Support/Subscription)	V-YMS-SSS-D-3P-F	$ 87.12	$ 83.39
VMware	U.S. Federal VMware AirWatch Green Management Suite 1-year Subscription - On Premise for 1 Device (Includes Basic Support/Subscription)	V-YMS-SSS-D-G-F	$ 27.00	$ 25.84
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Orange Management Suite: 1 Device for 3 years	V-YMS-SSS-D-P-F	$ 33.00	$ 31.59
VMware	U.S. Federal VMware AirWatch Orange Management Suite 1-year Subscription - Shared Cloud for 1 Device (Includes SaaS Basic Support/Subscription)	V-YMS-SSS-U-3G-F	$ 145.20	$ 138.98
VMware	U.S. Federal Production Support/Subscription for VMware AirWatch Orange Management Suite: 1 Device for 1 year	V-YMS-SSS-U-3P-F	$ 171.60	$ 164.25
VMware	U.S. Federal Basic Support/Subscription for VMware AirWatch Orange Management Suite: 1 Device for 3 years	V-YMS-SSS-U-G-F	$ 55.00	$ 52.64
VMware	U.S. Federal Upgrade: VMware AirWatch from Mobile Device & Airwatch Content Locker View to Yellow Management Suite Subscription - On Premise (I	V-YMS-SSS-U-P-F	$ 65.00	$ 62.22
VMware	U.S. Federal Upgrade: VMware AirWatch from Mobile Device & Airwatch Content Locker View to Yellow Management Suite Subscription - Shared Cloud	V-YMS-WKS-MF-2M-SSS-F	$ 10.84	$ 10.59
VMware	U.S. Federal Upgrade: VMware AirWatch from Airwatch Content Locker View to Airwatch Content Locker Collaborate Subscription - Shared Cloud (Includ	V-YMS-WKS-MF-3Y-SSS-F	$ 171.60	$ 167.71
VMware	U.S. Federal VMware vCloud Air Accelerator	V-YMS-WKS-MF-SSS-F	$ 65.00	$ 63.53
VMware	U.S. Federal VMware Desktop Viritualization Health Check	CON-VCA-ACL-F	$ 19,035.00	$ 18,603.48
		CON-VDI-HC-S-F	$ 24,406.60	$ 23,853.30

carahsoft

CARAHSOFT'S RESPONSE TO THE

State of Utah
NASPO ValuePoint

REQUEST FOR PROPOSAL

NASPO ValuePoint Master Agreement for Cloud Solutions

SOLICITATION NO. CH16012

Technical Proposal

Thursday
March 10, 2015

CARAHSOFT TECHNOLOGY CORP.
1860 MICHAEL FARADAY DRIVE, SUITE 100
RESTON, VA 20190

888.66.CARAH | WWW.CARAHSOFT.COM

carahsoft.

March 10, 2015

State of Utah Division of Purchasing
3150 State Office Building
Capitol Hill
Salt Lake City, Utah 84114

Re: Carahsoft's Response to the State of Utah's Request for Proposal for NASPO ValuePoint Master Agreement for Cloud Solutions, Solicitation # CH16012.

Dear Mr. Hughes,

Carahsoft Technology Corp. appreciates the opportunity to respond to the State of Utah's Request for Proposals/Q/Information for Project Description.

5.2.1	Carahsoft Technology Corporation understands that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.
5.2.2	When writing this response Carahsoft utilized the OEMs being proposed as a part of this response to assist in preparing this response. Staff responsible for creating this proposal include Robert R. Moore – Vice President, Jack Dixon – Contract Specialist, & David Holl – Proposal Coordinator.
5.2.3	Carahsoft Technology Corporation is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.
5.2.4	Carahsoft Technology Corporation acknowledges that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.
5.2.5	Carahsoft Technology Corporation is including an all-encompassing list of solutions in this response which covers the SaaS, PaaS, & IaaS categories. Services completion/deployment will vary based on manufacturer but will utilize either the manufacturers own integration policies and procedures or a third party subcontractor specializing in servicing the manufacturers' specific solution.
5.2.6	Carahsoft can provide varying levels of data risk support based on customer requirements, manufacturer, and solution type. Please see our response to Attachment H for further detail.

Please feel free to contact me directly at 703.871.8504/Robert.Moore@carahsoft.com or Jack Dixon at 703.230.7545/Jack.Dixon@carahsoft.com with any questions or communications that will assist the Agency in the evaluation of our response. This proposal is valid for 90 days from the date of submission.

Thank you for your time and consideration.

Sincerely,

Robert R. Moore
Vice President

TABLE OF CONTENTS

RFP Signature Page 1
Acknowledgement of Amendments 4
Executive Summary 6
Prime Contractor: Carahsoft Technology Corp. 6
Mandatory Minimums 8
Business Profile 12
Organizations Profile 21
Technical Response 23
Confidential, Protected, or Proprietary Information 183
Exceptions and/or Additions to the Standard Terms and Conditions 185
In Summary 186
Supplemental Information 187

RFP SIGNATURE PAGE

The Lead State's Request for Proposal Signature Page completed and signed. See Section 5.1 of the RFP.

Please find below Carahsoft's RFP Signature Page below.

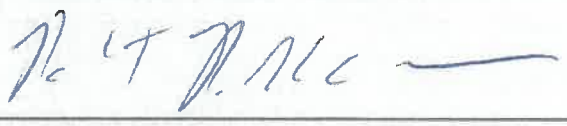
State of Utah Vendor Information Form

Legal Company Name (include d/b/a if applicable) Carahsoft Technology Corporation	Federal Tax Identification Number 52-2189693	State of Utah Sales Tax ID Number 9721863-0143	
Ordering Address 1860 Michael Faraday Drive, Suite 100	City Reston	State VA	Zip Code 20190
Remittance Address (if different from ordering address) 1860 Michael Faraday Drive, Suite 100	City Reston	State VA	Zip Code 20190
Type ☐ Proprietorship ☐ Partnership ☐ Government ☒ For-Profit Corporation ☐ Non-Profit Corporation	Company Contact Person Robert R. Moore		
Telephone Number (include area code) 703.871.8504	Fax Number (include area code) 703.871.8505		
Company's Internet Web Address www.carahsoft.com	Email Address robert.moore@carahsoft.com		
Offeror's Authorized Representative's Signature [signature]			
Type or Print Name Robert R. Moore			
Position or Title of Authorized Representative Vice President			
Date: 3/10/2016			

State of Utah
Request for Proposal

Legal Company Name (include d/b/a if applicable) Carahsoft Technology Corporation	Federal Tax Identification Number 52-2189693	State of Utah Sales Tax ID Number 9721863-0143	
Ordering Address 1860 Michael Faraday Drive, Suite 100	City Reston	State VA	Zip Code 20190
Remittance Address (if different from ordering address) 1860 Michael Faraday Drive, Suite 100	City Reston	State VA	Zip Code 20190
Type [X] Corporation [ ] Partnership [ ] Proprietorship [ ] Government	Company Contact Person Robert R. Moore		
Telephone Number (include area code) 703.871.8504	Fax Number (include area code) 703.871.8505		
Company's Internet Web Address www.Carahsoft.com	Email Address Robert.Moore@Carahsoft.com		
Discount Terms (for prompt payment discounts): Not Applicable	Days Required for Delivery After Receipt of Order (see attached for any required minimums)		

By submitting a proposal in response to this RFP, the Offeror acknowledges and agrees that the specifications, terms and conditions, or other elements of the RFP are not ambiguous, confusing, contradictory, unduly restrictive, erroneous, or anticompetitive. The Offeror further acknowledges that it has read this RFP, along with any attached or referenced documents, and this document, including the General Provisions.

Offeror's Authorized Representative's Signature 	Date 3/10/2016
Type or Print Name Robert R. Moore	Position or Title Vice President

NOTICE

ACKNOWLEDGEMENT OF AMENDMENTS

Please find below Carahsoft's Acknowledgement of Amendments.

ACKNOWLEDGEMENT OF AMENDMENTS TO RFP (SOLICITATION CH16012)

This attachment represents that the Offeror has read, reviewed, and understands the totality of Solicitation CH16012, including the final RFP document posted on February 10, 2016.

By signing below, the Offeror attest to reviewing the documents listed above.

Carahsoft Technology Corporation
Offeror

Representative Signature

EXECUTIVE SUMMARY

The one or two page executive summary is to briefly describe the Offeror's Proposal. This summary should highlight the major features of the Proposal. It must indicate any requirements that cannot be met by the Offeror. The Lead State should be able to determine the essence of the Proposal by reading the executive summary. See Section 5.4 of the RFP.

Prime Contractor: Carahsoft Technology Corp.

Carahsoft Technology Corporation understands that the State of Utah & NASPO ValuePoint is seeking a Master Agreement for Cloud Solutions.

Carahsoft has assembled a team from our vast portfolio of over 200 hundred vendors that includes our premiere network of cloud solutions, resellers, and subcontractors as the best solution to meet the State of Utah's requirements. The intent of our proposal is to deliver the highest value proposition at the lowest possible cost to the State of Utah, NASPO ValuePoint, & all participating entities for the acquisition of cloud solutions. Carahsoft understands the need for high quality cloud based service providers that have the ability to provide a menu of cloud solution offerings. Carahsoft's superior contract management and network of Cloud Solution Providers will ultimately increase the State & Participating Entities overall efficiency, reduce costs, improve operational scalability, provide business continuity, increase collaboration efficiencies, and all for expanded flexibility.

Carahsoft Technology Corp. is an IT solutions provider delivering best-of-breed hardware, software, and support solutions to federal, state and local government agencies since 2004. Carahsoft has built a reputation as a customer-centric real-time organization with unparalleled experience and depth in government sales, marketing, and contract program management. This experience has enabled Carahsoft to achieve the top spot in leading software license GSA resellers.

VENDOR RELATIONSHIPS – Just as each state, territory, and participating entity is unique in how they employ cloud solutions, Carahsoft's cloud offering follows a unique business model focusing on providing superior sales and marketing execution, a track record of success, high integrity, and a focus on strategic vendor relationships.

PROVEN EXECUTION (Growth and Experience of Sales) – Carahsoft has been supporting the IT needs of Government and Education Customers for more than 12 years. Our Public Sector Sales Team supports the Government, Education, and Healthcare vertical markets and is an enormous component of Carahsoft's ongoing and continued growth. In 2014, Carahsoft had revenues of over $2B in the public sector market. Our State & Local Government Sales Force is solely dedicated to supporting the unique needs of Higher Education, K- 12 Schools, State Government, and Local Government customers.

CONTRACT VEHICLES – Over the past ten years Carahsoft has acquired and maintained a wide variety of purchasing contract vehicles for agencies at the state, local, and federal levels. Carahsoft holds statewide contracts in many states across the country, and we have a great deal of experience with contract transitions. Associated with all contracts are dedicated and experienced contract management resources.

Carahsoft has leveraged its vast contracting experience and extended it to quoting and order management. Carahsoft seamlessly generates quotes within 30 minutes or less and processed over 56,000 orders in 2014 that were each completed the same day received.

GROWTH & STABILITY – Carahsoft has continued to show impressive growth year after year, turning annual revenue from $3.4 million in our first year in 2004 to $1.065 billion in 2011, $1.465 billion in 2012, $1.8 billion in 2013, and $2.45 billion in 2014. In September of 2014, 7,501 orders were processed worth over $626 million. We are a stable, conservative, and profitable company and have received numerous accolades including the 2013 GovCon Government Contractor of the Year Award in the greater than $300M revenue category. Carahsoft was also recognized in the following areas:

- Largest GSA Schedule 70 Contract holder for software
- 7th of the Washington Business Journal's 100 Largest Private Companies List for 2014
- 2012 Federal 100 Winner, Craig P. Abod, President and CEO
- 2013 Federal 100 Winner, John Lee, Vice President of Cloud Services

As a part of this response Carahsoft has utilized multiple Cloud Solution Vendors, covering all of the Cloud Solution Categories; SaaS, IaaS, PaaS. Carahsoft's strong vendor relationships and partner ecosystem have created an efficient and cost effective response which encompasses all vendor solutions into a single, easy to utilize vehicle. While the technical requirements of each solution vary, Carahsoft strives to consolidate these specifications and responses into a cohesive unit.

MANDATORY MINIMUMS

This section should constitute the Offeror's point-by-point response to each item described in Section 5 of the RFP, except 5.1 (Signature Page) and 5.4 (Executive Summary). An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 5 of the RFP.

5.1 – Signature Page

Proposals must be submitted with a vendor information form, located on Bidsync as an attachment to the RFP, which must contain an ORIGINAL HANDWRITTEN signature executed in INK OR AN ELECTRONIC SIGNATURE, and be returned with the Offeror's proposal.

Please find Carahsoft's Signature Page completed above.

5.2 – Cover Letter

Proposals must include a cover letter on official letterhead of the Offeror. The cover letter must identify the RFP Title and number, and must be signed by an individual authorized to commit the Offeror to the work proposed. In addition, the cover letter must include:

5.2.1 A statement indicating the Offeror's understanding that they may be required to negotiate additional terms and conditions, including additional administrative fees, with Participating Entities when executing a Participating Addendum.

5.2.2 A statement naming the firms and/or staff responsible for writing the proposal.

5.2.3 A statement that Offeror is not currently suspended, debarred or otherwise excluded from federal or state procurement and non-procurement programs.

5.2.4 A statement acknowledging that a 0.25% NASPO ValuePoint Administrative Fee and any Participating Entity Administrative fee will apply to total sales for the Master Agreement(s) awarded from the RFP.

5.2.5 A statement identifying the service model(s) (SaaS, IaaS, and/or PaaS) and deployment model(s) that it is capable of providing under the terms of the RFP. See Attachment C for a determination of each service model subcategory. The services models, deployment models and risk categories can be found in the Scope of Services, Attachment D. Note: Multiple service and/or deployment model selection is permitted, and at least one service model must be identified. See Attachment H.

5.2.6 A statement identifying the data risk categories that the Offeror is capable of storing and securing. See Attachment D and Attachment H.

Please find above Carahsoft's Cover Letter addressing these requirements.

5.3 – Acknowledgement of Amendments

If the RFP is amended, the Offeror must acknowledge each amendment with a signature on the acknowledgement form provided with each amendment. Failure to return a signed copy of each amendment acknowledgement form with the proposal may result in the proposal being found non-responsive.

Carahsoft acknowledges all amendments. Also please find below Carahsoft's Acknowledgement of Amendments form completed.

5.4 – Executive Summary

Offerors must provide an Executive Summary of its proposal. An Executive Summary should highlight the major features of an Offeror's proposal. Briefly describe the proposal in no more than three (3) pages. The evaluation committee should be able to determine the essence of the proposal by reading the Executive Summary. Any requirements that cannot be met by the Offeror must be included.

Please find above Carahsoft's Executive Summary addressing these requirements.

5.5 – General Requirements

5.5.1 Offeror must agree that if awarded a contract it will provide a Usage Report Administrator responsible for the quarterly sales reporting described the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

Carahsoft agrees that if awarded a contract they will provide a Usage Report Administrator responsible for quarterly sales reporting described in the Master Agreement Terms and Conditions, and if applicable Participating Addendums.

5.5.2 Offeror must provide a statement that it agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading an Offeror's ordering instructions, if awarded a contract.

Carahsoft agrees to cooperate with NASPO ValuePoint and SciQuest (and any authorized agent or successor entity to SciQuest) with uploading Carahsoft's ordering instructions, if awarded a contract.

5.5.3 Offeror must at a minimum complete, provide, and maintain a completed CSA STAR Registry Self-Assessment. Offeror must either submit a completed The Consensus Assessments Initiative Questionnaire (CAIQ), Exhibit 1 to Attachment B, or submit a report documenting compliance with Cloud Controls Matrix (CCM), Exhibit 2 to Attachment B. Offeror must also represent and warrant the accuracy and currency of the information on the completed. Offerors are encouraged to complete and submit both exhibits to Attachment B.

For ease of access and evaluation, Carahsoft has provided these Assessment documents under separate cover. All copies have been submitted electronically per the instructions of the RFP. Please note that specific assessments have been labeled as confidential- additional information is provided in the Confidential, Protected, or Proprietary Information section.

5.5.4 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

SERVICE LEVEL FRAMEWORK

The service levels ("Service Levels") applicable to the Services specified in Sections 1 and 2 are set forth in Schedule B to this SD ("Service Levels for Cloud Platform Services"). The framework that governs all Service Levels is set forth in this Section.

Commencement of Service Levels

Commencing thirty (30) days from the Service Start Date (as set forth in the applicable Order Form), Virtustream's performance of the Services will meet each applicable Service Level. If Virtustream's performance of the Services does not meet the applicable Service Level, then Virtustream will use commercially reasonable efforts to restore its performance to meet such Service Level.

Service Level Reports

Service Levels will be calculated and measured monthly by Virtustream on a calendar month basis and reported each month for the previous month. The reports will be provided to Customer by the tenth (10th) working day of the month following that to which such report relates, commencing on the second (2nd) month following the Service Start Date and each month thereafter. The monthly service level report will contain at least the following items: (i) Uptime statistics for the month concerned; (ii) an analysis of reported incidents over the previous month, broken down by type for discussion; (iii) action plans for items giving rise to concern; (iv) comments and observations on any issues arising from Virtustream's performance monitoring activities; (v) recommendations on service delivery strategies to maintain or enhance the service level; and (vi) review of general business requirements ("Service Level Report"). Cloud Platform Services (CPS) has its own specific service levels as described in this document. Cloud Cover Services (CCS) has service levels that pertain to the CCS offerings and are reported separately. Not all Virtustream customers have CCS but all Virtustream customers use CPS.

Service Level Review Meetings

Monthly Service Level review meetings will be conducted by Virtustream with Customer where the monthly Service Level report specified above will be discussed. If any of the Service Levels measured over the previous calendar month period is not achieved in that month, then Virtustream will include the steps taken to rectify the problem in the next monthly Service Level Report. In addition, the issue shall be an agenda topic for discussion at the next monthly service review meeting. Additionally, after restoring service or otherwise resolving any immediate problem as specified in this SD, if Virtustream fails to provide Services in accordance with the Service Levels, Virtustream shall:

a. Promptly investigate and report on the causes of such problem;

b. Provide a Root Cause Analysis of such failure as soon as practical after such failure or at Customer's request;

c. Correct such problem that is Virtustream's fault or responsibility, as soon as reasonably practicable and coordinate the correction of such problem if Virtustream does not have responsibility for the cause of such problem.

d. Advise Customer of the status of remedial efforts being undertaken with respect to such problem;

e. Demonstrate to Customer's reasonable satisfaction that the causes of such problem (that is Virtustream's fault or responsibility) have been or shall be corrected on a permanent basis; and

f. Take corrective actions to prevent any recurrence of such problem (that is Virtustream's fault or responsibility).

Root Cause Analysis

Promptly following Virtustream's failure to meet a Service Level, Virtustream will perform a root cause analysis to determine the reason for that failure. Upon Virtustream's determination of the cause of such failure, it will provide to Customer a preliminary report citing the cause of such failure. If Virtustream determines that the failure was due to Virtustream, an additional report will be provided that details the root causes of the failure, and which details any measures that should be taken to minimize the possibility that such failures will re-occur. Virtustream will correct the problem and use reasonable commercial efforts to minimize the re-occurrence of such failures.

Service Level Exceptions

Virtustream shall not be liable for any failure to meet the Service Levels, to the extent such failure was caused by one or more of the following:

a. A failure of Customer or any of its employees, agents or contractors (including any of Customer's third party service providers) to perform any of its responsibilities under this SD;

b. Any act or omission of Customer or any of its employees, agents or contractors (including Customer's third party service providers or other third parties acting on behalf of Customer);
c. Any hardware, software or other product of a third-party or Customer equipment;
d. Any failure of Customer to secure the proper access rights or maintenance and support services with respect to any component of the Services (e.g., hardware, software, network, maintenance) for which Virtustream does not bear operational responsibility;
e. Downtimes resulting from a Virtustream's scheduled maintenance windows;
f. Customer's reprioritization of the tasks to be performed by Virtustream where such reprioritization causes Virtustream to miss a Service Level;
g. Viruses; provided that the infected Virtustream-provided system had virus protection for which the virus protection software updates were up to date;
h. An election by Customer to purchase a base commitment that is not sufficient to run Customer's system (e.g., If a customer elects to size a µVM pool that is insufficient to run the designated workload);
i. Issues occurring outside of standard working hours (as defined for business level customers) — for which the Service Level Objectives (SLOs) do not apply;
j. Cloud Cover Services (CCS) offerings — for which the Service Level Objectives (SLOs) do not apply;
k. Resolution delays due to lack of client response and/or Customer provided credential based information;
l. Priority levels not agreed upon by both customer and supplier;
m. Claims of performance degradation not substantiated through Customer provided diagnostic testing results.

5.7 Recertification of Mandatory Minimums and Technical Specifications

Offeror must acknowledge that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in its proposal.

Carahsoft acknowledges that if awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the technical capabilities discussed in this proposal.

BUSINESS PROFILE

This section should constitute the Offeror's response to the items described in Section 6 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 6 of the RFP.

6.1 – Business Profile Provide a profile of your business including: year started, organizational structure, client base (including any focus by region, market sector, etc.), growth over the last three (3) years, number of employees, employee retention rates (specific for employees that may be associated with the services related to the RFP) over the last two (2) years, etc. Businesses must demonstrate a minimum of three (3) years of experience providing cloud solutions for large scale projects, including government experience, to be eligible for award.

Carahsoft Technology Corp. was started in Reston, Virginia in 2004. Carahsoft remains headquartered in Reston Virginia employing over 500 people that specifically support the Public Sector (Federal, State, Local, and Public Funded Educational Entities Nationwide within the United States.) Carahsoft has built a reputation as a customer focused organization with depth of experience in government sales, marketing, and contract program management. Carahsoft is one of the largest sellers of Cloud (including SaaS, PaaS, and IaaS) to U.S. the Public Sector.

Carahsoft's organizational structure allows for very focused and individualized support of any customer. The Executive Management team at Carahsoft is responsible for all aspects of day to day running of the organization. Reporting to the Executive Management Team are Directors. It is the Director's primary responsibility to oversee a particular technology area(s) and to monitor and manage all aspects of the staff, customers, and business within that area. An example of a Technology Area at Carahsoft is the VMware Virtualization practice. A host of technology offerings that use VMware at their core are supported by a single business unit overseen by a single Director that has reach back and access to the Executive Management staff. The Director's are then supported by a group of Team Leads. Each Team Lead Oversees a business area (typically defined by customer type (i.e. State Customers) or technology type (i.e. Virtual Desktop). Each team lead oversees a staff that is responsible for executing and managing the activities within that business unit.

At its' core, this organizational structure is lean and efficient, lacking layers of middle management, and empowering individuals with decision making capability in order to support all customers quickly an efficiently.

Carahsoft boasts an excellent employee retention rate. Specific benchmarks that we track include employee retention at 2 years of employment and 4 years of employment with rates of 65% and 90% respectively.

Carahsoft has been providing cloud solutions since opening its doors in 2004. US Public Sector entities have relied on Carahsoft to provide a wide variety of cloud technologies. Carahsoft serves as the cloud distributor and provides access to the core cloud technology with the core technology being supported by companies such as SalesForce, Google, ServiceNow, etc. Carahsoft currently support a state-wide implementation of Service Now's cloud technology within the Commonwealth of Pennsylvania. This implementation is known as the Enterprise Information Help Desk and manages all incident requests. Additionally, in 2013, Carahsoft has contracted with the State of Ohio to provide a cloud solution built around the technology from Salesforce. Ohios' Department of Administrative Services has contracted for Carahsoft to provide a variety of services including Service Cloud, Radian6 and Marketing Cloud as well as others. Both the Ohio and Pennsylvania cloud solutions are still being provided to these organizations.

Contracts similar in scope and size of this NASPO Cloud RFP:

California Multiple Award Schedule	California CMAS 3-12-70-2247E
Delaware Salesforce Contract	Delaware SE-CLD-001
Florida Commercial-off-the-shelf Software Contract	Florida COTS 43230000-14-01
Iowa Salesforce Contract	Iowa 2015-BUS-004
Ohio Master Cloud Services Agreement	Ohio MCSA-0016
Ohio State Term Schedule	Ohio STS 534354
Texas DIR Salesforce Contract	DIR-SDD-1793
Texas DIR Emergency Preparedness Contract	DIR-SDD-2035
Texas DIR Software/SaaS Contract	DIR-TSO-3149
VITA Desktop Productivity Software Contract	VITA VA-140401-CARA

6.2 – Scope of Experience Describe in detail the business' experience with government or large consortium contracts similar to the Master Agreements sought through this RFP. Provide the approximate dollar value of the business' five (5) largest contracts in the last two (2) years, under which the Offeror provided Solutions identical or very similar to those required by this RFP. Government experience is preferred.

CONTRACT VEHICLES – Over the past ten years Carahsoft has acquired and maintained a wide variety of purchasing contract vehicles for agencies at the state, local, and federal levels. Carahsoft holds statewide contracts in many states across the country, and we have a great deal of experience with IT Master contracts accessible to numerous public agencies. Carahsoft has extensive experience in successfully launching, maintaining, and managing these contracts and projects over a wide range of government customers. The range of government projects include agency/ county/ city wide project, state-wide efforts, and multi-state contracts, as well as supporting projects that cross a wide range of Federal government customers. Examples of some of these projects include:

TEXServe Multi-jurisdictional Purchasing Program: Carahsoft promoted and managed the Texserve Contract-allowing the full VMware Products & Services portfolio to be procured by Texas K-12 Users at a discounted price.

TEXserve services including: VMware Technical Support, Pre-sales licensing configuration & design, contract promotion, ad hoc revenue reporting, and customer nurturing/ upsell campaigns. Carahsoft worked with Texserve, K-12 customers, to partner with a select number of VMware Premier and Enterprise Authorized Resellers utilizing their expertise under the Texserve contract.

ONENET Purchasing Consolidation: Carahsoft serves as the prime contractor and program manager for the ONENET contract serving the entire ONENET community providing the ability to procure VMware software (licensing/support) through a trusted network of strategic partners at a discounted rate. Carahsoft has a proven track record of providing the highest level of technical support while ensuring that members receive the proper software products and services conveniently under the ONENET Contract.

TX DIR Contract Sales: Carahsoft maintains a number of purchasing vehicles with the State of Texas Department of Information Resources (DIR.) 2014 DIR sales accounted for greater than $50M in revenues. Carahsoft actively markets these contracts and has grown revenues at greater than 10% annually for the past 5 years.

Total GSA State & Local Sales: Carahsoft holds a US General Services Administration (GSA) Schedule 70 Technology Contract. This contract is open to State and Local agencies to purchase as a form of Cooperative

Purchasing. Carahsoft markets the availability of this contract to eligible users and maintains sales revenues to eligible State and Local entities at greater than $50M annually.

As a whole, Carahsoft's five largest public sector contracts have totaled approximately $211,571,007 in sales in the past 2 years.

Carahsoft GSA Schedule	GS-35F-0119Y	$127,242,948.95
Texas DIR Emergency Preparedness Contract	TX-DIR-SDD-2035	$ 39,007,058.19
Texas DIR BMC Contract	TXDIR-SDD-1727	$ 15,734,306.68
Texas DIR Salesforce Contract	TXDIR-SDD-1793	$ 14,876,679.26
Texas DIR Adobe Contract	TX-DIR-SDD-2504	$ 14,710,013.43

Total Sales: $211,571,006.51

These contracts make up close to 2/3 of the total sales on contract that Carahsoft completed in that span. All of these contracts are currently in place with government entities.

6.3 – Financials Offeror must provide audited financial statements, of the last two years, to the State that demonstrate that an Offeror meets at a minimum Dun and Bradstreet (D&B) credit rating of 3A2 or better, or a recognized equivalent rating. Please provide the Respondent's D&B Number and the composite credit rating. The State reserves the right to verify this information. If a branch or wholly owned subsidiary is bidding on this RFP, please provide the D&B Number and score for the parent company that will be financially responsible for performance of the agreement.

Carahsoft has deemed its audited financials to be considered confidential. Additional information is provided in the Confidential, Protected, or Proprietary Information section. For D&B report along with additional clarification, please see page 360 in the Supplemental Information Section.

6.4 – General Information

6.4.1 Provide any pertinent general information about the depth and breadth of your Solutions and their overall use and acceptance in the cloud marketplace.

Carahsoft has assembled a team from our vast portfolio of vendors that includes our leading premiere network of cloud solutions, resellers, and subcontractors as the best solution to meet the State of Utah's requirements. They include:

AODocs, CA, DocuSign, FireEye, Google, QTS, Salesforce, SAP, ServiceNow, Virtru, Virtustream, VMware

Carahsoft is submitting as the exclusive offeror for all Google, Salesforce, and ServiceNow solutions and services for the NASPO Cloud solicitation. These manufacturers have deemed Carahsoft as the prime contractor who can effectively and efficiently manage the NASPO cloud contract on their behalf.

As a part of this response Carahsoft has utilized multiple Cloud Solution Vendors, covering all of the Cloud delivery models; SaaS, IaaS, PaaS. Carahsoft's strong vendor relationships and partner ecosystem have created an efficient and cost effective response which encompasses all vendor solutions into a single, easy

to utilize vehicle. While the technical requirements of each solution vary, Carahsoft strives to consolidate these specifications and responses into a cohesive unit. For example:

CA Technologies is a leader in IT Management Solutions in the industry. CA has be steadily moving its premier on premise management solutions to the cloud. CA Clarity Project and Portfolio Management (PPM) is one of the leading solutions used by state governments today.

Google's SaaS offering, Google Apps, has been commercially available since 2006 and presently has ~5.3 million paying customers covering 26m+ end user licenses. Google Apps represents a combination of the most popular consumer products that have been prepared for Enterprise use through the means of adding Administrative and Compliance Controls to the suite.

Gmail is the anchor product in the SaaS offering. Google has over 1B consumer users of Gmail and from that success designed a means by which customers could bring their own email-enabled domain name(s) into this managed service to replace legacy on-premises systems at a significantly reduced price. The straightforward means of migrating data as well as configuring the service and the knowledge that a majority of these business users may already be familiar with Gmail via personal use has made the adoption of Google Apps a logical choice.

Examples of the evolution of this SaaS offering include:
- Acquisition in 2007 of one of the leading email security and compliance vendors and the integration of those services to the Gmail Advanced Settings options. These features include the ability for customer System Administrators to set Spam, Content, Attachment and TLS policies to meet their specific requirements.
- In 2011 Google launches the Google Apps Status Dashboard, a publicly accessible website with RSS feeds to keep the world apprise of current system status.
- In 2012 Google increases the Gmail storage allocation from 10gb to 25gb, no change in price
- In 2013 Google modifies the storage space to unify email and Drive storage and increase the allocation to 30Gb, no change in price
- In 2014 Google offers a new premium SKU that offers unlimited unified Storage
- In 2015 Google enhances the Gmail Advanced Settings features to include pre-defined lexicons to support Data Loss Prevention scanning in email.

The above list is a short list of the variety of services, support offerings, features and best practices that Google has adopted into the service delivery of the SaaS offering. In addition to the wide use of GMail, Google has six other products with over a Billion active users. Those are Google Search, Chrome, Android, Google Maps, YouTube and Google Play.

Chrome as a browser and an operating system are further evidence of strong usage and market acceptance. In a report released by Net Applications in April of 2015, Chrome browser held 25.68% market share while IE11 had 25.04, followed by IE8 at 16.0. The increase in adoption by Enterprise customers is attributed to the real time updates against emerging threats and the Chrome for Enterprise browser controls.

Chromebooks, the laptops that run Google Chrome as the OS, are seeing a rapid increase in sales in the K-12 market worldwide. This is attributed to the low-cost and the easy-to-manage machines.

Google's PaaS/IaaS offerings entitled Google Cloud Platform was first announces in 2008 with Google App Engine, a platform to develop and host web applications. Early success on this platform included The Royal Wedding Website and BestBuy moving their online Gift Card/Registry service to the platform. Over the years, and based on market demand, Google began to externalize off PaaS/IaaS service offerings that Google developed originally for their own infrastructure and platform utilization.

Google continues to expose the benefits of Google's infrastructure to outside entities.

Or, put differently, Google lets customers use the same infrastructure that allows Google to return billions of search results in milliseconds, serve 6 billion hours of YouTube video per month and provide storage for 1Billion Gmail users.

Salesforce is the enterprise cloud computing leader dedicated to helping companies and government agencies transform into connected organizations through social and mobile technologies. Since launching its first service in 2000, Salesforce's list of over 150,000 customers span nearly every industry worldwide. The company's trusted cloud platform is creating a connected government experience for over 1000 government agencies including all federal cabinet government agencies and the majority of US States. With the world's leading cloud platform, Salesforce is freeing government data from legacy systems, empowering citizens and connecting agencies to administer government in powerful new ways. Government agencies are using Salesforce solutions for a multitude of government functions including grants management, constituent communications and correspondence management, incident and case management, call/contact center management, outreach programs, learning management, volunteer management, project management, and even donor management, among numerous others.

SAP is the fastest growing company at scale in the cloud with a user base of over 95 million subscribers. We also have the largest cloud portfolio of over 30 solutions for all lines of business as well as business suites. We also have 41 data centers in 21 locations in 11 countries.

6.4.2 Offeror must describe whether or not its auditing capabilities and reports are consistent with SAS 70 or later versions including, SSAE 16 6/2011, or greater.

Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, our various cloud providers continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by third party auditor annually at a minimum. Additional audits and certifications include: CSA 'Consensus Assessments Initiative', JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe.

Some examples include:

ServiceNow's security framework is based on ISO/IEC 27002 and has been ISO 27001 certified since 2012. Annually, ServiceNow undergoes ISO 27001 Surveillance audits and well as SSAE 16 attestations for both SOC 1 Type 2 and SOC 2 Type 2. Customers under an NDA can request these reports annually in assisting with both their vendor management and regulatory or compliance programs. ServiceNow provides Security Event Logs using Application Level Audit Logs and Infrastructure Monitoring,

Application Level Audit Logs. The ServiceNow application writes detailed audit log information that is stored in tables within a customer's instance. Since this is considered customer data and is stored within a customer's instance, ServiceNow does not attempt to monitor or view this data unless specifically requested by a customer. As a result the customer is responsible for monitoring the contents of these logs files and, at the customer's choosing, exporting the logs through the capabilities provided within the platform.

Infrastructure Monitoring. All components of the infrastructure supporting the private cloud feed alerts and logs into the SIEM. In addition, ServiceNow has deployed an Intrusion Detection System (IDS), positioned to listen to all inbound network traffic, with all events going to the SIEM as well. The SIEM is configured to automatically send alerts for common attacks. ServiceNow is responsible for managing the SIEM environment and securing the logs. ServiceNow retains all infrastructure logs for at least 90 days. The Security Operations Center (SOC) is also responsible for completing a daily checklist across a range of security domains, including privilege account usage, IDS alerts, file integrity monitoring (FIM), and database access. The daily checklists and captured events are managed through an instance of ServiceNow. Any variances that are discovered are raised as incidents for tracking, notifications, and investigation.

CA SaaS environment is compliant with SSAE16 for services where infrastructure and application are managed and maintained by CA. CA Agile Management currently does not hold SSAE16 certification. For SaaS offerings where infrastructure is managed by a third party, provider's SSAE16 reports are available upon request.

6.5 – Billing and Pricing Practices

6.5.1 Describe your billing and pricing practices, including how your billing practices are transparent and easy to understand for Purchasing Entity's.

Carahsoft's Order Management team works to ensure that billing and payment are completed in an efficient and simple manner. Purchase Orders and Invoices are provided to the customer early to ensure that payment can be completed whenever the customer is ready and within the confines of the agreed upon deal. Our OM team is available to answer any questions a Purchasing Entity has in order to assist with the process and confirm that they have everything needed for payment.

Carahsoft's pricing is dictated by the manufacturers- Carahsoft ensures that the Purchasing Entity's receive the best possible price by working directly with the manufacturer and ensuring that pricing meets or exceeds the contract being used. In addition, Carahsoft works with the manufacturer to ensure that all pricing changes are accounted for within the contract, as applicable.

6.5.2 Identify any typical cost impacts that a Purchasing Entity might need to consider, if any, to implement your cloud solutions.

When a purchasing entity determines they need implementation services to their cloud solutions, the Carahsoft offering provides these additional services. For Example:

ServiceNow Response: Customers typically engage ServiceNow for the initial implementation and training services and then for any major new future application implementations to get the best-of-breed expertise

for good standard solution support. ServiceNow developed the platform and applications so anyone could support changes to the configuration without having to hire outside consultants. The customer is empowered as they gain experience either by shadowing ServiceNow consultants during initial implementations, as they talking to other customers through the Community website, or by asking for technical support through the portal. So initial costs typically occur for ServiceNow when it is first implemented and there might be requested services as customers add new application support but there are no ongoing costs typically.

CA Cloud SaaS solutions are fully operational multi-tenant solution that are fully ready to use at outset. These Solutions are typically complex management solutions that do require setup and training. For example many customer will purchase a limited time block of consulting to help with loading data, and configuring reports. Training is also available for all applications to either augment start-up packs or walk customers through basic tasks.

In addition to the licensing fees there are optional Google services that a Purchasing Entity may find meet additional mandatory requirements. Examples would include adding on other SaaS solutions like Virtru for end to end encryption or AODocs for Document Management. The key benefit to moving to Cloud based vendors is a new set of transformative tools that are more productive and most cost effective than traditional client server solutions. Other additional costs may come into play of the Purchasing Entity wants to outsource all of the configuration and migration work to the selected reseller leading to additional time and materials expenses.

The Salesforce solution is available immediately for use via the internet after a Purchasing Entity makes a purchase of the solution. Other additional costs would include any implementation fees to be performed by a certified Salesforce implementation partner. These fees vary based on the type of project and length and complexity of implementation.

6.5.3 Offeror must describe how its Solutions are NIST compliant, as defined in NIST Special Publication 800-145, with the service models it offers.

Carahsoft's cloud solution offerings all fit within the guidelines listed in NIST publication 800-145 and repeated in Attachment D of this response. Please see response 8.1.5 for a more detailed explanation.

6.6 – Scope and Variety of Cloud Solutions

6.6 Specify the scope and variety of the service models you offer under this solicitation. You may provide a list of the different SaaS, IaaS, and/or PaaS services that you offer.

Carahsoft proudly offers a number of SaaS, PaaS, and IaaS supported by the cloud technologies as listed below. Many of our top tier cloud vendors also provide subscription and utility based pricing models which would be available to the State. Below is a list of each manufacturer being proposed in this response, along with the specific type of solution (SaaS, IaaS, and PaaS) they fit into:

SaaS – AODocs, CA Technologies, DocuSign, FireEye, Google, QTS, Salesforce, SAP, ServiceNow, Virtru, VMware
PaaS – Google, QTS, Salesforce, SAP, ServiceNow, Virtustream
IaaS – FireEye, Google, QTS, Virtustream, VMware

6.7 – Best Practices

6.7 Specify your policies and procedures in ensuring visibility, compliance, data security and threat protection for cloud-delivered services; include any implementations of encryption or tokenization to control access to sensitive data.

Carahsoft utilizes varying procedures for ensuring visibility, compliance, data security and threat protection for cloud-delivered services. Please see the below examples of potential options for meeting the State's expectations:

ServiceNow Response: ServiceNow applications have the advantage of being built on a single cloud platform that consists of one user interface, one code base and one data model; delivering holistic visibility into processes, creating a single source of truth, irrespective of whether the processes and systems are within the customer's environment or hosted in the cloud. ServiceNow invests significant resources in providing its services in a secure manner. This includes global teams delivering 24x7 operations and technical support from ServiceNow staff. ServiceNow currently has offices with staff focused on the management of the private cloud in Australia, the Netherlands, the U.K, North America, and Asia. The ServiceNow environment is a private cloud, fully owned and operated by ServiceNow, which supports a logically single tenant architecture. Customer data is isolated from other customer data by leveraging an enterprise-grade cloud architecture and a dedicated database and application set per instance. This gives ServiceNow customers cost reduction through shared infrastructure, while having the security benefits of customer-specific isolation at the application and data layers. In addition to the security features that come standard within the platform and each customer instance, customers can leverage the additional security features within ServiceNow to augment the security configuration of their instances based on their own needs and risk profile.

CA Response: This is addressed throughout all of our policies and procedures. CA SaaS Operations and Delivery runs an Information Security Management Framework (ISMS), which includes security organization, documentation, monitoring, and continuous improvement cycle. The security documentation comprises of CA SaaS Operations information security policies, procedures, guidelines and checklists. ISMS documentation is reviewed along with applicable controls annually. CA offers a variety of SaaS solutions, details for each offering has been provided in Exhibit 1 and 2 of this proposal.

Salesforce Response: Salesforce has many customers that are subject to laws pertaining to the processing of personally identifiable information (PII) or personal data. Salesforce offers its customers a broad spectrum of functionalities and customer-controlled security features that its customers may implement in their respective uses of the Salesforce services. Salesforce believes that these provide its customers the flexibility to comply with laws with stringent privacy and security requirements. Encryption options vary based on Salesforce Commercial Cloud or Salesforce Government Cloud offering.

Government Cloud Encryption:
As part of the Salesforce Government Cloud, Salesforce is capable of responding to FIPS 140-2 cryptographic implementations for data being transferred between the State's web browser and Salesforce. Data that resides within Salesforce's protected boundary does not use FIPS 140-2 validated encryption as compensating/mitigating controls are in place to protect data. Additional information is provided below.

Data In Motion:

Salesforce employs cryptographic mechanisms to protect information during transmission. All transmissions between the user and Salesforce are encrypted by default with a 2048- bit Public Key. Our service uses International/Global Step Up certificates. We support one- way TLS, in which customers create secure connections before sharing private data.
Secure routing and traffic flow policies ensure that customer traffic is encrypted entering Salesforce until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the Salesforce Government Cloud isolation boundary.

Data At Rest:
NIST SP 800-53 Rev. 4 states in SC-28, "Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system." SC-28 also states, "Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate." All secondary storage media (hard drives, disk drives, and tapes) containing customer data are maintained within Salesforce's secure production data centers until the media has been sanitized and destroyed. Salesforce relies on physical access controls as a compensating control to protect the data.

ORGANIZATIONS PROFILE

This section should constitute the Offeror's response to the items described in Section 7 of the RFP. An Offeror's response must be a specific point-by-point response, in the order listed, to each requirement in the Section 7 of the RFP.

7.1 – Contract Manager

The Offeror must provide a Contract Manager as the single point of contact for management of the NASPO ValuePoint Master Agreement, administered by the State of Utah. The Contract Manager must have a minimum of three (3) years' experience managing contracts for cloud solutions.

7.1.1 Provide the name, phone number, email address, and work hours of the person who will act as Contract Manager if you are awarded a Master Agreement.

Bethany Blackwell
Senior Manager
703-230-7435 (office)
703-501-1134 (cell)
Bethany.blackwell@carahsoft.com
Working hours: 7am-7pm EST M-F

7.1.2 Describe in detail the Contract Manager's experience managing contracts of similar size and scope to the one that will be awarded from this RFP. Provide a detailed resume for the Contract Manager.

The proposed contract manager, Bethany Blackwell, has over 5 years of experience in managing SaaS contracts in both the State and Local and Federal markets.

Bethany developed and manages contracts and associated terms for cloud contracts in more than 10 states. The combination of the State and Federal contract vehicles and BPAs being managed is valued at over $300M. Annually, she oversees 1000+ SaaS transactions off of these contract vehicles which include licensing and implementation that provide end to end cloud solutions to public sector customers.

Name	Position
Bethany Blackwell	**Carahsoft Senior Account Manager – Will serve as the NASPO ValuePoint Contract Manager**
Background	
• Senior Manager for cloud solutions products, including Salesforce.com, DocuSign, BMC Software • Vendor/Partner manager for 20+ complimentary solution vendors and 25+ implementation partners and system integrators • Graduated Virginia Tech in 2010 - dual degree with concentrations in Psychology and Political Science • 5+ years of experience at Carahsoft	
Skills	

• Expertise in negotiating SaaS contract vehicles and terms at State level • Knowledge of contract vehicles, BPAs, multi-year deals, multi-vendor deals • Management of enterprise size product contracts • Establish and maintain positive customer relationships through proactive communication • Maintained interactions with customers to ensure quick, accurate quotes; facilitated easy ordering process for customers
Relevant Experience
• Oversees the management and execution of 900+ individual SaaS contracts, valued at 85M+ annually • Maintain the annual recurring subscription renewal bases to ensure no customer's lapse in service • Oversees the ordering and distribution of licenses on statewide enterprise licenses agreements and various BPAs • Established vendor specific terms and conditions for 10 different statewide contracts • Assist customers in shifting buying strategy from perpetual to subscription licensing model

7.1.3 Describe in detail the roles and responsibilities of the Contract Manager as they apply to the NASPO ValuePoint Master Agreement that will be awarded from this RFP.

The Contract Manager assigned to this contract will be in charge of all coordination and organization efforts between Carahsoft and NASPO ValuePoint. This includes, but is not limited to:

- contract negotiation
- roll-out plan
- amendments completion
- renewal execution
- reseller/subcontractor additions
- contract pricelist updates and upkeep
- contract compliance
- marketing coordination

TECHNICAL RESPONSE

This section should constitute the Technical response of the proposal and must contain at least the following information:

A. A complete narrative of the Offeror's assessment of the Cloud Solutions to be provided, the Offerors ability and approach, and the resources necessary to fulfill the requirements. This should demonstrate the Offeror's understanding of the desired overall performance expectations and clearly indicate any options or alternatives proposed.

In response to the State of Utah request for Cloud Solution Proposals, Carahsoft has assembled a response that includes a number of Cloud Solution Offerings from within the Carahsoft Cloud framework. These offerings are all supported in part or wholly by twelve leading cloud technology providers. Each provider's technology is an integral part of Carahsoft's proposal. Within this framework, Carahsoft will orchestrate, assemble, and execute on all activities necessary to support this contract, engaging each cloud technology provider as needed in the delivery of a particular service or solution offering.

The Carahsoft Cloud framework will provide for all requirements of the State of Utah Request for Proposal to be fulfilled. Carahsoft will be able to provide Cloud Solution Offerings to the State of Utah as well as to those entities that may participate via the cooperative purchasing program. The Carahsoft Cloud proposal provides for the provision of PaaS, IaaS, and SaaS offerings that are compliant with all requirements as outlined by the State. Carahsoft will provide dedicated resources to supporting this agreement. Carahsoft will insure that adequate resources are supplied to fully support this agreement during all phases from contract launch through termination. Usage requirements and demand resources fluctuate over time and Carahsoft's Cloud offering has been constructed in a manner that provides for the ability to scale without interruption, disruption, or any other similar interruption of customer service and solution availability.

B. A specific point-by-point response, in the order listed, to each requirement in the Section 8 of the RFP. Offerors should not provide links to a website as part of its response.

Offeror's should focus their proposals on the technical qualifications and capabilities described in the RFP. Offerors should not include sales brochures as part of their response.

For the purposes of Carahsoft's response to the technical requirements (section 8) of this RFP, please note that any response provided related to a specific manufacturer should be treated as a response to the following categories:

SaaS – AODocs, CA Technologies, DocuSign, FireEye, Google, QTS, Salesforce, SAP, ServiceNow, Virtru, VMware
PaaS – Google, QTS, Salesforce, SAP, ServiceNow, Virtustream
IaaS – FireEye, Google, QTS, Virtustream, VMware

8.1 – Technical Requirements

8.1.1 Offeror must identify the cloud service model(s) and deployment model(s) it intends to provide to Eligible Users. See Attachment D.

CA	APM	CA APIM SaaS offering helps accelerate, secure and manage APIs. CA is responsible for development and management of application. AWS provides IaaS services to CA for management of the underlying cloud infrastructure.
	MAA	CA Mobile App Analytics stimulates collaboration between business analysts, developers, operations and support in order to accelerate mobile app delivery and improve end-user experience. This service is hosted at CenturyLink Data center and the infrastructure is managed and maintained by CA SaaS Ops and Delivery team.
	CA Agile	CA Agile Central is a SaaS offering that is generally used to document and manage work within the SDLC.
	ASM	CA App Synthetic Monitor (ASM) provides end-to-end transaction response-time visibility into cloud, mobile and Web applications. Application utilizes Rack Space IaaS services.
Google	The Cloud Service Models that we intend to provide include SaaS, PaaS, and IaaS. In our response we will describe the various options for using Google Apps under the SaaS model and the functions of Google Cloud Platform under Paas and Iaas.	
AODocs	The Cloud Service Models that we intend to provide is SaaS.	
Virtru	All Virtru services are cloud-based and accessed via browser or downloadable browser extensions and plugins.	
Salesforce	Salesforce's deployment model is a "public" cloud infrastructure, as defined by NIST 800-145	
ServiceNow	Cloud service model: Software as a Service (SaaS) Deployment model: Private Cloud	
QTS	"QTS is a leading national provider of Infrastructure as a Service (IaaS) data center solutions and fully managed cloud services and a leader in security and compliance. The company offers a complete, unique portfolio of core data center products, including custom data center (C1), colocation (C2) and cloud and managed services (C3), providing the flexibility, scale and security needed to support the rapidly evolving hybrid infrastructure demands of web and IT applications. With 12 data centers in eight states, QTS owns, operates and manages approximately 4.7 million square feet of secure, state-of-the-art data center infrastructure and supports more than 850 customers. QTS' Critical Facility Management (CFM) can provide increased efficiency and greater performance for third-party data center owners and operators. QTS offers a number of IaaS solutions.	
SAP	Ariba	Our solutions are offered and delivered in a true subscription-based model and shared service (multi-tenant) offering. There is no software to install, no hardware to buy, no maintenance or support costs and no need to hire consultants or tech specialists to run the system. We deploy and manage the infrastructure. Customers only need a web browser for access. Subscriptions include system maintenance, automatic upgrades, enhancements and application of service packs, Level 1– 3 help desk support, professional services and best practices built directly into the application.
	Fieldglass	The SAP Fieldglass application is exclusively offered in a software as a service (SaaS) model.
	Hanna	SAP HANA Enterprise Cloud (HEC) is a private managed isolated & dedicated ladnscape (single tenant) offering end-to-end cloud-based infrastructure and managed services for SAP applications powered by SAP HANA. It is a fully scalable, enterprise-ready, mission-critical, secure and high-availability cloud service.
	Hybris	The SAP Hybris Commerce, Cloud Edition offering are all single tenent hosted VM environments. Customers have their own VM's with SAP Hybris instances deployed to those VM's. The SAP Hybris Commerce, Cloud Edition currently

		has Development, Staging, Testing, and Production environment. More environments can be added as required.
	SuccessFactors	Our solutions are delivered through a private cloud using a multi-tenant architecture. We refer to this as a Controlled Cloud. It includes a contractual framework reflecting applicable data privacy regulations, implementation and maintenance in accordance with Technical and Organizational Measures (TOMS) and regular audits by an independent third party for industry compliance and transparency.
VMware	vCloud Air	IaaS – Public, Hybrid, Community
	Horizon Air Desktop & Apps	IaaS – Public
	vCloud Suite	IaaS – Private, Hybrid, Community
	Airwatch	IaaS – Private SaaS – Public
	Horizon 6	IaaS – Private
	Realize Air Complaince	SaaS – Public
	SocialCast	SaaS – Public
FireEye	All FireEye cloud offerings included in this response fit the SaaS cloud service model and private cloud deployment model.	
VirtueStream	Virtustream solution is fully NIST compliant for Essential Characteristics, as the Infrastructure as a Service (IaaS) Service Model, with all deployment options – Private Cloud, Community Cloud, Public and Hybrid Cloud.	

8.1.2 For the purposes of the RFP, meeting the NIST essential characteristics is a primary concern. As such, describe how your proposed solution(s) meet the following characteristics, as defined in NIST Special Publication 800-145:
8.1.2.1 NIST Characteristic – On Demand Self-Service: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how self-service technical capability is met.

CA	APM	N/A. This is a SaaS service and clients do not have direct access to the underlying infrastructure in order to provision computing capabilities. CA is responsible for the management and maintenance of the infrastructure and will make any necessary adjustments as part of providing this service to its clients.
	MAA	This is a SaaS offering and On-Demand service is not available, however, MAA customers are enabled to manage their accounts and carry out configuration changes required to manage mobile applications.
	CA Agile	We are a fully multi-tenant environment and do not provide the On-Demand Self-Service capability.
	ASM	This does not apply as this is a SaaS service. ASM customers are able to manage all aspects of their accounts, create sub-accounts, and make any configuration changes necessary for their monitors.
Google	SaaS, Google Apps administrators have access to an Admin Panel that allows them to perform user administration, service configurations, reporting on demand. Paas/IaaS, Google Cloud Platform is an integrated set of Compute tools, Storage Tools, Networking Tools, Big Data analytic tools, Management tools and Services APIs. A customer can use any of these services on demand via the Developer's Console.	
AODocs	SaaS, AODocs administrators have access to an Admin Panel that allows them to perform user administration, product configurations,reporting on demand.	

Virtru	All required services can be provisioned immediately when required. Users only need to install application to get single-user capability, or login to administrative dashboard for administrative features.	
Salesforce	Salesforce PaaS and SaaS solutions are delivered on-demand via the web and can be accessed with a browser and internet connection or mobile device. No additional software or infrastructure is required. Salesforce hosts the entire solution, thus freeing up customers to manage their mission, not manage an infrastructure solution. Additionally, Salesforce is browser agnostic and supports all major browsers (Firefox, Chrome, Safari, IE). No installations on users' laptops or desktops are required and thus the solution is accessible from anywhere an internet connection and supported browser are available, including mobile devices.	
ServiceNow	Customer instances are provisioned automatically after an agreement between a customer and ServiceNow is executed. ServiceNow actively monitors customer instance performance and can automatically scale its application servers out horizontally by adding them to the load balancer pools for a particular instance.	
Docusign	DocuSign's DTM® solution is ISO 27001:2013 certified and many of the ISO 27001:2013 controls are mapped to the NIST 800-53 requirements; we can provide additional information upon request.	
QTS	On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.	
SAP	Ariba	The solution provides self-service user profile management. Users profit from the intuitive, minimal-step nature of the user interface with little or no training. Changes to user profile includes workflow capability for profile changes.
	Fieldglass	All system resources are available to all customers without limitation. The system is highly configurable with most configurations being available to the customer's administrators.
	Hanna	HANA Enterprise Cloud is a private managed cloud therefore infra & services could be requested (added or decommisioned) on demand by placing change requests with SAP HEC teams. HEC roles & responsibilties document clearly articulates what is included in the monthly HEC pricing and what is available on-demand in addition to scaling up or down on the infra/compute.
	Hybris	N/A
	SuccessFactors	All self-service is in one place, including benefits and payroll if those products are in scope. Self-service is an intuitive experience. We provide the ability for employees to have configured permissions to take action in the tool such as field or data updates for personal information, benefits changes, payroll actions, completing workflow for assigned activities in the tool, etc. Self-service for both employees and managers is configurable to fit your business rules and organizational requirements.
VMware	VMware's IaaS and SaaS offerings complies with the On-Demand Self-Service characteristic, because once purchased, a user can unilaterally provision compute resources with no human interaction with VMware. The subscription includes access to two self service consoles: My VMware for account management, and the VMware vCloud Air Console which is the primary interface for access consumption and management of cloud resources purchased from VMware. (See doc for a complete list of products/ features that comply)	
FireEye	FireEye is offering 4 distinct SaaS cloud solutions each featuring self-service features specific to the unique capabilities of the offerings: 1.Email Threat Prevention (ETP) Email Provisioning	

	Once the ETP infrastructure is provisioned, customers can self-service the acceptance of up-stream mail and delivery to user mailboxes by configuring their own domain settings. No user mailbox provisioning is required as ETP will automatically check the validity of the email recipient with the downstream service. 2.Mobile Threat Prevention (MTP) User Provisioning Once the MTP infrastructure is provisioned, customers can self-service the creation of service users by integrating with an LDAP service or manually adding the users via the user interface. Device Provisioning Once the MTP infrastructure is provisioned, customers can self-service the creation of managed devices by instructing users to install the FireEye MTP Application on their mobile device and having a valid user account provisioned. 3.Threat Analytics Platform (TAP) User Provisioning Once the TAP infrastructure is provisioned, customers can create and assign role-based access control to user accounts. The enrollment process includes the ability to create two-factor authentication for newly provisioned users. Data Sources Once the TAP infrastructure is provisioned, customers can configure new data sources to feed the TAP instance without the assistance of FireEye. The TAP communications broker accepts data feeds in the following formats: syslog, flat files, TCP/UDP streams, and JDBC connections. 4.FireEye as a Service with Continuous Vigilance (FaaS CV) User Provisioning Once the FaaS infrastructure is provisioned, customers can create and assign role-based access control to user accounts via the on premise FireEye sensors.
VirtueStream	Virtustream IaaS provides a self-service portal called xStream, where users can access, view, edit, provision, and modify compute, storage, network and application services based on granular Role Based Access Control, which can be integrated with Active Directory or LDAP. Virtustream portal that enables the user to provision VMs, order services through a catalog, add storage, upload service templates, and run various reports all through the same portal.

8.1.2.2 NIST Characteristic – Broad Network Access: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how network access is provided.

CA	APM	The APIM service is accessed via HTTPS on a supported browser with no requirements for a workstation client install ; mobile friendly and optimized for use with iOS and Android tablets
	MAA	Upon native authentication, MAA dashboard is accessible by any host over public internet. Also, mobile devices connect to the service using REST API.
	CA Agile	All access to the application is through a browser.
	ASM	The ASM dashboard and API are accessible from any host connected to the public Internet. The API and dashboard require authentication, and each account is only accessible by the account owner (customer).
Google	SaaS, Google Apps is device, platform and network agnostic. As a pure play cloud-based solution the services can be accessed via any modern browser from any network access point. Customers that have requirements to limit access to trusted devices or trusted access points have access to Device Management tools via the Admin Panel at no additional cost. PaaS/IaaS, Google Cloud Platform management services can be accessed via any modern browser from any network access point. End-users can accesses services through one or more	

	appropriate tools (browser, CLI, APIs, etc.). Administrators can also monitor and manage services through a mobile app.
AODocs	SaaS, AODocs is service, platform and network agnostic. As a pure play cloud-based solution the services can be accessed via any modern browser from any network access point.
Virtru	All Virtru services are available on the publically available internet.
Salesforce	Salesforce PaaS and SaaS solutions are delivered on-demand via the web and can be accessed with a browser and internet connection or mobile device. No additional software or infrastructure is required. Salesforce hosts the entire solution, thus freeing up customers to manage their mission, not manage an infrastructure solution. Additionally, Salesforce is browser agnostic and supports all major browsers (Firefox, Chrome, Safari, IE). No installations on users' laptops or desktops are required and thus the solution is accessible from anywhere an internet connection and supported browser are available, including mobile devices.
ServiceNow	ServiceNow's physical architecture is deployed into ServiceNow's managed dedicated colocation cage space. Multiple diverse Internet connections terminate within the dedicated cage space providing redundant access from the Internet to the ServiceNow environment. All users, administrators and developers connect to the ServiceNow private cloud over HTTPS, leveraging TLS, for communication to and from a ServiceNow instance with all normal interactions via a web browser. There is no requirement to install any client software on any desktop, laptop, tablet, or smart phone used to access a ServiceNow instance.
Docusign	Please see above.
QTS	Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations). QTS recognizes that the connectivity challenges of today are largely driven by consolidation, virtualization and adaptive architectures. Our agile connectivity solutions provide you with both unification across your communication infrastructure and with built-in network scale, reliability, and high-performance. QTS metroConnect is a fast, reliable, high bandwidth connection to hundreds of network and service providers inside the local Carrier Hotel. With access to the numerous networks at the carrier hotel, QTS delivers the interconnection necessary to support your connectivity, business continuity and application collaboration needs. metroConnect offers redundancy and diversity options that ensure your content is always available. •High availability •Backed by a 99.999% SLA •24x7x365 monitoring and management •Carrier-neutral model •Convenient access to an array of Carriers and Internet providers •Dedicated, secure, and highly resilient connectivity with speeds of 100Mbps, 1Gbps or 10Gbps* •Supports all connectivity redundancy, business continuity, and collaborative application needs QTS data centerConnect Service Data centerConnect is a secure, scalable, cost-effective way to connect your primary and secondary sites between two or more client environments located in different QTS data centers providing a reliable interconnection option for any size business. QTS data centerConnect enables data replication and recovery through its resilient and redundant network. This ensures your business operates successfully with seamless, day-to-day transactions over a high-performance, low latency connection that supports business continuity, data replication and other IT business application needs. With QTS data centerConnect you get: •High Availability – Resilient network architecture provides high availability and reliability

	•Dedicated and Secure – Dedicated bandwidth with secure MPLS encapsulation •Scalable Bandwidth – Easily scale your bandwidth (from 10Mb up to 1Gb) •Flexible Network Configurations – Supports multiple network topologies •Cost-effective, Bundled Solution – All inclusive, bundled offer •Fully Managed, End-to-End – End-to-end, proactive monitoring and management, 24x7x365 QTS internetConnect Service internetConnect provides a multi-homed, high performance, dual access, multi-carrier network that meets all your Internet service needs. We ensure maximum uptime, guaranteed availability, and various bandwidth speeds through our flexible, high performance, carrier-neutral offer. For enterprises and government agencies conducting business over the Internet, QTS internetConnect Service provides a highly reliable, secure connectivity solution for production environments. •Direct access to multiple ISP backbones gives unmatched reliability and guarantees maximum uptime ◦Dual connections with direct access to multiple ISP backbones ◦Diverse, redundant paths to multiple backbone providers ◦Dual paths, with diverse entry points into the QTS Data Center •Anti-DDoS Mitigation Services provide an additional level of protection and security •Dedicated with burstable bandwidth options provides resiliency and flexibility •Backed by an industry leading 100% SLA •Optional service plans to meet your needs QTS ethernetConnect Service You need to be able to connect your employees and customers to your applications and to the outside world. Whether hybrid cloud, disaster recovery/disaster recovery as a service, data replication, data migration or other applications, you need the ability to seamlessly and conveniently connect your business together and to the outside world as if there is no distance between you. QTS ethernetConnect offers a variety of connectivity options. You can centralize your services with a single provider. And since QTS can handle everything from ordering to billing you have a single provider for a complete solution – "One Stop Shopping". QTS understands your needs and will tailor your end-to-end solution for your business. •High Bandwidth – Speeds are available in select increments of 100Mb to 10Gb •Data Privacy – Data is separated from IP traffic as it traverses the carrier backbone •High Performance Options – Solutions can be developed to fit your specific performance or reliability requirements •Consistency – Ethernet circuits travel over a single carrier's infrastructure and data follows a consistent path.	
SAP	Ariba	Ariba uses Cisco Routers and Catalysts (high-speed switches) for ensuring maximum network connection performance. They deliver enterprise-class versatility, integration, and power to Ariba. Together, these routers provide the required support for Internet/intranet access with firewall security.
	Fieldglass	Customers are only required to use a standard web browser with default settings to access and use the Fieldglass solution.
	Hanna	Cloud Capabilities are available over the network (via secure MPLS or VPN network connectivity) and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms such as mobile phones, laptops. HEC is an extension of customers existing netwerk and uses customes IP range and /24 range.
	Hybris	All capabilities of SAP Hybris are available over the network. Furthermore, they are accessible by standard mechanism including heterogenous thin or

		thick client platforms through either standard web technologies or through the hybris OCC REST web service API's.
	SuccessFactors	Our solution was designed from the outset for high availability. We provide a system availability SLA of 99.5%. Every component (hardware and software) is completely redundant. There is a redundant piece of equipment or software for every hardware or software component for every layer of the infrastructure stack (server, software and network). We load balance at every tier in the infrastructure, from the network to the database servers. F5 load balancers are used to route traffic to an available web server to process the request. Application server clusters are enabled so that servers can fail without interrupting the user experience. We maintain an N+1 approach for all equipment in the hosted cloud environment, so that there is never a single point of failure. All customer database backups are encrypted and streamed in a secure manner from the customer's "primary" data center to their "alternate" data center, allowing for a timely restoration of service in the event of disaster. Based on the terms of the agreement, we will designate one of the data centers as the customer's "primary" data center, with an additional data center designated as the "alternate" for data redundancy and disaster recovery purposes. Load balancers will automatically detect a software or hardware error and take the servers out of service if needed without interrupting the user experience or application. They also allow capacity addition or reduction without interrupting service. All of the JBOSS application servers are clustered. Each is designated as a primary and a secondary, so any application server can fail without any loss of service or interruption of the application or user experience. The database servers are also clustered using a Veritas high availability cluster. The Veritas suite will detect any hardware or software errors in the database machines and automatically fail them over to a standby server
VMware	VMware's IaaS offerings complies with the Broad Network Access characteristic. All fo these products' capabilities are available over the public internet and can be used by heterogeneous thin or thick client platforms. Consumers only need internet access to access these resources. Additional capabilities exist including the ability to secure communications over the public internet including IPSEC VPN, SSL Client VPN, and the ability to consume via WAN connectivity. VMware's SaaS offering AirWatch can be accessed over the internet or private network through standard mechanisms.	
FireEye	All FireEye cloud offerings included in this response meet the definition of broad network access. Each of the solutions performs its designed functionality over standard internet-facing services and is accessible via a web browser from any internet connected device when valid credentials are provided.	
VirtueStream	Virtustream IaaS provides Broad Network Access, where it can provide landing zone for any private network (Point-to-Point, Virtual Private Label Switching, Multi-Protocol Label Switching, or Direct Connect), public network (Internet, Trusted Internet Connectivity as landing zone, IPSEC VPN and SSL VPN) and also extranet connectivity (shared network, i.e, Cloud Connect, Cloud Exchange, etc.) which is growing rapidly as option for connecting cloud resources.	

8.1.2.3 NIST Characteristic - Resource Pooling: Provide a brief written description of how the cloud solutions proposed satisfies this individual essential NIST Characteristic. Attest capability and briefly describe how resource pooling technical capability is met.

Carahsoft's multiple Cloud Service Provider's solution provides for Resource Pooling, as defined by NIST, in a variety of methods. Each method optimizes the cloud subscriber's experience while optimizing the availability of compute, network, and data resources. Each service provider provides Resource Pooling, see below for details.

CA	APM	CA API Management SaaS (SaaS APIM) has been built from the ground up to be a multi-tenanted, SaaS-based offering that leverages Amazon's infrastructure to scale appropriately; utilize a continuous integration model to provide for frequent updates; and fail over across multiple availability zones.
	MAA	MAA core service utilizes dedicated infrastructure layered with virtualization capabilities. It doesn't share computing resources with other services. Tenants are segregated using application containerization capabilities.
	CA Agile	We monitor all system resources and have alerting mechanisms when resource constraints have reached a defined threshold. We can easily scale our systems to accommodate any additional capacity. If we determine a single user is using a significant amount of resources we will proactively reach out to them to understand what they are trying to accomplish and help them to formulate more performant queries.
	ASM	All ASM core servers are dedicated physical servers. ASM Public Status Pages are served from dedicated web servers (used only by CA ASM) in the Amazon Cloud, on shared tenancy virtualization. Amazon Cloud virtual machines used by ASM are managed by and provisioned by CA ASM systems administrators.
Google	SaaS, Google's global infrastructure is a shared pool of resources that dynamically serve each end user with a primary data center access point that may rotate throughout the session without the end user being aware while at the same time replicating any data across at least two additional geographically dispersed data centers which also may rotate through the session. PaaS/IaaS, Google Cloud Platform also operates across the global Google infrastruture. The elements of this service can be defined within the Developer's console to run within a higher level of abstraction which covers four regions; Central US, Eastern US, Western Europe, East Asia where each region has three or four zones.	
AODocs	AODocs infrastructure is hosted in Google App Engine and data of our customers on Google Drive. This protection is insured by Google.	
Virtru	Virtru Services are offered in a fully multi-tenant mode if the customer requests.	
Salesforce	Salesforce is a multitenant cloud-based subscription service. Multi-tenant cloud solutions provide a single, shared infrastructure, one code base, one platform that is all centrally managed, with platform-based API to support all integration traffic, and multiple release upgrades included as part of the subscription service. Multi-tenancy and the Cloud Computing model remove unneeded tasks from the process of delivering, managing, and integrating software. Salesforce customers will not need to maintain any hardware or software. Without multiple versions to support, integrations don't break during updates; they are simply updated automatically. As a result, both the initial integration and its continued maintenance are simplified. More resources can be focused on creating a better product, with a faster cycle of innovation, instead of having to manage the complexity of many different versions to support a vast installed base. Salesforce's position as an online service enables us to roll out all levels of improvement, from patch releases to major upgrades that are largely transparent to the end users. When a bug is fixed and tested, it is rolled out to the application as part of regular maintenance; the nature of the service prevents special patches and code branches for individual customers, so all fixes can potentially benefit all customers.	
ServiceNow	The ServiceNow environment is a private cloud, fully owned and operated by ServiceNow, which supports a logically single tenant architecture. Customer data is isolated from other customer data	

	by leveraging an enterprise-grade cloud architecture and a dedicated database and application set per instance. This gives ServiceNow customers cost reduction through shared infrastructure, while having the security benefits of customer-specific isolation at the application and data layers. In addition to the security features that come standard within the platform and each customer instance, customers can leverage the additional security features within ServiceNow to augment the security configuration of their instances based on their own needs and risk profile. Customers share a hardware platform (no virtualization), but access entirely separate individual instances of the ServiceNow platform.	
Docusign		
QTS	Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.	
SAP	Ariba	Ariba recognizes that customers need the highest-possible availability and reliability. To that end, Ariba infrastructure is scalable and redundant at all tiers. To provide high availability and reliability, Ariba has extensive error handling and fail-over capabilities. In order to ensure the highest availability, Ariba uses such best practices as frequent systems backup and maintenance, redundant systems, proactive customer notification of unplanned down-time and international support coverage.
	Fieldglass	Fieldglass is offered in a SaaS model. All customers access the same Fieldglass application version in a multi-tenancy database. The system is hosted in a secure hosting facility. All system resources are available to all customers without limitation.
	Hanna	SAP HEC does not pool resources for critical business systems as it's a managed private cloud, which is dedicated to one particular customer. However, network routers, availability reporting & monitoring could be shared. Details can be provided during HEC technical assessment workshop.
	Hybris	All computing resources of the data centers are pooled to serve multiple customers. Each customer gets their own separate VM's and their own instances of hybris deployed to those VM's.
	SuccessFactors	Load Balancing & Server Clustering -- We load balance at every tier in the infrastructure, from the network to the database servers. Application server clusters are enabled so that servers can fail without interrupting the user experience. Database servers are clustered for failover. We maintain an N+1 approach for all equipment in its hosted environment, so that there is never a single point of failure. Complete Redundancy - Every infrastructure component is redundant. There are at least two of each hardware component that processes the flow and storage of data. Backup & Restore - the Data center runs full data backups weekly and incremental data backups nightly.
VMware	All VMware's IaaS products comply with the Resource Pooling characteristic (except for the Hybrid Cloud Manager which is Not Applicable). vCloud Air provides a pool of vCPU, vRAM, Network and storage on the shared physical infrastructure. vCloud Air provides the required location independence and requires that the customer directly specify location of the datacenter that will host their cloud at time of instantiation. Note VMware's SaaS is also Not Applicable.	
FireEye	The FireEye cloud infrastructures consists of web and application servers, operating systems, and databases in a hosted environment and are comprised of both physical and virtual devices.	

	Computing power and resources are load-balanced across infrastructure and replicated to redundant datacenters in the event of a disaster. Client-specific data stored in databases are logically separated from other clients' data providing segmentation and isolation.
VirtueStream	Key to Virtustream solution is its proprietary and patented solution of uVM technology, which is effectively a granular solution for resource pooling, providing application performance, pay for consumption only and segregate resources for security and compliance, but aggregate for cost efficiency. In addition, Virtustream is currently one of very few Cloud Service Provider with capabilities for Geo-Fencing and Geo-Tagging of the virtual machines to a specific data center, and getting down to cluster and host machine level. The resources are pooled based on two specific criteria: •ONLY Accessible Using Private Network – We call this pool "Enterprise" which most of Virtustream's IaaS workload is residing. There is no direct access from Internet into this pool. This is protected via a pair of routing and firewall from any other zones.

8.1.2.4 NIST Characteristic - Rapid Elasticity: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how rapid elasticity technical capability is met.

CA	APM	CA API Management SaaS (SaaS APIM) has been built from the ground up to be a multi-tenanted, SaaS-based offering that leverages Amazon's infrastructure to scale appropriately; utilize a continuous integration model to provide for frequent updates; and fail over across multiple availability zones.
	MAA	The pool of web and application servers can be grown or shrunk when necessary. Any changes to the size of the pool remains transparent to end-users and customers, and would only be done by CA MAA systems administrators.
	CA Agile	This is a SaaS service, therefore, CA monitors all system resources and have alerting mechanisms when resource constraints have reached a defined threshold. Data storage and network capacity are monitored and scaled to meet current client demands. Compute resources are scaled to meet client processing requirements
	ASM	All ASM core servers are dedicated physical servers; there is no elasticity. The ASM Public Status Pages are served from web servers in the Amazon Cloud, and the pool of web servers can be grown or shrunk if necessary. Any changes to the size of the pool would be transparent to end-users and customers, and would only be done by CA ASM systems administrators. Since this is a SaaS environment the CA SaaS Operations and delivery along with RackSpace are responsible for management of the capacity and monitoring.
Google	Saas, Google Apps can scale from 1 user to tens of thousand users. The usage of the services included are designed to horizontal scale within the confines of the per user storage allocation. Google Apps can be purchased with a 30gb per user allocation or with unlimited storage. Paas/IaaS, Google Cloud Platform was designed to scale on demand both in terms of available resources for applications designed and running on Google App Engine but also Compute Engine resources and more.	
AODocs	AODocs can scale from one user to tens of thousand users. The storage is based on the Google Apps storage which could be from 30Gb to unlimited storage depending on the Google Apps subscription.	
Virtru	Presently we over-provision services by 2.5x peak traffic in order to handle spikes. We are in the process of implementing horizontal scaling of all services and expect to have that work completed in the second half of 2016.	
Salesforce	User AuthenticationLogon is form-based. When users log into the Salesforce application, they submit a username and password, which are sent to Salesforce via an TLS-encrypted session.	

	Security features are developed by Salesforce and built into the application. Third-party packages are not used for development or implementation of security internal to the application. In addition, single sign-on and two-factor authentication may be used to authenticate users. Some organizations prefer to use an existing single sign-on capability to simplify and standardize their user authentication. You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication. Federated authentication using Security Assertion Markup Language (SAML) allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign-on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization. Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the profile level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by profile, not organization wide. You must request that this feature be enabled by Salesforce. Salesforce can be configured to utilize Active Directory directly via Delegated Authentication, or indirectly via Federated Identity using either SAML 1.1, or SAML 2.0. Additionally your users can be loaded from information drawn from your Active Directory servers and modifications made in Active Directory can be propagated into Salesforce. Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity Connect product.User ProvisioningUser provisioning and management is performed through the Salesforce Administrative Setup environment and is performed by Salesforce customers. Users, their profiles, permissions and passwords may be managed, edited, activated and deactivated as needed by those with appropriate permissions. An administrator (appointed by the customer and not by Salesforce) with appropriate privileges can manage session timeout, password policies, IP range login restrictions, delegated authentication/SSO, and requirements as part of this process. On first time login or password reset request, users are required to change their passwords to gain access. Salesforce also offers delegated authentication, enabling customers to provision and deactivate users from an external directory service.User Access ProfilesSalesforce enables administrators to manage roles and relationships between roles from within the application, in a single easy to read page depicting the role hierarchy. All users and application-level security are defined and maintained by the organization administrator and not by Salesforce. The organization administrator is appointed by CSBS. An organization's sharing model sets the default access that users have to each other's data. There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field Level security. Details about sharing models and sharing model elements are provided below: Private Only the record owner, and users above that role in the hierarchy, can view, edit, and report on those records.

	Public Read Only All users can view and report on records but not edit them. Only the owner, and users above that role in the hierarchy, can edit those records. Public Read/Write All users can view, edit, and report on all records. Public Read/Write/Transfer All users can view, edit, transfer, and report on all records. Only available for cases or leads. Profiles A profile contains the settings and permissions that control what users with that profile can do within Salesforce. Profiles control: Standard and custom apps the user can view (depending on user license) Service providers the user can access Tabs the user can view (depending on user license and other factors, such as access to Salesforce CRM Content) Administrative and general permissions the user has for managing the organization and apps within it Object permissions the user is granted to create, read, edit, and delete records Page layouts a user sees Field-level security access that the user has to view and edit specific fields Record types are available to the user Desktop clients users can access and related options Hours during which and IP addresses from which the user can log in Apex classes a user can execute Visualforce pages a user can access User Roles Every user must be assigned to a role, or their data will not display in opportunity reports, forecast rollups, and other displays based on roles. All users that require visibility to the entire organization should be assigned the highest level in the hierarchy. It is not necessary to create individual roles for each title at the company, rather a hierarchy of roles should be defined to control access of information entered by users in lower level roles. When a user's role is changed, any relevant sharing rules are reevaluated to add or remove access as necessary. Record Types If the customer's organization uses record types, edit the record type to modify which pick list values are visible for the record type. A default pick list values can be set based upon the record type for various divisions. Field Level Security Field-level security settings let administrators restrict user's access to view and edit specific fields on detail and edit pages and in related lists, list views, reports, Offline Edition, search results, email and mail merge templates, Custom Links, and when synchronizing data.

	The fields that users see in detail and edit pages are a combination of page layouts and field-level security settings. The most restrictive field access settings of the two always apply. For example, if a field is required in the page layout and read-only in the field-level security settings, the field-level security overrides the page layout and the field will be read-only for the user.	
ServiceNow	ServiceNow is a multi-instance architecture that gives every customer its own unique database, which means that it is impossible for your data to be commingled with any other customer. The multi-instance architecture is not built on large centralized database software and infrastructure. Instead, we deploy instances on a per-customer basis, allowing the multi-instance cloud to scale horizontally and infinitely. For our multi-instance cloud, we deploy separate application logic (Apache Tomcat Java Virtual Machines) and database processes (MySQL) for every customer. This allows ServiceNow to scale its application servers out horizontally by adding them to the load balancer pools for a particular instance.	
QTS	Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly out ward and in ward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time. Delivering scalable, secure, high-performing, virtual data centers for government applications QTS is committed to not only giving your cloud the most secure home, but also the ability to utilize best-of-breed technologies. Flexible, high-performing, future proof infrastructure: Built upon the VMware vCloud® Suite, you'll benefit from reliable, high-performing infrastructure using a platform that includes VMware, EMC and Cisco. This compatible solution easily integrates with private VMware environments and provides a pathway to a hybrid cloud.Our scalability increases agility, efficiency and productivity: Your technologists can focus more time on your business and customers, and less time on your infrastructure. Rapid provisioning and improvements in utilization enhances your speed to market, delivers applications faster, and gets projects out the door. Virtually unlimited bandwidth and communications diversity QTS operates carrier-neutral data center facilities. This means that customers can select their communications service providers from hundreds of carriers, Internet Service Providers, dark fiber and satellite companies to meet their transport requirements. Selecting a provider from such a broad list of options gives customers exceptional route diversity and pricing options, as well as different Service Level Agreements and installation schedules. Customers who need very high amounts of bandwidth to conduct their business efficiently will never have to worry about running out of capacity at a QTS facility. Similarly, customers who require exceedingly high communications security have the benefits of selecting from physically diverse routes between their ends points and dark fiber that is not shared with any other users. In short, there are virtually no limitations to the type, amount, or security of communications available at each QTS data center facility.	
SAP	Ariba	There are no scalability limits with our products. We can scale accordingly to fit any data amount or user volume scenario.
	Fieldglass	The hosted Fieldglass solution can be horizontally and vertically scaled very quickly as the web server farm is fully virtualized. Only the SQL server is bare metal by design.
	Hanna	SAP HEC can be rapidly scaled to provision infrastructure & services on demand per customer requests.
	SuccessFactors	Our solution was designed and developed, from the outset, to be a highly scalable application. We also use the concept of "PODS," from a hardware perspective. A POD is a fault tolerant cluster of application & DB servers

		designed, as a scalable unit, to provide core processing and data storage services for fixed increment of customers. Attributes include: A POD is designed to support millions of subscribers. Our current 2nd Generation POD is scaled to 5M+ Multi-Vendor High Performance Blade Servers with 40GBps backplane fabric interconnects Multiple redundant Application Engines Clustering for availability and performance Hardware load balancers to route each new incoming session to the most available web and application processor Designed to support a high rate of concurrent connections while maintaining sufficient redundant capacity to meet SLA requirements New production PODs undergo a verification process before being brought into service Excess capacity PODs are always available on standby (scalability-on-demand) We will increase capacity if data center utilization surpasses the 70% threshold
VMware	All vCloud Air offerings partially comply with Rapid Elasticity. vCloud Air can be purchased as a pool of vCPU, vRAM, Network and Storage on shared or dedicated physical infrastructures that can be elastically provisioned and released. VMware's vCloud Air On Demand is fully compliant because capabilities can be elastically provisioned and released. VMware's SaaS Products i.e. AirWatch, does comply but the NIST requirement is not relevant to SaaS offerings. Note the vCloud Air Hybrid Cloud Manager is not Applicable.	
FireEye	FireEye cloud environments are continuously monitored by cloud service operations (CSO) personnel to help ensure secure operation and available of the system. Capacity is actively monitored and pro-active upscaling is conducted to ensure resources are always available to end-users. Procedures are in-place for rapidly adding resources in the event the infrastructure approaches capacity.	
VirtueStream	Virtustream's self-service portal, ticketing system and also the Technical Account Manager, who is the single point of contact for State of Utah allows for provisioning and deprovisioning of resources and services. In addition, Virtustream is uniquely positioned to provide application level provisioning as part of its standard automation and orchestration tool. Resources can be scaled based on application size, memory, storage, network requirements. xStream utilizes a supply chain to define resource profiles, attributes and offerings than can be provisioned.	

8.1.2.5 NIST Characteristic - Measured Service: Provide a brief written description of how the cloud solutions proposed satisfies this NIST Characteristic. Attest capability and briefly describe how measured service technical capability is met.

CA	APM	Continuous monitoring of all service components (infrastructure and application) is deployed to proactively identify any component or service trending towards failure or approaching capacity. This portion is handled for the underlying cloud infrastructure by AWS with active participation by CA including escalations of issues.
	MAA	CA MAA systems administrators track the resource consumption of each virtual machine in use. ITIL flows are utilized to ensure service delivery. MAA customers do not need this information in order to use the service, nor do they have access to view it.

	CA Agile	Continuous monitoring of all service components (infrastructure and application) is deployed to proactively identify any component or service trending towards failure or approaching capacity CA's best-of-breed monitoring solutions are deployed and supplemented with vendor specific diagnostic tools where appropriate 24x7 staffed network operation center (NOC) to analyze and respond to automated monitoring alerts
	ASM	CA ASM systems administrators track the resource consumption of each virtual machine in the cloud. Since this is a SaaS service, ASM customers do not need this information in order to use the service, nor do they have access to view it.
Google	Saas, Google Apps is already optimized for unlimited use by all end users. Google ensures high availability, low latency and fault tolerance as a part of the contracted services. No metering or rate limiting would be required as Google does not charge based on bandwidth use. Paas/IaaS, Google Cloud Platform includes application development tools, Google App Engine, compute resources, Compute Engine and Container Engine, data storage solutions and networking solutions. The pricing model is based on actual usage and that usage can be monitored with Google's Cloud Monitoring Service which also includes options to autoscale a project.	
AODocs	AODocs is already optimized for unlimited use by all end users. AODocs ensures high availability, low latency and fault tolerance as a part of the contracted services. No metering or rate limiting would be required as AODocs does not charge based on bandwidth use.	
Virtru	All services in our system monitored for availability, stability, security, and intrusion using a combination of tools, such as Dtrace, LogTrail, CloudWatch, DataDog, ElasticSearch and AlienVault.	
Salesforce	Subscription-based Service The Salesforce PaaS and SaaS offerings are subscription based and in a per user/month or user/year format billed annually with some of our products offered as total logins per month or by defined number of members billed annually. Bandwidth Salesforce is designed to use as little bandwidth as possible so that the site performs adequately over high-speed, dial-up, and wireless Internet connections. While average page size is on the order of 90KB, Salesforce uses compression as defined in the HTTP 1.1 standard to compress the HTML content before it is transmitted as data across the Internet to a user's computer. The compression often reduces the amount of transmitted data to as little as 10KB per page viewed due to the lack of image content. The site was designed with minimum bandwidth requirements in mind, hence are extensive use of color coding instead of images. Our average user also is known to view roughly 120 pages from our site per day. Our application is stateless; therefore, there are no communication requirements in the background once the page loads, like traditional client server applications, e.g., Outlook. Therefore, once the page loads, there are no additional bandwidth requirements until a user queries or writes information to Salesforce. System Overview In addition to our Trust site (http://trust.salesforce.com/trust/status), you will also have access to a System Overview, which will help Salesforce customers monitor performance and usage of their own Salesforce org. This overview includes: Schema - # and % of custom objects and data storage Business Logic - # and % of Rules, Apex triggers and classes, as well as % of code used Licenses API Usage - # and % of requests in the last 24 hours User Interface - # and % of custom apps, sites, flows, custom tabs and pages	

	Portal The above list is of all the possible metrics that Salesforce customers may have in their system overview.	
ServiceNow	ServiceNow is a subscription service measured by number of user accounts or number of managed nodes. ServiceNow has a documented capacity-planning model, which is used to determine sizing requirements and scaling options. The need to address capacity and horizontal system scaling is in the background, transparent to our customers.	
Docusign		
QTS	Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability 1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.	
SAP	Ariba	We have an Internal Tools Development Team which has established active monitoring systems with alerting and automated escalation. This includes log monitoring from the backend of the systems and this is tied to established internal processes related to security incident management. The environment, policies, tickets and reports are reviewed under ISAE 3402 assurance audit every six months.
	Fieldglass	Fieldglass utilizes various methods to ensure the system is available and is operating as expected. • Our network performance monitor ensures that all servers and devices are available and performing as expected. • All devices and servers on our network log into our enterprise SIEM tool. All activity is monitored by the Fieldglass security team to ensure activity does not vary from our known baseline. • An Active Performance Monitor has been built into the Fieldglass system. This monitor logs all system activity and enables Fieldglass engineers to drill into data such as concurrent user count, thread count, memory, CPU, SQL duration, server duration, client duration, page hits, etc. This data can be drilled into by day, hour, minute, server, and user. • Customer SLAs are tracked and communicated on a monthly basis. For 2015 we have a 99.4% success rate in meeting all customer page response time SLAs.
	Hanna	SAP HEC services are measured via SAP solution manager and reports are shared with the customer on a monthly basis as well as via self-service reports. SAP HEC operations team monitors the customer landscape and any disruption is addressed after reaching out to the customer and associated approval.
	SuccessFactors	Our hosting sites are designed to accommodate customers desiring a high level of managed service performance. In order to achieve such a level of performance, proactive monitoring is available through a variety of on-line tools that are implemented and managed by Cloud Operations. At a customer management level, the Cloud Operations monitors a series of "key metrics" that measure the results of various processes involved in supporting the business operations and service reliability. These metrics include reports of transaction volumes, latency, system availability, capacity, change management, and help incident response times as compared with established service level goals and standards. To facilitate required system performance, we monitor and tune the use of resources, and makes projections of future capacity requirements. We employ

		a variety of services to monitor and enhance application performance. The network makes extensive use of high availability architecture, and is monitored on a 24x7 basis at multiple levels. We utilize real time web applications performance monitoring software to do the following: Sample web traffic in real time via performance analysis software Track web application errors, (e.g. http 4xx-5xx errors) Monitor end-to-end user performance trends Detailed session analysis for session troubleshooting This data is reviewed on a daily and weekly basis by Operations Support, and is further supported with automated alerts. We proactively gather performance statistics, set triggers to alert on capacity thresholds, and regularly review utilization trends for capacity planning.
VMware	VMware's provides automatic monitoring and metering services to their IaaS and SaaS offerings. Note the vCloud Hybrid Manager is not applicable as it is not metered, because it is for management.	
FireEye	FireEye cloud environments are continuously monitored by cloud service operations (CSO) personnel to help ensure secure operation and availability of the system. An internal monitoring system operates 24 hours per day to assess system availability and performance. The system is configured to send email alert notifications to FireEye operations personnel on a real-time basis communicating potential issues with the production systems.	
VirtueStream	The fundamental of Virtustream solution is based on uVM Technology, which is very unique in terms of billing. Virtustream solution takes average consumption of compute resources, and State of Utah would only pay for actual resources based on a monthly average. This is in comparison with traditional cloud solution, where the billing is based on allocation of resources in T-Shirt size (Micro, S, M, L, XL, XXL), and if the server is up, consumer of the cloud pays, but when it is down, they don't. In case of the Virtustream solution, customer only pays based on the average of vCPU, RAM, IOPS and Network I/O; the key is average, not aggregate and based on consumption not allocation. In addition, all storage, security, application management services are offered as a monthly fee, based on the VMs; also, Virtustream can provide consultative and project support based on time and materials. The µVM brings significant benefits: enabling application level performance SLAs – which an average VM cannot. µVMs eliminate wasted headroom in fixed size VMs, generating significant efficiency improvements (up to 40% beyond traditional virtualization) and Virtustream only charges by the µVM so you only pay for the resources you actually consume not what you might need. Using µVMs also enables applications to be used across multiple hypervisors, across multiple clouds and between different locations – enabling true hybrid clouds. µVM technology allows Virtustream to offer enterprise class clouds capable of running both mission-critical enterprise applications and web-scale applications, delivering the full benefits of cloud to the enterprise.	

8.1.3 Offeror must identify for each Solution the subcategories that it offers for each service model. For example if an Offeror provides a SaaS offering then it should be divided into education SaaS offerings, e-procurement SaaS offerings, information SaaS offering, etc.

CA	APM	In addition to the APIM SaaS offering CA Technologies also offers educational services and consultancy services. CA provides education and training services to its clients.
	MAA	CA MAA helps app developers visualize, investigate, manage, and support user interactions with their mobile apps. It provides deep insights into the performance, user experience, crash, and log analytics of mobile apps. CA MAA is aimed to help

		enterprises understand the experience of mobile app users across the DevOps application lifecycle. Enterprises can accelerate the delivery of user-experience-focused mobile applications and can achieve faster time to market by continuous application delivery while ensuring robust security.
	CA Agile	We provide a SaaS offering that is generally used to document and manage work within the SDLC. In addition to the CA Agile offering CA Technologies also offers educational services and consultancy services
	ASM	CA ASM is a SaaS offering that provides customers with the ability to monitor the availability, health, and performance of network services (web sites, email servers, etc.).
Google	Education SaaS offering - Google Apps for Education Messaging SaaS offering - Google Apps for Work, Google Apps Unlimited Collaboration SaaS offering - Google Apps Unlimited Identity Management SaaS offering - Google Apps SSO eDiscovery/Archving SaaS offering - Google Apps Vault Application Development PaaS - Storage IaaS offering -	
AODocs	AODocs Team Folders AODocs Document Management AODocs Retention Application AODocs Email Connector	
Virtru	SaaS email encryption and SaaS file encryption.	
Salesforce	Salesforce is the enterprise cloud computing leader dedicated to helping companies and government agencies transform into connected organizations through social and mobile technologies. Over 150,000 Salesforce customers across nearly every industry have successfully transformed their operations including over 1000 government agencies, representing all federal cabinet level agencies and the majority of the United States. Customer examples include: State of Texas, State of Colorado, State of California, GSA, USDA, USAID, and others. Salesforce was named one of the World's Most Innovative Companies by Forbes for the last five years in a row. Salesforce is #1 in Enterprise Cloud Computing and #1 in CRM according to IDC. Salesforce ranks as the Leader in the Gartner Magic Quadrant for "CRM Customer Engagement Centers" (SaaS), "Sales Force Automation" (SaaS), and "Enterprise Platform as a Service" (PaaS). Government agencies are using Salesforce PaaS and SaaS solutions for a multitude of government functions including grants management, constituent communications and correspondence management, incident and case management, call/contact center management, outreach programs, learning management, volunteer management, project management, and even donor management, among numerous others.	
ServiceNow	SaaS Offerings: •Cloud and Infrastructure Management Tools •Customer Relationship Management •Project and Portfolio Management (PPM) Tools •Security •Workflow and Electronic Signature •Proposed new category: Information Technology Service Management Tools	

QTS	QTS has built some of the world's largest, most robust, and redundant data centers. The company's innovative 3C product set of custom data center, colocation, and cloud and managed services provides a fully integrated platform and a flexible, scalable level of service that is difficult to match. Our service categories include: IaaS Custom Data Center IaaS Enterprise Cloud IaaS Managed Cloud IaaS vCGS Cloud IaaS Federal Solutions IaaS Healthcare Solutions IaaS Financial Service Solutions Colocation Connectivity Critical Facilities Management Hybrid IT Solutions Disaster Recovery as a Service (DRaaS) Managed Services: Managed Hosting, Managed Network, Managed Systems, Managed Security, Managed Storage & Backup, Managed Disaster Recovery, Data Security	
SAP	Ariba	We provide solutions that allow enterprises to efficiently manage the purchasing of non-payroll goods and services required to run their business. We refer to these non-payroll expenses as "spend."" Our solutions include software, network access, and expertise. They are designed to provide enterprises with technology and business process improvements to better manage spend and, in turn, save money. Our solutions streamline the business processes related to the identification of suppliers of goods and services, the negotiation of the terms of purchases, and ultimately the management of ongoing purchasing and settlement activities. Our solutions allow enterprises to take a systematic approach with products and services that work together. By combining software, network access and professional services into a comprehensive solution, we help customers to address six key areas of spend management: Visibility - enhance spend visibility and control across spend categories, disparate systems and corporate divisions Sourcing - identify top suppliers, negotiate procurement terms, leverage aggregate spend, and manage procurement contracts Contract Management - streamline and automate from contract creation to compliance Procurement – streamline requisitioning and procurement across all types of spend Invoice and Payment - automate invoicing and payment processes Supplier Management - optimize buyer-supplier interactions throughout the spend lifecycle
	Fieldglass	The SAP Fieldglass Vendor Management System (VMS) application is a workforce management SaaS offering.
	Hanna	HANA Enterprise Cloud is a private managed cloud primarily for all SAP enterprise-wide SAP applications such as: ERP, CRM, SRM, BW, etc. All SAP applications can be hosted in HANA Enterprise Cloud (via BYOL or Subscription Licensing model)
	SuccessFactors	Our original product release dates are as follows:

		Performance Management – 2001 Goal Management – 2002 360/Multi-Rater Reviews - 2002 Succession Management - 2004 Compensation Management – 2004 Analytics & Reporting – 2005 Learning & Development – 2006 Recruiting Management – 2006 Variable Pay Compensation – 2007 Employee Profile – 2007 Stack Ranker – 2008 Employee Central – 2009 Metrics Navigator – 2009 Goal Execution – 2010 Calibration – 2010 Workforce Planning (Acquisition) – 2010 Workforce Analytics (Acquisition) - 2010 Plateau LMS (Acquisition) – 2011 JAM – 2011 Employee Central Payroll – March 2012 Onboarding (acquisition of KMS) – May 2013
FireEye	FireEye is offering 4 distinct cloud solutions that can be classified into the following service categories and sub-categories: 1.Email Threat Prevention (ETP) Security – SaaS 2.Mobile Threat Prevention (ETP) Security – SaaS 3.Threat Analytics Platform (TAP) Threat Intelligence – SaaS 4.FireEye as a Service with Continuous Vigilance (FaaS CV) Managed Security Service – SaaS	
VirtueStream	Virtustream is an Infrastructure as a Service (IaaS) offering focused on mission critical workloads and applications. The solution provides as part of the response is IaaS only. Virtustream's IaaS is targeted for all virtualized, x86 based cloud solution. While we have secured and segmented infrastructure for FedRAMP, FISMA, PCI and other regulated workload, it is best suited for any and all enterprise workload as long as the workload can be virtualized and run on x86 platform. For non x 86 environments, Virtustream provides Collocated areas, which is cross connected with the cloud.	

8.1.4 As applicable to an Offeror's proposal, Offeror must describe its willingness to comply with, the requirements of Attachments C & D.

Carahsoft complies with the requirements in attachment C & D. Cloud service models by vendor are broken out in section 6.6 of this response per the request in attachment C.

8.1.5 As applicable to an Offeror's proposal, Offeror must describe how its offerings adhere to the services, definitions, and deployment models identified in the Scope of Services, in Attachment D.

Carahsoft's cloud vendors fit into multiple categories as listed out in Attachment D. Many of our vendors fit a hybrid cloud deployment method with ability to silo off a private cloud if security needs dictate such. Our cloud vendors are broken out by service model in section 6.6 of this response. Carahsoft's cloud vendors

also fit into many categories as listed in section 1.1.3 of Attachment D. Depending on the type of data and service requested our vendors can support everything from on demand self service delivery to a completely managed and measured service option.

8.2 Subcontractors

8.2.1 Offerors must explain whether they intend to provide all cloud solutions directly or through the use of Subcontractors. Higher points may be earned by providing all services directly or by providing details of highly qualified Subcontractors; lower scores may be earned for failure to provide detailed plans for providing services or failure to provide detail regarding specific Subcontractors. Any Subcontractor that an Offeror chooses to use in fulfilling the requirements of the RFP must also meet all Administrative, Business and Technical Requirements of the RFP, as applicable to the Solutions provided. Subcontractors do not need to comply with Section 6.3.

Carahsoft will be utilizing Subcontractors to provide services and solutions for specific manufacturers within this response. In other cases, Carahsoft will work with the manufacturers to provide these services and solutions to all Participating Entities. All Subcontractors shall be vetted to ensure they have the necessary qualifications to do business within the State of Utah and any applicable Participating States. All Subcontractors will also comply with the applicable terms and conditions of the RFP and subsequent contract, as well as all Participating Addendums for the States they are subcontracting in.

8.2.2 Offeror must describe the extent to which it intends to use subcontractors to perform contract requirements. Include each position providing service and provide a detailed description of how the subcontractors are anticipated to be involved under the Master Agreement.

Carahsoft will use subcontractors as a third party company to provide services in relation to the solutions provided by the manufacturer. No other functions of contract management or execution will be performed by the subcontractor. While Carahsoft cannot determine all roles and responsibilities of the positions for each subcontractor, there are multiple different standards which subcontractors utilize for these types of contracts. Here is an example set of the traditional roles a subcontractor would play on behalf of Carahsoft for this RFP:

Job Title: Consulting Engineer
Functional Responsibility: Working under close supervision, person provides technical or scientific and project support for multiple large-scale projects that cross-cut multiple specialization and product development areas. Applies advanced business and/or technical expertise to assist others with defining, analyzing, validating and documenting complex customer operating environments, states of technology and current engineering processes. Provides advanced technical support to others involved in applying specialized knowledge to complex customer processes and requirements. Supports complex technical investigations through advanced research techniques, analysis or development phases of engineering projects. Works with other engineering disciplines in the development and application of processes to improve quality, reliability, cost customer appeal, and satisfaction.

Job Title: Project Manager

Functional Responsibility: Possesses a thorough understanding of the process requirements and provide both technical and management oversight of the project. Responsible for customer satisfaction, serves as the single point of contact, compliance with the Statement of Work, project planning and management, resource allocation, and reporting.

Job Title: Senior Information Architect
Functional Responsibility: Provides supervision, person designs Intranet/Internet/Extranet architectures and develops implementations plans; administration activity; i.e., hardware, security, firewalls. Implements security architecture using LDAP, SSL and firewalls. Installs, configures and maintains all Intranet/Internet/Extranet tools, databases and features; provides support to e-commerce and other systems. Implements server design, development, and operation as well as analyze and develop requirements for hardware sizing/capacity, data validation, security and integration points to other applications.

Job Title: Information Architect
Functional Responsibility: Designs Intranet/Internet/Extranet architectures and develops implementations plans; administration activity; i.e., hardware, security, firewalls. Implements security architecture using LDAP, SSL and firewalls. Installs, configures and maintains all Intranet/Internet/Extranet tools, databases and features; provides support to e-commerce and other systems. Implements server design, development, and operation as well as analyze and develop requirements for hardware sizing/capacity, data validation, security and integration points to other applications.

Job Title: Senior Consulting Engineer
Functional Responsibility: Provides supervision, person provides technical or scientific and project support for multiple large-scale projects that cross-cut multiple specialization and product development areas. Applies advanced business and/or technical expertise to assist others with defining, analyzing, validating and documenting complex customer operating environments, states of technology and current engineering processes. Provides advanced technical support to others involved in applying specialized knowledge to complex customer processes and requirements. Supports complex technical investigations through advanced research techniques, analysis or development phases of engineering projects. Works with other engineering disciplines in the development and application of processes to improve quality, reliability, cost customer appeal, and satisfaction.

8.2.3 If the subcontractor is known, provide the qualifications of the subcontractor to provide the services; if not, describe how you will guarantee selection of a subcontractor that meets the experience requirements of the RFP. Include a description of how the Offeror will ensure that all subcontractors and their employees will meet all Statement of Work requirements.

Carahsoft will be making the determination of what subcontractors to include on the NASPO ValuePoint Cloud contract upon time of award. Carahsoft will ensure a subcontractor has all of the necessary certifications to do business in the State before adding them to the contract as a subcontractor. In addition, Carahsoft will do credit checks and meet with the subcontractor on multiple occasions to confirm that they are reliable and exceed expectations as a services and solutions provider. Finally, an agreement will be put in place between Carahsoft and the subcontractor to ensure optimal efficiency with the subcontractor's responsibilities.

A subcontractor will be actively involved in understanding and shaping any Statements of Work created for the services of a deal in order to make sure that they have the capacity to meet all of the necessary requirements. These Statements of Work will dictate the terms upon which the subcontractor is deployed for services, so Carahsoft will work specifically with subcontractors that are active in the public sector and understand the nuances of selling to government entities.

8.3 Working with Purchasing Entities

8.3.1 Offeror must describe how it will work with Purchasing Entities before, during, and after a Data Breach, as defined in the Attachments and Exhibits. Include information such as:

- Personnel who will be involved at various stages, include detail on how the Contract Manager in Section 7 will be involved;
- Response times;
- Processes and timelines;
- Methods of communication and assistance; and
- Other information vital to understanding the service you provide.

Security is of the uptmost importance to all of the Service providers that Carahsoft is submitting. Should and actual breach occur, it is the first priority of Carahsoft and the service provider to identify the source of the breach and implement safe guards to prevent one from happening in the future. The Service Provider will promptly notify the Purchasing Entity of the incident. Notification of the breach will be provided by the service directly to the security or customer contact that is identified by the Purchasing Entity. Methods of communication could include phone or email notification.

8.3.2 Offeror must describe how it will not engage in nor permit its agents to push adware, software, or marketing not explicitly authorized by the Participating Entity or the Master Agreement.

Carahsoft ensures that no unwanted marketing efforts are made to customers through an easy to manage opt out system in our database. Carahsoft can also limit communications by vendor to ensure that only those vendors approved by the customer reach out with marketing materials or product updates. Carahsoft will never support or assist in the pushing of adware or unwanted software to participating customers.

8.3.3 Offeror must describe whether its application-hosting environments support a user test/staging environment that is identical to production.

For applicable cloud offerings, user test/ staging environments are available that are identical to real-time production environments.

8.3.4 Offeror must describe whether or not its computer applications and Web sites are be accessible to people with disabilities, and must comply with Participating entity accessibility policies and the Americans with Disability Act, as applicable.

The user interfaces provided for within this proposal are accessible to people with disabilities using assistive technologies.

8.3.5 Offeror must describe whether or not its applications and content delivered through Web browsers are be accessible using current released versions of multiple browser platforms (such as Internet Explorer, Firefox, Chrome, and Safari) at minimum.

All cloud solution offerings within this proposal that are delivered via web browsers are accessible using current releases of common internet browsers such as Internet Explorer, Firefox, Chrome, Safari, and more.

8.3.6 Offeror must describe how it will, prior to the execution of a Service Level Agreement, meet with the Purchasing Entity and cooperate and hold a meeting to determine whether any sensitive or personal information will be stored or used by the Offeror that is subject to any law, rule or regulation providing for specific compliance obligations.

Upon request of the customer, Carahsoft can host meetings via Adobe Connect web conferencing software or travel in person if the need presents itself. Carahsoft is happy to support and comply with any regulations or sensitive data compliance needs that the customer identifies. Carahsoft has the ability to limit customer information to a secure and isolated database if needed.

8.3.7 Offeror must describe any project schedule plans or work plans that Offerors use in implementing their Solutions with customers. Offerors should include timelines for developing, testing, and implementing Solutions for customers.

Project scheduling and work planning documents are developed in conjunction with customer requirements. Project planning activities are conducted with a focus on developing a statement of work that defines deliverables, customer and contractor areas of responsibility, as well as project benchmarks, and deadlines. Project complexity and customer requirements determine the overall timelines for development, testing, and solution implementation.

8.4 Customer Service

8.4.1 Offeror must describe how it ensure excellent customer service is provided to Purchasing Entities. Include:

- Quality assurance measures;
- Escalation plan for addressing problems and/or complaints; and
- Service Level Agreement (SLA).

The core of Carahsoft's business is to provide the best customer service to our government customers and vendor partners. We are an IT solutions provider delivering best-of-breed hardware, software, and support solutions to federal, state and local government agencies since 2004. Carahsoft has built a reputation as a customer-centric real-time organization with unparalleled experience and depth in government sales, marketing, and contract program management. This experience has enabled Carahsoft to achieve the top spot in leading software license GSA resellers. Carahsoft has leveraged its vast contracting experience and extended it to quoting and order management. Carahsoft seamlessly generates quotes within 30 minutes or less and processed over 56,000 orders in 2014 that were each completed the same day received. Over the past ten years Carahsoft has acquired and maintained a wide variety of purchasing contract vehicles for agencies at the state, local, and federal levels. Associated with all contracts are dedicated and experienced contract management resources. Quality and accuracy is the driving factor behind Carahsoft's successin the government market. All solutions proposals and price quotes that are sent to our customers go through a three step review process for quality. The first is a pricing review that is automatically run against the pricing database to ensure pricing accuracy for the proper contract. The second review is at the certified Account Representative level who will check pricing and configurations for accuary and also review any SOWs that are included. Finally, mangagement review confirms the quality and accuracy of the proposal that will be sent to the Purchasing Entity. Carahsoft has instituted an escalation procedure for any problems or complaints that may arise. There are four levels of escalation and include review by the Account Representative assigned to the

Purchasing Entity, followed by the Regional Manager of the territory, next to the Vice President of State and Local and finally to the President/CEO. Each stage of escalation shall have a response SLA of no more than 24 hours.

8.4.2 Offeror must describe its ability to comply with the following customer service requirements:

a. You must have one lead representative for each entity that executes a Participating Addendum. Contact information shall be kept current.
b. Customer Service Representative(s) must be available by phone or email at a minimum, from 7AM to 6PM on Monday through Sunday for the applicable time zones.
c. Customer Service Representative will respond to inquiries within one business day.
d. You must provide design services for the applicable categories.
e. You must provide Installation Services for the applicable categories.

Carahsoft confirms and agrees that we will name a lead representative for each Participating Addendum. The contact information will be listed on the Carahsoft website and kept current. Carahsoft confirms it will have a representative available by phone and email available 7am-6pm on Monday through Sunday in the applicable time zones. Carahsoft confirms that it will respond to all inquiries within one business day or sooner. Carahsoft will engage with our service providers to provide design services in the applicable categories Carahsoft will engage with our service providers to provide installation services in the applicable categories.

8.5 Security of Information

8.5.1 Offeror must describe the measures it takes to protect data. Include a description of the method by which you will hold, protect, and dispose of data following completion of any contract services.

Security is of the utmost importance to Carahsoft and our service providers. As an example of our Service Provider's security standards, please see the government security response for Salesforce: Government Trusted Security and Infrastructure
Salesforce understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security.

Independent audits confirm that our security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce Force.com gives you the peace of mind only a world-class security infrastructure can provide.

Third-party validation
Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, we continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by third party auditor annually at a minimum. Additional audits and certifications include: CSA 'Consensus Assessments Initiative', JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe.

Protection at the application level

Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define company-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts.

Protection at the facilities level
Salesforce security standards are stringent and designed with demanding customers in mind, including the world's most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk or tape. These backups provide a second level of physical protection. Neither disks nor tapes ever leave the data center.

Protection at the network level
Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs.

Trust.salesforce.com is the Salesforce community's home for real-time information on system performance and security. On this site you'll find:

- Live and historical data on system performance
- Up-to-the minute information on planned maintenance
- Phishing, malicious software, and social engineering threats
- Best security practices for your organization
- Information on how we safeguard your data

8.5.2 Offeror must describe how it intends to comply with all applicable laws and related to data privacy and security.

Carahsoft is happy to support and comply with any regulations or sensitive data compliance needs that the customer identifies. Carahsoft has the ability to limit customer information to a secure and isolated database if needed. Under no circumstances will Carahsoft ever publish or release secure customer data. Carahsoft's cloud vendors are all FIPS certified or have equivalent security standards in place to ensure no customer data is released outside of the secure cloud.

8.5.3 Offeror must describe how it will not access a Purchasing Entity's user accounts or data, except in the course of data center operations, response to service or technical issues, as required by the express terms of the Master Agreement, the applicable Participating Addendum, and/or the applicable Service Level Agreement.

Carahsoft will use customer accounts and data only in the processing of an order and management of the customer's service entitlements. Carahsoft's vendors, as outlined in their specific Master Agreements, only us customer account data for the express purpose of providing the service to the customer. Included in that service is implementation, technical support, and training efforts. Under no circumstances will Carahsoft or its cloud partners use customer information outside of normal operating procedures.

8.6 Privacy and Security

8.6.1 Offeror must describe its commitment for its Solutions to comply with NIST, as defined in NIST Special Publication 800-145, and any other relevant industry standards, as it relates to the Scope of Services described in Attachment D, including supporting the different types of data that you may receive.

CA	APM	CA technologies understands that security is a top concern when evaluating cloud-based applications, which is why CA technologies operations worldwide conform to rigorous certification, compliance and security programs and processes. In addition, we contract with independent auditors to regularly evaluate and validate the security of our service. High risks are identified, validated and remediated before production systems are made available. Medium risks are evaluated and resolved on a priority basis.
	MAA	
	CA Agile	We use CIS and NIST standards as baselines for hardening our systems. We are currently working towards a NIST 800-53r4 certification however this is not yet complete. We are continuously reviewing our compliance with these standards. We perform monthly scans against our Production Infrastructure based on CIS standards. We scan for both vulnerabilites and compliance best practices bases on NIST 800-53v4 standards. Vulnerabilites are tracked and remidiated based on severity and risk.
	ASM	Please see our response to APM/MAA
Google	Google's currently maintains a FedRAMP Authorization to Operate. FedRAMP incorporates the relevant NIST SP and FIPS security requirements. Further, Google contractually commits to maintaining SOC2 and ISO27001 certifications.	
AODocs	AODocs is committed to comply SOC2 type 2.	
Virtru	Virtru's business depends on its ability to support healthcare and criminal justice markets, which requires us to maintain compliance with HIPAA and CJIS standards which both make extensive use of NIST standards	
Salesforce	On May 23, 2014 Salesforce achieved a FedRAMP Agency Authority to Operate at the moderate impact level (as described in FIPS 199 and 200) issued by Health and Human Services (HHS) for the Salesforce Government Cloud. Additionally, on May 15, 2015, HHS, as the FedRAMP authorizing agency, approved the Salesforce Government Cloud authorization package that was updated based on annual attestation requirements and updates to the FedRAMP baseline which is FISMA compliant and based on the current release of NIST SP 800-53 Rev. 4. Salesforce provides contractual assurance to its customers that the Customer Data hosted in Salesforce's services will be kept confidential and not accessed by third parties except under narrow circumstances (such as a customer support issue or as required by law). In the case of customer support, the company's personnel will access a customer's Org only with prior approval and subject to confidentiality obligations.	
ServiceNow	ServiceNow is a cloud service provider offering a SaaS solution deployed from a private cloud that meets the five essential characteristics of cloud computing as described in 8.1. ServiceNow applies the same data classification for all hosted customer data. ServiceNow does not inspect or monitor its customers' information and therefore has no ability to sub-classify	

	customer data. The overriding requirement of the assigned classification is that customer data remains hosted in the private cloud until the customer terminates their subscription. It is never stored anywhere apart from the private cloud. Customers remain the data owner and data controller for all data placed into their instance. ServiceNow does not examine, inspect, monitor or analyze customers' data. Customers apply access controls to restrict access to data within their instances based on their own requirements and needs, including their own data classification.	
QTS	QTS understands the growing number of requirements along with the complexity of managing the high cost-risk if you are not in compliance, and makes compliance a top priority. Our dedicated QTS Internal Audit team is focused on helping you define controls and processes to meet your ever-expanding compliance requirements. We are steadfast in protecting your data with the commitment to allocate required resources, technology and controls to not only help you achieve and maintain compliance today, but to expertly support your needs as they inevitably grow and change in the future. QTS tackles compliance differently. We provide a flexible, integrated approach to meet the IT compliance and regulatory needs across a wide variety of industries – from Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA) to U.S.–EU Safe Harbor. Our approach reduces the complexity and workload to effectively support their compliance efforts.	
SAP	Ariba	Our security framework, which consists of semi-annual independent third party AICPA audit under the Trusted Services Principles of security, confidentiality, process integrity and availability as well as annual certification by an independent Qualified Security Assessor for PCI DSS, is highly aligned with the NIST controls. Our security framework and cloud services are designed to receive process and store data sets of a commercial business-to-business nature and are multi-tenant and international in scope. FISMA/NIST is designed to protect US government data that can include classified information as well as sensitive PII such as ePHI and SSN's or government identifiers. We practice data avoidance where these data sets are concerned primarily to reduce the risk to us and to our customers but also to avoid additional regulatory compliance which has onerous reporting and high costs which would have to be passed on to our customers. Where FISMA regulated entities can take advantage of our solutions, the data sets they expect to store must be validated to avoid being under regulatory requirements beyond what we can provide in terms of both security as well as reporting.
	Fieldglass	Fieldglass has based its security program on the ISO 27002 security standard and has maintained its ISO 27001 certification since February 2011. However, to ensure that a robust security framework was developed, additional controls were added and/or modified based on COBIT DS5 Ensure Systems Security, specific NIST special publications, and vendor specified best practices. Fieldglass uses a SSAE 16 audit with a twelve-month audit cycle to validate that the controls defined within the security framework are operating effectively.
	Hanna	SAP will show the compliance with the SAP Cloud Security Framework by the compliance audits and/or certification audits only as it pertains to the HANA Enterprise Cloud. SAP Cloud and Infrastructure Delivery's Security, Risk & Compliance Office has developed the Integrated

		Information Security Management System (IISMS) Framework. The IISMS Framework is based on SAP's corporate quality and security policy as well as the corporate security standards and guidelines relating to information security and business continuity. This IISMS Framework was adapted to SAP Cloud Security Services as SAP Cloud Security Framework (Cloud SFW). SAP's security, process and compliance team conducts technical security audits to validate that security concepts have been implemented successfully and to safeguard the usage of newly developed tools. Compliance Audits Cloud solutions from SAP have passed ISAE3402/SSAE16-SOC 1 Type II and/or SOC 2 Type II audits (in the following referred to as SOC audits) and can provide the related audit reports on request. Certification Audits The SAP HANA Enterprise Cloud has attained certifications according to the following ISO standards are available (related audits are in the following referred to as ISO audits): • ISO 27001:2013 • ISO 22301:2012 • ISO 9001:2008
	SuccessFactors	Our IT architecture is aligned with ISO 27002. We are Safe Harbor certified and in alignment with BS10012 and ISO 20000 for Service Delivery. We demonstrate an on-going commitment to protecting the confidentiality, integrity and availability ("CIA") of data from internal and external threats, making us a reliable and secure system provider. Our secure multi-tenant Software as a Service (SaaS) platform is designed for availability, security, scalability, and performance. Industry best practices and standards are adopted and incorporated. Our Network also complies with the Authority to Operate as a Moderate Risk Federal Information System by the Office of Personnel Management and Department of Homeland Security; NIST SP800-53 Security Controls; EU Privacy Directive 95/46/EC for EU and non-EU customer data; Payment Card Industry (PCI) Data Security Standard (DSS) v 2.0; Safe Harbor. We provide privacy compliant data center facilities not only in the United States but also as a Member State of the European Union (EU) or a state of the European Economic Area (EEA). Currently, such data centers are certified for ISO27001, ISO9001 and PCI-DSS compliance. Our security services provide complete and thorough monitoring of all traffic on the network on a 24x7x365 basis, and include security technology, alert services and incident management support. We are audited twice annually to SSAE16 (US) or ISAE 3402 (international) accounting standards.
VMware	VMware is fully committed to complying with NIST and all other relevant industry standards including FedRAMP, FISMA, PCI, CSA CAIQ, etc. This is demonstrated by VMware's track record of pursuing and obtaining certifications such as those listed above. vCloud Government Service has been certified to store and secure Low Risk Level and Moderate Risk Level data as defined by FIPS PUB 199. In addition, VMware is capable of enhancing the vCloud Government Service to meet participating State's requirements to be able to store data that is defined by FIPS Pub 199 as High Risk Data. VMware is committed to maintaining compliance with all of our existing and future compliance certifications. Our ability to remain competitive as a software and services provider in the public sector depends upon it. Thus we have established a comprehensive security and compliance team to ensure that we maintain compliance as well as a strong security posture.	

	VMWare supports regular internal and external audits to ensure compliance with its certifications as required. The AirWatch Information Security Program is built on the security framework laid out in NIST 800-53. Although AirWatch is not required to register with any regulatory agencies, we provide a suite of tools for our customer's to maintain industry-relevant compliance guidelines within their mobile device fleets. AirWatch has recently been awarded the HP-IAPP Privacy Innovation Award for Most Innovative Privacy Technology by the International Association of Privacy Professionals (IAPP) for our commitment to delivering an EMM platform focused on end-user privacy. To help ensure the confidentiality, integrity, and availability of our cloud offering, we comply with the European Data Protection Directive (95/46/EC) and our top-tier data center partners have undergone SSAE16 SOC2 Type II audits and have ISO 27001 certifications.
FireEye	FireEye has mature and well documented security and privacy programs. The programs include third party certifications for SSAE 16 SOC 2, FedRAMP certifications, Model clauses, Privacy and security standards among others. The data that FireEye receives is only in conjunction with the malware analysis.
VirtueStream	The Virtustream Federal Cloud (IaaS) has met the requirements for a FedRAMP moderate P-ATO. The IAAS is assessed annually by a FedRAMP certified 3rd Party Assessment Organization (3PAO). The annual assessment will review a subset of the NIST 800-53 Revision 4 controls as designated by FedRAMP. Virtustream's 3PAO shall demonstrate impartiality throughout the assessment to accurately assess the status of all security controls in place.

8.6.2 Offeror must list all government or standards organization security certifications it currently holds that apply specifically to the Offeror's proposal, as well as those in process at time of response. Specifically include HIPAA, FERPA, CJIS Security Policy, PCI Data Security Standards (DSS), IRS Publication 1075, FISMA, NIST 800-53, NIST SP 800-171, and FIPS 200 if they apply.

CA	APM	AWS EC2 datacenters annually undergo SOC 3 audits. The application currently does not hold a Soc 2 attestation.
	MAA	CA MAA is certified for SOC 2 Type 1 Security Audit.
	CA Agile	Our data center provider has a SOC 2 audit report that can be provided upon request. Our application does not currently have such certifications.
	ASM	Rackspace datacenters annually undergo various certification including SOC 3 audits. The application currently does not hold a Soc 2 attestation.
Google	Google has a FedRAMP ATO at the Moderate impact baseline. FedRAMP incorporates many NIST SPs and FIPS including 800-53, FIPS 199, FIPS 200), and has a specific offering. Google Apps for Education that is FERPA and COPPA compliant. Other compliance standards such as HIPAA and CJIS don't offer certification per se, but are commonly accommodated (i.e. Google will sign a BAA to meet HiTECH/HIPAA requirements, and has numerous customers who bear responsibility for meeting CJI processing requirements). PCI DSS is generally not applicable to SaaS systems (though we can do email hygiene processing to protect against incidental usage), but Google IaaS/PaaS does meet PCI DSS v3 standards. Google also holds and is committed to maintaining SOC2 and ISO27001 certifications.	
AODocs	AODocs doens't hold an HIPAA certifications per se, but are commonly accommodated to meet HIPAA requirements signing a BAA.	
Virtru	HIPAA, FERPA, CJIS, NIST 800-53, NIST SP-800	
Salesforce	Salesforce and the Salesforce Force platform is ISO 27001 certified and PCI-DSS compliant. SOC1, SOC2 and SOC3 audits are performed by third party auditor annually at a minimum. Additional audits and certifications include:	

	FedRAMP Authority to Operate from Department of Health and Human Services CSA 'Consensus Assessments Initiative' JIPDC (Japan Privacy Seal) Tuv (Germany Privacy Mark) TRUSTe HIPAA In provisioning and operating the services, Salesforce complies with the provisions of HIPAA's Privacy Rule and Security and the HITECH Act that are applicable to business associates. Salesforce's customers are still responsible for complying with the same in their capacity as a covered entity or business associate using the Salesforce services. The services' features permit customers to customize use as per a compliance program for HIPAA (including the HITECH Act) and many customers store protected health information (PHI) on our service. From a legal standpoint, some of our customers have asked Salesforce to assist them in meeting their compliance obligations; for example, by entering into business associate agreements (BAA) to address formal legal requirements pertaining to use and disclosure of protected health information (PHI). FERPA Salesforce maintains appropriate administrative, physical, and technical safeguards to help protect the security, confidentiality, and integrity of data our customers submit to the Salesforce Services as Customer Data. Salesforce's customers are responsible for ensuring the security of their Customer Data in their use of the service and implementing any necessary customer-controlled settings. To aid, Salesforce offers robust security functionality that provides our customers the flexibility to use the application in a configuration that furthers compliance with local data protection laws and regulations. While Salesforce complies with applicable law in provisioning and operating the Salesforce services, it is the sole responsibility of Salesforce's customers to ensure compliance with applicable laws in their respective uses of the Salesforce services.PCI-DSSSalesforce is PCI Level 1 compliant and has received a signed Attestation of Compliance (AoC) for the Payment Card Industry Data Security Standard (PCI-DSS). Salesforce customers who must adhere to PCI compliance may store personal account numbers ("PAN" or "credit card numbers") in Salesforce, with the following caveats: - PANs may only be stored in a custom field encrypted via Classic Encryption or supported field types via the Platform Encryption functionality. PANs must not be stored in clear text fields, attached files, or any other location. - Customer administrators must configure Salesforce features to support their organization's PCI controls.NIST SP 800-171NIST Special Publication 800-171 is intended for use by federal agencies when agencies are providing CUI to nonfederal organizations (or when CUI is developed by those organizations for federal agencies) for purposes unrelated to information processing. In other words, the nonfederal organizations are not operating their information systems to process agency data, including CUI, on behalf of the agency but rather for other purposes (e.g., when designing or producing an aircraft, performing a study, or conducting background investigations for security clearances). Salesforce recommends that its customers use the classifications as detailed in FIPS 199. FIPS 140-2, FIPS 197, FIPS 199, and FIPS 200 On May 23, 2014 Salesforce achieved a FedRAMP Agency Authority to Operate at the moderate impact level (as described in FIPS 199 and 200) issued by Health and Human Services (HHS) for the Salesforce Government Cloud. Additionally, on May 15, 2015, HHS, as the FedRAMP authorizing agency, approved the Salesforce Government Cloud authorization package that was updated based on annual attestation requirements and updates to the FedRAMP baseline which is FISMA compliant and based on the current release of NIST SP 800-53 Rev. 4.

	As part of the Salesforce Government Cloud, Salesforce is capable of responding to FIPS 140-2/3 cryptographic implementations for data being transferred between the customer's web browser and Salesforce. Data that resides within Salesforce's protected boundary does not use FIPS 140-2 validated encryption as compensating/mitigating controls are in place to protect data. Additional information is provided below. Data Transmission between the customer's web browser and Salesforce: Salesforce employs cryptographic mechanisms to protect information during transmission. All transmissions between the user and Salesforce are encrypted by default with a 2048-bit Public Key. Our service uses International/Global Step Up certificates. We support one-way TLS, in which customers create secure connections before sharing private data. Secure routing and traffic flow policies ensure that customer traffic is encrypted entering Salesforce until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the Salesforce Government Cloud isolation boundary. Data Transmission for Backup Media: Media containing customer data is not transported outside of controlled salesforce.com areas and therefore relies on physical access controls to protect the data. Data at Rest: NIST 800-53 Rev. 3 states in SC-28, "Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system." SC-28 also states, "Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate." All secondary storage media (hard drives, disk drives, and tapes) containing customer data are maintained within Salesforce's secure production data centers until the media has been sanitized and destroyed. Salesforce relies on physical access controls as a compensating control to protect the data. Primary Data Storage: User passwords are stored in the RDBMS encrypted via the SHA algorithm with a 256-bit hash. This is a one way hash. The passwords are encrypted by the application. For primary data storage, Salesforce provides customers with a built-in capability to apply field-level encryption, using 128-bit keys with Advanced Encryption Standard (AES) encryption (as defined by FIPS 197), for a selection of custom fields included in the Salesforce Platform and CRM applications. Field-level encryption ensures the data associated with designated fields is encrypted in storage.
ServiceNow	ServiceNow's security policy is based on ISO27001:2013 and has been since 2012. ServiceNow also has annual SSAE 16 SOC 1 Type 2 and SOC2 Type 2 attestations with controls being based off NIST 800-53. The ServiceNow Service Automation Government Cloud Suite is a FedRAMP Compliant Cloud System with a JAB Provisional Authorization. This cloud offering has regulatory restrictions to the types of tenants that can use it. ServiceNow's FedRAMP compliant and standard commercial datacenter environments are virtually identical. The differences that do exist, such as only allowing access to specially adjudicated US citizens, exist for regulatory reasons not because the environment is superior in some way.
QTS	QTS assists with mapping between DOD IT RMF/DIACAP and NIST as well as International Standards Organization (ISO) standards and many others. QTS maintains control mappings that include: • NIST 800-53/FedRAMP (Low/Moderate/High)

	• DOD IT RMF/DIACAP (MAC I/II/III Sensitive & Public) • HIPAA-HITECH-Omnibus • PCI-DSS • ISO/NATO • CNSS/ICD/DCID/NISPOM	
SAP	Ariba	We are audited and certified by independent third-party auditor PricewaterhouseCoopers (PwC) for compliance with ISAE 3402 SOC1 Type II, SOC2 and SOC3 every six months. Upon completion of the audit, an attestation letter is issued, stating our compliance. In addition, our primary hosting facility (Equinix) infrastructure is audited for compliance with SSAE 16 SOC1 Type II. The Service Organization Controls report (SOC) is aimed at three different audiences. SOC1 (aimed at financial auditors) is the same type of report as the SAS70 but also includes an attestation letter signed by both our company and the auditor. SOC2 is aimed at IT and security practitioners. The SOC3 is the publicly viewable web seal to show that we have been audited. In addition, we have attained PCI (Payment Card Industry) - DSS (Data Security Standard) certification as a Level 1 Service Provider and compliance with the Visa USA Cardholder Information Security Program (CISP) and MasterCard Site Data Protection (SDP) program. These programs were created specifically for merchants and service providers who process, store, or transmit cardholder data. The PCI DSS is a set of comprehensive requirements for enhancing payment account data security which was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. It was developed to help facilitate the broad adoption of consistent data security measures on a global basis. The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data. CISP and SDP reflect Visa's and MasterCard's respective longstanding commitment to information security.
	Fieldglass	SAP Fieldglass has achieved the following certifications: • ISO 27001 • SSAE 16 SOC 1 and SOC 2 HIPPA Fieldglass does not store Protected Health Information (PHI) on its system and is not required to comply with the Health Insurance Portability and Accountability Act. PCI The Fieldglass application does not process credit card information. We are not (and are not required to be) PCI compliant.
	Hanna	Please see response to 8.6.1
	Hybris	The Savvis datacenter located in Boston, MA is SSAE16 Type II SOC I Compliant. This replaces the older SAS70 Type II audit standard.
	SuccessFactors	We have been audited to the SOC 2 Trust Services Criteria. This signifies that our control objectives and control activities have been examined by an independent accounting and auditing firm, and that these controls fairly presented the controls in operation as of a specific date and were suitably designed to achieve the control objectives. Our SOC 2 audits are conducted semi-annually (May, November) by PricewaterhouseCoopers (PwC). We also hold US Federal FISMA Moderate

		Authority to Operate with both OPM and NTIS. We are compliant with EU Privacy Directive 95/46/EC and are Safe Harbor self-certified. https://safeharbor.export.gov/companyinfo.aspx?id=26196We are aligned with ISO 27001 for Information Security, BS 10012 for Data Protection, and ISO 20000 for Service Delivery to create an Integrated Compliance Framework ("ICF"). Where these standards overlap in subject matter, Information Security ISO 27001 takes precedence. Our Network also complies with Authority to Operate as a Moderate Risk Federal Information System by the Office of Personnel Management and Department of Homeland Security; NIST SP800-53 Security Controls; EU Privacy Directive 95/46/EC for EU and non-EU customer data; Payment Card Industry (PCI) Data Security Standard (DSS) v 2.0; Safe Harbor. We are aligned with ISO 27001 for Information Security, BS 10012 for Data Protection, and ISO 20000 for Service Delivery to create an Integrated Compliance Framework ("ICF"). Where these standards overlap in subject matter, Information Security ISO 27001 takes precedence. Our Network also complies with Authority to Operate as a Moderate Risk Federal Information System by the Office of Personnel Management and Department of Homeland Security; NIST SP800-53 Security Controls; EU Privacy Directive 95/46/EC for EU and non-EU customer data; Payment Card Industry (PCI) Data Security Standard (DSS) v 2.0; Safe Harbor.
VMware	VMware IaaS Services ISO/IEC 27001: ISO/IEC 27001 is a globally recognized standard for the establishment and certification of an information security management system (ISMS). vCloud Air continues to maintain a current ISO/IEC 27001 Certification and has recently issued updated certification for ISO/IEC 27001:2013. Achieving certification means that VMware has implemented a holistic security program that conforms with the ISO 27001 standard requirements, both in the security management system and control activities. The audit of the ISMS was completed by Brightline CPAs and Associates - an ANAB accredited certification body. HIPAA: The Health Insurance Portability and Accountability Act of 1996(HIPAA), which has incorporated requirements from the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009, established national standards for the security and privacy of Protected Health Information (PHI) in the United States. To help customers comply with HIPAA, VMware offers a Business Associate Agreement (BAA) to all interested customers using our US-based data centers. The BAA was designed in conjunction with a leading law firm with expertise in HIPAA and provides fair and reasonable terms for healthcare providers, insurers, and other organizations. VMware has completed an independent third party examination of vCloud Air against applicable controls of HIPAA. SOC 1 (SSAE16/ISAE 3402): Service Organization Control (SOC) 1 reports are conducted in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 16 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPS). The SOC 1 framework reports on internal controls over financial reporting for any service organization such as VMware vCloud Air. SOC 1 aligns to the International Standard on Assurance Engagements (ISAE) 3402 international reporting standards. SOC 1 examinations are specifically intended to meet the needs of the managements of vCloud Air's customers and vCloud Air's customers' auditors, as they evaluate the effect of the controls at vCloud Air on the clients' financial statement assertions. VMware has completed an independent third-party examination of vCloud Air which spans a twelve (12) month review period. SOC 2: The Service Organization Control 2 (SOC 2) report is composed of a comprehensive set of criteria on security, availability, processing integrity, confidentiality, and privacy and is similarly set forth by the America Institute of Certified Public Accountants (AICPA). The SOC 2 reports are

	intended for use by stakeholders (e.g. customers, regulators, business partners, suppliers, directors) of the service organization that have a thorough understanding of the service organization and its internal controls. VMware has completed an independent third-party examination of vCloud Air that also spans a twelve (12) month review period. SOC 3: Trust Services Report for Service Organizations Control 3 (SOC 3) reports are designed to meet the needs of customers who want assurance on the controls at a service organization related to security, availability, processing integrity, confidentiality, or privacy. vCloud Air has completed an independent third-party SOC 3 examination of VMware vCloud Air. SOC 3 is composed of a comprehensive set of trust principles including security, availability, processing integrity, confidentiality and privacy. Cloud Security Alliance: VMware vCloud Air has completed the Cloud Security Alliance (CSA) Consensus Assessments Initiative Questionnaire (CAIQ). CAIQ provides industry-accepted ways to document what security controls exist in IaaS, PaaS and SaaS offerings. FedRAMP Provisional Authority: VMware vCloud Government Service, provided by Carpathian, now has FedRAMP Provisional Authority to Operate issued by the Joint Authorization Board (JAB). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a ""do once, use many times"" framework that can reduce government organizations' costs, time, and staff required to conduct redundant agency security assessments. U.S. government agencies can now leverage vCloud Government Service to meet the stringent security and privacy requirements of FedRAMP. FIPS 140-2: VMware vCloud Government Service is fully FIPS 140-2 compliant including hardware which provides its 2-Factor Authentication capabilities. FIPS Pub 199: As discussed previously, vCloud Government Services is certified to store and secure Low Risk Data and Moderate Risk Data as defined by FIPS Pub 199. VMware is willing to work with participating States that require High Risk Data Storage to enhance vCloud Government Services to store and secure this data. FIPS Pub 199: As discussed previously, vCloud Government Services is certified to store and secure Low Risk Data and Moderate Risk Data as defined by FIPS Pub 199. VMware is willing to work with participating States that require High Risk Data Storage to enhance vCloud Government Services to store and secure this data. CJIS: vCGS recently underwent a CJIS assessment by CoalFire, Inc. CJIS is not a certification, it is a policy that must be followed and accredited for each deployment which requires it. The goal of VMware's CoalFire assessment was to create a baseline configuration that can be reused across any CJIS opportunity to accelerate the implementation and accreditation timeframes. FERPA: Like CJIS, FERPA compliance is assessed and confirmed for each deployment that requires it. VMware's vCloud Government Service FedRamp certification and others provide evidence that the underlying infrastructure is capable of meeting rigorous information security and availability requirements. VMware will work with Participating Entities to meet FERPA requirements on a task order basis. PCI Data Security Standards (DSS): Neither vCloud Air nor vCGS are currently PCI certified at this time. VMware will work with Participating Entities to meet PCI requirements on a task order basis. IRS Publication 1075: Because both IRS 1075 and FedRAMP are based on NIST 800-53, the compliance boundary for IRS 1075 is the same as the FedRAMP authorization. This, vCGS complies with IRS Publication 1075 on the basis that it is FedRAMP certified. FISMA: vCGS is FISMA Low and Moderate compliant.

	NIST 800-53: NIST 800-53 provides the core controls that must be met to achieve FedRAMP compliance. VMware vCloud Government Service has FedRAMP Provisional Authority to Operate issued by the Joint Authorization Board (JAB), thus we are compliant with NIST 800-53. NIST SP 800-171: VMware vCloud Government Service has FedRAMP Provisional Authority to Operate issued by the Joint Authorization Board (JAB). NIST 800-171 outlines a subset of the NIST 800-53 requirements, and as stated above, VMware vCloud Government Service is compliant with these guidelines. Since NIST 800-171 outlines a subset of the NIST 800-53 requirements, VMware vCloud Government Service is compliant with NIST SP 800-171. FIPS 200: Neither vCloud Air nor vCGS are currently FIPS 200 certified at this time. VMware will work with Participating Entities to meet PCI requirements on a task order basis. VMWare AirWatch The AirWatch Information Security Program is built on the security framework laid out in NIST 800-53. Although AirWatch is not required to register with any regulatory agencies, we provide a suite of tools for our customer's to maintain industry-relevant compliance guidelines within their mobile device fleets. AirWatch has recently been awarded the HP-IAPP Privacy Innovation Award for Most Innovative Privacy Technology by the International Association of Privacy Professionals (IAPP) for our commitment to delivering an EMM platform focused on end-user privacy. To help ensure the confidentiality, integrity, and availability of our cloud offering, we comply with the European Data Protection Directive (95/46/EC) and our top-tier data center partners have undergone SSAE16 SOC2 Type II audits.
FireEye	Currently the standards that apply are SSAE 16 SOC 2 Type 2, with a FedRAMP ATO in place and full FedRAMP certification in process. We are also in the process of becoming FedRAMP ISO 2700x certified.
VirtueStream	Security is the foundation of our business. Virtustream's xStream™ cloud software assists our customers to meet mandatory Legislative requirements, and achieve and maintain SSAE16, ISAE3402, PCI-DSS 3.0, FISMA, ISO 27001-2005/2013, ISO 9001-2008, HIPAA, CSA STAR and other leading cloud certifications and compliance frameworks in the customer's own environment (when coupled with identified operational and management controls).

8.6.3 Offeror must describe its security practices in place to secure data and applications, including threats from outside the service center as well as other customers co-located within the same service center.

CA	APM	CA technologies understands that security is a top concern when evaluating cloud-based applications, which is why CA technologies operations worldwide conform to rigorous certification, compliance and security programs and processes. In addition, we contract with independent auditors to regularly evaluate and validate the security of our service. High risks are identified, validated and remediated before production systems are made available. Medium risks are evaluated and resolved on a priority basis.
	MAA	All MAA core servers are behind firewalls; only systems administrators have access to the servers; all data is encrypted when transmitted between data centers. The MAA dashboard and API are protected with HTTPS/TLS encryption, and users are required to authenticate in order to access these.
	CA Agile	We use a co-located data center provider and within that environment we have a dedicated cage to which only our Operations Team has access. We also monitor all traffic across our systems using HIDS (OSSEC) and NIDS (Snort) to notify of any suspicious activity.
	ASM	All ASM core servers are behind firewalls; only systems administrators have access to the servers; all data is encrypted when transmitted between data centers. The ASM dashboard and API are protected with HTTPS/TLS encryption, and users are required to use a username and password to login to their accounts.

Google	In this DPA the obligations of Google to hold all customer data as confidential and wholly owned by the customer is detailed. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. Google aims to design its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing RSA keys are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords; two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; a need to know basis; and must be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include password expiry, restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g., credit card data), Google uses hardware tokens.
AODocs	AODocs being built in Google AppEngine and Google Drive.
Virtru	Please see the Virtru Security Policies and Procedures and the Virtru Privacy Policies and Procedures provided in the Supplemental Information section of this response.
Salesforce	Government Trusted Security and Infrastructure Salesforce understands that the confidentiality, integrity, and availability of our customers' information are vital to their business operations and our own success. We use a multi-layered approach to protect that key information, constantly monitoring and improving our application, systems, and processes to meet the growing demands and challenges of security. Independent audits confirm that our security goes far beyond what most companies have been able to achieve on their own. Using the latest firewall protection, intrusion detection systems, and TLS encryption, Salesforce Force.com gives you the peace of mind only a world-class security infrastructure can provide. Third-party validation Security is a multidimensional business imperative that demands consideration at multiple levels, from security for applications to physical facilities and network security. In addition to the latest technologies, world-class security requires ongoing adherence to best-practice policies. To ensure this adherence, we continually seek relevant third-party certification, including ISO 27001, the SysTrust audit (the recognized standard for system security), and SSAE 16 SOC 1 audit (an examination and assessment of internal corporate controls, previously known as SAS 70 Type II). SOC1, SOC2 and SOC3 audits are performed by third party auditor annually at a minimum. Additional audits and certifications include: CSA 'Consensus Assessments Initiative', JIPDC (Japan Privacy Seal), Tuv (Germany Privacy Mark), and TRUSTe. Protection at the application level

	Salesforce protects customer data by ensuring that only authorized users can access it. Administrators assign data security rules that determine which data users can access. Sharing models define company-wide defaults and data access based on a role hierarchy. All data is encrypted in transfer. All access is governed by strict password security policies. All passwords are stored in SHA 256 one-way hash format. Applications are continually monitored for security violation attempts. Protection at the facilities level Salesforce security standards are stringent and designed with demanding customers in mind, including the world's most security-conscious financial institutions. Authorized personnel must pass through five levels of biometric scanning to reach the Salesforce system cages. All buildings are completely anonymous, with bullet-resistant exterior walls and embassy-grade concrete posts and planters around the perimeter. All exterior entrances feature silent alarm systems that notify law enforcement in the event of suspicion or intrusion. Data is backed up to disk or tape. These backups provide a second level of physical protection. Neither disks nor tapes ever leave the data center. Protection at the network level Multilevel security products from leading security vendors and proven security practices ensure network security. To prevent malicious attacks through unmonitored ports, external firewalls allow only http and https traffic on ports 80 and 443, along with ICMP traffic. Switches ensure that the network complies with the RFC 1918 standard, and address translation technologies further enhance network security. IDS sensors protect all network segments. Internal software systems are protected by two-factor authentication, along with the extensive use of technology that controls points of entry. All networks are certified through third-party vulnerability assessment programs. Secure Data Centers Data centers provide only power, environmental controls, and physical security. Salesforce employees manage all other aspects of the service at the data centers. Colocation data center personnel do not have network or logon access to the Salesforce systems. Colocation personnel have physical access to the Salesforce secure server room in the event of an emergency, but do not have keys to the individual racks containing hardware. Data centers maintain a common baseline of physical and environmental controls across data centers. The exterior perimeter of each anonymous data center building is bullet resistant, has concrete vehicle barriers, closed-circuit television coverage, alarm systems, and manned 24/7 guard stations that together help defend against non-entrance attack points. Inside each building, multiple biometric scans and guards limit access through interior doors and to the Salesforce secure rooms at all times. Access to Salesforce's secure server rooms in the datacenter is authorized based on position or role. Additional access controls enforced by an electronic key box are implemented for the dedicated Salesforce Government Cloud racks to ensure that access is limited to Qualified U.S. Citizens. Salesforce has an established process to review data center access logs to the server room. Additionally, an at least annual assessment of the data center is performed to ensure the data centers are meeting Salesforce's security control requirements. In addition to securing the data center locations, it is critical that the data center facilities maintain robust critical infrastructure to support Salesforce through the following services:

	Temperature and Humidity Controls • Humidity and temperature control • Redundant (N+1) cooling system Power • Underground utility power feed • Redundant (N+1) CPS/UPS systems • Redundant power distribution units (PDUs) • Redundant (N+1) diesel generators with on-site diesel fuel storage Secure Network Logistics • Concrete vaults for fiber entry • Redundant internal networks • Network neutral; connects to all major carriers and located near major Internet hubs • High bandwidth capacity Fire Detection and Suppression • VESDA (very early smoke detection apparatus) • Dual-alarmed, dual-interlock, multi-zone, pre-action dry pipe water-based fire suppression
ServiceNow	The ServiceNow cloud is built for the enterprise customer with every aspect aimed towards meeting the customer's demand for reliability, availability and security. ServiceNow's comprehensive approach to address this demand is enabled by the following: (a) ServiceNow's robust cloud infrastructure runs on its own applications and utilizes industry best-of-breed technology to automate mission critical functionalities in the cloud service with around-the-clock and around-the-world delivery; (b) ServiceNow achieves flexibility and control in its ability to deliver a stable user experience to the customer by having a logical single tenant architecture; (c) ServiceNow's application development which has a paramount focus on quality, security, and the user experience is closely connected to the operations of delivering those applications in a reliable and secure cloud environment; (d) ServiceNow invests in a comprehensive compliance strategy that allows its customers to attain their own compliance to applicable laws by obtaining attestations and certifications and running its subscription service from paired data centers situated close to where its customers are located; and (e) ServiceNow's homogeneous environment where all applications are on a single platform offers ServiceNow a competitive advantage in being able to concentrate its efforts to make the customer's user experience the best possible. The "Data Security Guide" contained within the "Subscription Service Guide" included with this response describes the measures ServiceNow takes to protect Customer Data when it resides in the ServiceNow cloud.
QTS	The QTS Information System Security Officer (ISSO) develops, disseminates, annually reviews and updates a formal, documented access control policy; System and Communications Protection and addresses the following: •Purpose and scope •Roles, responsibilities •Compliance QTS develops, disseminates, and annually reviews/updates a formal, documented security policy executive summary, SP Executive Summary - Information System Security Program Policies, which addresses: •management commitment •coordination among customer entities

	QTS cloud's Policies are maintained within a biometric secure office located in the Suwanee facility at 300 Satellite Blvd, Suwanee, GA 30024. It is disseminated to all individuals, including but not limited to employees, contractors, consultants, temporaries, and other personnel affiliated with third parties, who use any QTS Information Resource that is owned or leased by QTS. This policy is consistent with QTS's mission and functions and with applicable laws, directives, policies, regulations, standards, and guidance. The previously mentioned artifacts are disseminated via a centralized secure document repository among all QTS cloud's personnel who have any service operations or service delivery role for QTS cloud's IaaS offerings system environments, and is to be individually or by group reviewed semi-annually, especially by any personnel who have administrative access. QTS can provide its Information Security Policies as required: • IT_POL_03_System_and_Communications_Protection_Policy (v1.2 – 1/17/14)	
SAP	Ariba	We are committed to the security and integrity of customer information. We utilize security measures to protect against the loss, misuse or alteration of the information under our control. To prevent unauthorized access, maintain data accuracy, and facilitate the correct use of information, we have put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information we collect within the solution.
	Fieldglass	Please see the Fieldglass Security and Hosting Overview provided in the Supplemental Information section of this response.
	Hanna	Communication between data centers is via VPN or MPLS; VPN is encrypted by default and MPLS can be encrypted as well. Internet facing customer systems are protected by perimeter protection systems using technologies such as web application firewall (WAF) or intrusion prevention systems (IPS). Perimeter protection systems operate by monitoring traffic and blocking attaches towards SAP HANA Enterprise Cloud customer systems.
	Hybris	Both IDS and IPS are included the SAP Hybris Commerce, Cloud Edition The security infrastructure includes firewall security and hardened security policies on all servers. Log management procedures are in-place for log review for firewall, applications, network devices, including file-integrity management. SAP Hybris utilizes technologies from leading security firms for Log Management and File Integrity Management. SAP Hybris employs two-factor authentication across its network. SAP Hybris undergoes vulnerability and penetration testing. SAP Hybris validates against requirements for PCI DSS 2.0. The infrastructure also includes Web Application Firewalls and DDoS Mitigation Services. In addition, security policies and change management policies are in-place ensuring that all access and changes to customer systems and information is accessible only by SAP Hybris staff with access authorization. Security of the software application which is controlled by the Customer (or its implementation partner) remains the responsibility of the Customer.
	SuccessFactors	Technologies and measures used to help protect the security of customer data include: Redundant firewalls in a dedicated environment Network intrusion detection to help guard against attacks by monitoring all data center traffic around-the-clock and notifying operations and security teams in the event of an imminent threat Vulnerability scanning to proactively test internet-connected web servers by searching for weaknesses in the same way that a hacker would

		Penetration testing at least annually Security teams monitoring the infrastructure 24x7x365 Any security issues discovered are reported in real time to information security staff and IT management, entered into our ticketing system for follow-up investigation, and tracked to resolution. All actions taken to resolve the problem are documented, allowing all problems to be tracked to completion. We provide application level memory separation between each client instance as well as data level segmentation and separation with each customer's data residing in its own schema and table space at the database tier. The database tier provides isolation and security of data, and the use of application clustering provides availability, reliability and scalability. Each customer's data is maintained in a separate database schema with its own discrete set of tables, facilitating a high degree of data isolation thus preventing potential for data segmentation breaches Flexibility to backup individual customer table spaces without affecting adjacent customers Each schema has separate authentication credentials and assigned resource profile to restrict access rights and resource consumption
VMware	The VMWare Approach to Compliance Many organizations have initiatives to virtualize their Information Technology (IT) infrastructure, or to move to a Cloud Computing model. However, these initiatives are often complicated by the increasing number of regulatory compliance requirements, which require protection of data such as PCI, HIPAA, FISMA, DIACAP, FedRAMP, GLBA, and other State and Federal requirements. Organizations are increasingly concerned with the complexity, risk, and impact that a new technology can bring to their existing environments. VMware addresses these challenges by establishing a Compliance Reference Architecture Framework (RAF) that provides a consistent method for VMware, its partners, and customers to assess and evaluate the impact of regulations on virtual and cloud environments. The intent of the RAF is to provide a single framework for VMware, its partners, and organizations to address a variety of compliance requirements across an IT infrastructure. We designed our security architecture using a defense-in-depth approach to implement multiple layers of security throughout the SaaS environment and to mitigate any potential attacks through multiple safeguards, including: • Access control mechanisms, firewalls, anti-virus/malware software, auditing mechanisms, network controls, maintaining defined configuration settings, etc. We perform regular internal scans to assess the vulnerability of our internal network.	
FireEye	All data is stored within locked and monitored cages in secure data centers. Customer data is restricted to a need to know basis. Data is logically tagged and virtually segregated in our cloud services. Access is managed and only given to those with need to know including internal employees and customers.	
VirtueStream	All data for this environment will remain in the United States. Customers can elect Intel's TxT technology to demonstrate geo-fencing of data to specific data centers. Virtustream data centers are physically accessible by designated employees and approved employees only. Virtustream employees who are assigned to the data center are issued a proximity card which is required to access the data center. Once inside, physical access to the data processing areas is further restricted to specific employees. Physical access to the data processing areas is protected by biometric locks on the doors. Data center personnel maintain a list of all approved personnel who have access to the data center offices and who have access to the data processing areas. Virtustream offers security solutions which customers can select to protect their data while in transit and at rest. Customers are responsible for the protection of their data within their customer	

	zone. Virtustream does not process, store, or disseminate customer data within the Virtustream-controlled management zone. Virtustream invokes a defense-in-depth model for monitoring the management zone with tools such as Splunk, Trend Micro, Fortinet, and Tenable. These tools are available for customers to select as a managed service.

8.6.4 Offeror must describe its data confidentiality standards and practices that are in place to ensure data confidentiality. This must include not only prevention of exposure to unauthorized personnel, but also managing and reviewing access that administrators have to stored data. Include information on your hardware policies (laptops, mobile etc).

CA	APM	All personnel with access to client data undergo annual, mandatory security training and are covered under the CA Technologies NDA. Violations of security policies are grounds for termination. All access to data and other resources used to deliver the service are granted under the least principle.
	MAA	Customer accounts are password protected, and users can only access their data in their accounts. System administrators have access to MAA servers, and database administrators have access to database servers. Account access is reviewed periodically.
	CA Agile	All customer data is treated as confidental and as a policy we do not access customer data without explicit written consent. Access to systems containing customer data is restricted to our Operations Team according to our Elevated Permissions Policy.
	ASM	Customer accounts are password protected, and users can only access their data in their accounts. System administrators have access to ASM servers, and database administrators have access to database servers. Account access is reviewed periodically. All data on CA laptops are encrypted and a PIN is required to boot.
AODocs	The data stored in Google AppEngine are backed up every day. The application is hosted on Google Cloud Platform infrastructure and benefits from the network security.	
Virtru	See 'Virtru Security Policies and Procedures' and 'Virtru Privacy Policies and Procedures'	
Salesforce	Logical Access Control Salesforce provides contractual assurance to its customers that the data hosted in the Salesforce Services will be kept confidential and not accessed except under narrow circumstances (such as a support issue) and only for a set amount of time chosen by customer. In such circumstances, we will access your org only with prior approval and subject to a Non-Disclosure Agreement (NDA). To protect against access through the application, Salesforce employees don't have access at the application level for any customers, unless the customer grants access through the "login as" feature. Access to the production environment infrastructure is restricted to a very limited number of full-time Salesforce employees required to manage the service. Salesforce's Technical Operations team and Release Managers have logical access to servers. These employees must authenticate to the production environment via a secure server (Secure Global Desktop) using 2 points of RSA two-factor authentication. This tool provides pixel data only to these administrators. Systems access is role-based and controlled and logged. DBAs do not have login access to customer's instances (org) and do not see customer data in an assembled manner. They manage the system in aggregate-performance tuning, allocating space, building indices, etc. The Oracle tables and rows in our infrastructure do not reflect the view of a single customer instance (org) since we are multi-tenant and the data is spread across multiple disk arrays.	

	Database administrator account activity is logged. These logs are sent to the security information and event management (SIEM) system. These database activities logs are reviewed for appropriateness by the Computer Security Incident Response Team (CSIRT) team on a regular basis. This log data is also available as a forensic audit trail to support CSIRT during incident investigations. A customer's instance (org) of Salesforce is an aggregate of the raw data. The data model is very complicated, normalized, and the rows are identified by base62 encoded keys (primary and foreign). Re-establishing data ownership and a business context for the data would be very difficult to do at the database level. In order to reassemble any given customer's application (org), someone would need access to our source code in order to reassemble the raw data in a manner that could be interpreted and understood, and would need the entire set of tapes or disks/arrays supporting a given Instance, as the data for any one customer is spread across several tapes/disks. Data center engineers with physical access to the servers do not have logical access to the production environment and administrators with logical access to the systems do not have physical access to the data centers.	
ServiceNow	ServiceNow applies the same data classification for all hosted customer data. ServiceNow does not inspect or monitor its customers' information and therefore has no ability to sub-classify customer data. The overriding requirement of the assigned classification is that customer data remains hosted in the private cloud until the customer terminates their subscription. It is never stored anywhere apart from the private cloud. Customers remain the data owner and data controller for all data placed into their instance. ServiceNow does not examine, inspect, monitor or analyze customers' data. Customers apply access controls to restrict access to data within their instances based on their own requirements and needs, including their own data classification.	
QTS	The customer will be assigned one or more Org Administrators. All users will be configured with RSA AD two-factor Risk Based authentication as a requirement for cloud portal access.	
SAP	Ariba	We participate in the following national and international standards committees: WebTrust: (2001 - current) The Security, Availability, Processing Integrity and Confidentiality of our applications are based on the Trust Services Principles now incorporated into the SSAE16/ISAE 3000 SOC 2 standards SSAE16: (formerly SAS 70) certification: (Since 2011) ISAE 3402: (The International Standard on Assurance Engagements since 2014) every six months we undergo a rigorous ISAE 3402 audit by independent auditor PricewaterhouseCoopers (PwC) Payment Card Industry (PCI) Data Security Standard (DSS): (Since 2008) we have adopted and adhere to the PCI-DSS). PCI certification and compliance with the Visa USA Cardholder Information Security Program (CISP) and MasterCard Site Data Protection (SDP) program Safe Harbor: (Since 2007) Current on the Safe Harbor list for ""Online Data"" for the ASN and Cloud Solutions/Services A firewall separates the Ariba corporate network from Ariba infrastructure computers. Therefore, unauthorized Ariba employees cannot access Ariba data from the Ariba corporate network infrastructure. Access is limited to specific roles or functions within Ariba Operations. Additionally, access is managed on an "exception" basis whereby personnel need clearance to be

		authorized. Access is time-limited, after which time re-authentication is required. Internally, we have deployed an active monitoring system tied back to Human Resources. Logical access management reports are rolled up monthly and are part of the monthly Privacy & Security board review. All logical access management is subject to review and audit under ISAE 3402 assurance every six months and annually under PCI DSS certification. Wireless technology is not allowed within the production operations infrastructure where customer data is received, processed and stored. All corporate laptops are whole disk encrypted. All approved portable devices are encrypted and have a phone home capability which allows them to be wiped remotely.
	Fieldglass	Fieldglass has the following categories for classifying information: Confidential - This is the information that Fieldglass and end users have a legal, regulatory and/or contractual obligation to protect or information that unauthorized disclosure, compromise, or destruction that results in severe damage, provides significant advantage to a competitor, or incurs serious financial impact to Fieldglass and/or our customers. Fieldglass will not disclose to a third party without signing a nondisclosure agreement requiring the third party to protect such information. Internal Use - This is information that, due to a technical or business sensitivity, requires special precautions to ensure the confidentiality and integrity of data by protecting it from unauthorized access, modification or deletion. This information is intended for use only within the company and must be limited to end users who are employed by Fieldglass or individuals that have a business requirement to access the data and have signed a non-disclosure agreement. Public - This information has been made available for public distribution through authorized company channels. Public information does not require special protection. It is information that can be disclosed to anyone without violating an individual's right of privacy. Knowledge of this information does not expose Fieldglass to financial loss, embarrassment, or jeopardize the security assets. Laptops Every Fieldglass laptop issued to employees and contractors have a DLP agent installed that cannot be modified. This agent detects whether customer data or the Fieldglass source code is being copied externally. Monthly access reviews are conducted by product and file share owners to ensure access is limited to a need-to-know basis. Privileged user account access is also monitored on a weekly basis.
	Hanna	SAP treats all customer data stored in cloud solutions from SAP as "Confidential" according to SAP's data classification standard. Personal Data is subject to strict security and legal requirements in the legislation of several countries, for example handling of Personal Data is regulated in the European Union (EU) Data Protection Directive and

		corresponding national laws. At SAP intercompany agreements exist, to ensure that these requirements are met in all SAP companies and branch offices throughout the world. Similar data protection agreements were executed with all subprocessors. Personal data must be classified as equally confidential regardless of whether it relates to employees, customers or third parties.
	Hybris	The security infrastructure includes firewall security and hardened security policies on all servers. Log management procedures are in-place for log review for firewall, applications, network devices, including file-integrity management. SAP Hybris utilizes technologies from leading security firms for Log Management and File Integrity Management. SAP Hybris employs two-factor authentication across its network. SAP Hybris undergoes vulnerability and penetration testing. SAP Hybris validates against requirements for PCI DSS 2.0. The infrastructure also includes Web Application Firewalls and DDoS Mitigation Services. In addition, security policies and change management policies are in-place ensuring that all access and changes to customer systems and information is accessible only by SAP Hybris staff with access authorization. Security of the software application which is controlled by the Customer (or its implementation partner) remains the responsibility of the Customer.
	SuccessFactors	We are aligned with ISO 27001 for Information Security, BS 10012 for Data Protection, and ISO 20000 for Service Delivery to create an Integrated Compliance Framework ("ICF"). Where these standards overlap in subject matter, Information Security ISO 27001 takes precedence. Our Network also complies with Authority to Operate as a Moderate Risk Federal Information System by the Office of Personnel Management and Department of Homeland Security; NIST SP800-53 Security Controls; EU Privacy Directive 95/46/EC for EU and non-EU customer data; Payment Card Industry (PCI) Data Security Standard (DSS) v 2.0; Safe Harbor.
VMware	VMware monitors for security events involving the underlying infrastructure servers, storage, networks, and information systems used in the delivery of vCloud Air over which VMware have sole administrative level control. The goal of this process is to identify security incidents and respond to them proactively. This responsibility stops at any point where customers have control, permission, or access to modify any aspect of the service offering. The customer is responsible for the security of the networks over which they have administrative level control. This includes, but is not limited to, maintaining effective firewall rules, exposing communication ports that are only necessary to conduct business, locking down promiscuous access, and other such capabilities. Proactive Security Monitoring over Internet and Social Media (e.g. searching filesharing sites for customer data, seeding data with honey tokens) VMware security teams perform OSINT monitoring on the Internet for all VMware products and services. This includes harvesting data from search engines, le sharing, and social networking sites. This data is analyzed for keywords and other specific indicators. With regards to potential data leaks, the customer is solely responsible for protecting the security of his or her content, including any access provided to employees, customers or third parties. vCloud Air provides certain software and functionality to help protect content from unauthorized access such as firewalls, load balancers, and IPsec VPNs. Customers are encouraged to deploy additional security mechanisms similar to what exists in their current data center to address other security controls such as data encryption, intrusion detection, le integrity monitoring, and other such concerns relevant to the sector and regulatory requirements that apply to the specific business of a customer.	

FireEye	FireEye has mature and well documented security and privacy programs. The programs include third party certifications for SSAE 16 SOC 2, and FedRAMP certifications, Model clauses, Privacy and Security Standards among others. The data that FireEye receives is only in conjunction with the malware analysis. Our data protection standards includes prevention of exposure to unauthorized personnel and managing and reviewing all access to systems (not just for admin) quarterly or when employees have a role change. FireEye has standards for hardware and software such as gold images for all operating systems and hardened systems, these are managed and distributed centrally. It also includes supported and managed configurations of hardware and software on mobile devices and acceptable use policy for all FireEye resources.
VirtueStream	Customers are responsible for the protection and confidentiality of data within their application and/or system which resides on the Virtustream IaaS. Virtustream customers are logically separated via VLAN and VRF technologies which ensure that different customers' data is not accessible and cannot be altered. Customers are responsible for controlling access to their data. Virtustream does not have direct access to customer data within their customer zone. Virtustream employees who are assigned to IaaS must pass a Virtustream background investigation. In addition, Virtustream employees assigned to the IAAS must adhere to any requirement by customers to pass federal, state, or local background investigations if they are to provide managed services to the customer zone. Virtustream offers an encryption at rest and encryption in transit managed service. This provides an additional level of protection for customer's data within their VLAN, All Virtustream employees with access to the IaaS are required to have hard drive encryption on their laptops. Virtustream performs quarterly privileged user access reviews.

8.6.5 Offeror must provide a detailed list of the third-party attestations, reports, security credentials (e.g., FedRamp), and certifications relating to data security, integrity, and other controls.

CA	APM	AWS EC2 datacenters annually undergo SOC 3 audits.
	MAA	CA MAA is certified for SOC 2 Type 1 Security Audit.
	CA Agile	N/A - we are working towards a NIST 800-53r4 certification but that is not yet complete.
	ASM	Rackspace datacenters annually undergo various certification including SOC 3 audits. The application currently does not hold a Soc 2 attestation.
Google	SOC 1 (SSAE 16) SOC 2 SOC 3 ISO 27001 ISO 27018 FedRAMP	
AODocs	AODocs is certified SOC2 Type 2	
Virtru	Vulnerability Scan and Penetration Testing by Cigital and FedRamp In Process sponsored by US Department of Interior	
Salesforce	Salesforce has comprehensive privacy and security assessments and certifications performed by multiple third parties. The following audits and their frequencies are performed: ISO 27001 - Annually (3 year certification) PCI-DSS - Annually FedRAMP - Annually SOC 1 (SSAE16/ISAE 3402, previously SAS 70) - Twice a year SOC 2 & SOC 3 - Twice a year Copies of our SOC reports can be provided to your Agency upon request and under NDA.	

	Under NDA, your Agency can also be provided Salesforce's complete FedRAMP Authority to Operate (ATO) package, which contains the following security assessment documentation: 01 - Salesforce Government Cloud System Security Plan 02 - Salesforce Government Cloud System Security Plan - Tracked Changes 03 - Salesforce Government Cloud Attachment 1 - Control Tailoring Workbook (CTW) 04 - Salesforce Government Cloud Attachment 2 - Control Implementation Summary (CIS) 05 - Salesforce Government Cloud Attachment 3 - PTA and PIA 06 - Salesforce Government Cloud Attachment 4 - E-Authentication 07 - Salesforce Government Cloud Attachment 5 - FIPS 199 Categorization 08 - Salesforce Government Cloud Attachment 6 - User Guide - Customer Configurations 09 - Salesforce Government Cloud Attachment 7 - Hardware, Network, and Software System Inventory 10 - Salesforce Government Cloud Attachment 8 - Customer Responsibilities 11 - Salesforce Government Cloud Rules of Behavior - Ground Rules for Security Success 12 - Salesforce Government Cloud Disaster Recovery Plan 13 - Salesforce Government Cloud Incident Response Plan 14 - Salesforce Government Cloud Configuration Guide 15 - Salesforce Government Cloud Continuous Monitoring Plan 16 - Salesforce Government Cloud Security Assessment Plan 17 - Salesforce Government Cloud Security Assessment Report (SAR) 18 - Salesforce Government Cloud Table 4.1 SAR 19 - Salesforce Government Cloud Test Cases (SRTM) 20 - Salesforce Government Cloud POA&M	
ServiceNow	•ISO/IEC 27001:2013 BrightLine Certificate Number 1980700-4 (see supplemental information section for official certificate) •SSAE 16 SOC 1 Type 2 (available under NDA) •SSAE 16 SOC 2 Type 2 (available under NDA) •FedRAMP Compliant	
QTS	QTS maintains control mappings that include: • NIST 800-53/FedRAMP (Low/Moderate/High) • DOD IT RMF/DIACAP (MAC I/II/III Sensitive & Public) • HIPAA-HITECH-Omnibus • PCI-DSS • ISO/NATO • CNSS/ICD/DCID/NISPOM	
SAP	Ariba	As assurance collateral, we can provide the BITS SIG and CSA Cloud Service Provider Questionnaire, Our ISAE 3402 SOC 1 Type II, SOC 2 and SOC 3 reports as well as the Attestation of Compliance for PCI DSS are signed by our qualified security assessor and management.
	Fieldglass	Independent third-party auditors conduct annual audits for the following: • ISO 27001 • SSAE 16 SOC 1 and SOC 2
	Hanna	Please see response 8.6.1
	Hybris	
	SuccessFactors	We have various third party certifications including ISO 27001 and BS10012.

VMware	VMware IaaS Services The International Organization for Standardization (ISO) has developed he ISO 27001 standard which defines an information security management system ("ISMS") as a systematic approach to managing sensitive company information so that it remains secure. It includes an organization's people, processes and IT systems and the application of a risk management process. vCloud Air has established and implemented an Information Security Management System (ISMS) based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information. vCloud Air engages an independent third party auditing firm on an on-going basis to validate vCloud's air adherence to the ISO 27001 standard. An ISO 27001 certificate is issued if the auditing firm has validated adherence to the standard. VMware IaaS Services The International Organization for Standardization (ISO) has developed he ISO 27001 standard which defines an information security management system ("ISMS") as a systematic approach to managing sensitive company information so that it remains secure. It includes an organization's people, processes and IT systems and the application of a risk management process. vCloud Air has established and implemented an Information Security Management System (ISMS) based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information. vCloud Air engages an independent third party auditing firm on an on-going basis to validate vCloud's air adherence to the ISO 27001 standard. An ISO 27001 certificate is issued if the auditing firm has validated adherence to the standard. VMware IaaS Services The International Organization for Standardization (ISO) has developed he ISO 27001 standard which defines an information security management system ("ISMS") as a systematic approach to managing sensitive company information so that it remains secure. It includes an organization's people, processes and IT systems and the application of a risk management process. vCloud Air has established and implemented an Information Security Management System (ISMS) based on ISO 27001 standards to manage risks relating to confidentiality, integrity, and availability of information. vCloud Air engages an independent third party auditing firm on an on-going basis to validate vCloud's air adherence to the ISO 27001 standard. An ISO 27001 certificate is issued if the auditing firm has validated adherence to the standard. vCloud Government Service (IaaS): FedRAMP Provisional Authority: VMware vCloud Government Service, provided by Carpathian, now has FedRAMP Provisional Authority to Operate issued by the Joint Authorization Board (JAB). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. This approach uses a ""do once, use many times"" framework that can reduce government organizations' costs, time, and staff required to conduct redundant agency security assessments. U.S. government agencies can now leverage vCloud Government Service to meet the stringent security and privacy requirements of FedRAMP.
FireEye	We have SSAE 16 SOC 2 Type 2 certification for specific cloud services, and associated datacenters. FireEye currently has a FedRAMP ATO for ETP and are in process for full FedRAMP, and ISO 27001 certification.
VirtueStream	Security is the foundation of our business. Virtustream's xStream™ cloud software assists our customers to meet mandatory Legislative requirements, and achieve and maintain FedRAMP, FISMA Moderate, PCI-DSS, SSAE16/SOC2/SOC3, ISO 27001/9001/22301, HIPAA, NIST 800-53, CSA STAR and other leading cloud certifications and compliance frameworks in the customer's own environment (when coupled with identified operational and management controls).

8.6.6 Offeror must describe its logging process including the types of services and devices logged; the event types logged; and the information fields. You should include detailed response on how you plan to maintain security certifications.

CA	APM	CA has various log monitoring tools that help us keep track of live production systems in order to understand load vs. resource utilization vs. performance. CA along with AWS monitors the service and provides real time alerting when systems suddenly die, or when system loads or response times approach critical thresholds. Logs are kept for forensic examination and identification of trends in order to proactively ensure stability.
	MAA	CA MAA servers log all activity, and data retention is anywhere from 14 to 180 days depending on the component and volume of logs generated
	CA Agile	All systems are required to send logs to a centralized log server. At a minimum log data must contain timestamps, usernames, IP Addresses, and query parameters.
	ASM	ASM servers log all activity, and data retention is anywhere from 30 days to 1 year depending on the application and volume of logs generated.
Google	This is largely the responsibility of the customer. Google's obligations, as described in 8.6.4, are to ensure there is no unauthorized access of Customer data. Customers are responsibility for ensuring their end users use the service according to the Customer's acceptable use policies. During the onboard process, Customers will be assisted in the configuration controls that are included to enforce acceptable use and security policies and trained in how to maintain oversight on the ongoing usage of the services in scope.	
AODocs	AODocs does not manage the authentification. The authentification is managed by Google.	
Virtru	See 'Virtru Security Policies and Procedures'	
Salesforce	Salesforce Infrastructure Logs Salesforce internal infrastructure logs are collected by various monitoring tools for activities on the systems that host Salesforce, and include: Server access Network access Firewall management events Network intrusion detection systems traffic Cache Database File integrity Network device configuration Anti-virus detection Log events are correlated to generate alerts. Alerts are configured to notify the Technical Operations and Computer Security Incident Response Team (CSIRT) teams. Security alerts require acknowledgement and follow up, if appropriate by the CSIRT. Firewalls and IDS systems are configured with automated syslog notifications for key events. Logs are archived and are currently stored for a minimum of (1) one year. NOTE: These logs are not available to customers. Customer Auditing Capabilities Within Salesforce, the creator and last updater, as well as timestamps, are recorded for every record. Additionally, the Salesforce Platform and Salesforce Applications have a multitude of history tracking and auditing features that provide valuable information about the use of an	

	organization's applications and data, which in turn can be a critical tool in diagnosing potential or real security issues. Auditing features include: Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information. Login History - You can review a list of successful and failed login attempts to your organization for the past six months within Salesforce. Field History Tracking - You can also enable auditing for individual fields, which will automatically track any changes in the values of selected fields. Although auditing is available for all custom objects, only some standard objects allow field-level auditing. Setup Audit Trail - Administrators can also view a Setup Audit Trail for the past six months within Salesforce, which logs when modifications are made to your organization's configuration. This trail can be downloaded into Excel or as a csv file. While the Login History and Setup Audit Trail are available for six months within Salesforce, audit trails can be downloaded and stored locally to meet longer audit log retention requirements. Detailed application logs can be used for forensics investigations by customers. These logs are stored for 12 months and are available for a fee. Event Monitoring (Additional License Option) In addition to Salesforce's core auditing capabilities, Salesforce also offers Event Monitoring as an additional license option. Your Agency can use event monitoring to discover how often and at what times your users are logging in to and out of your organization. This includes insight into what Salesforce applications are being adopted by users, who is logging in and from where, what pages users are viewing, what reports users are running and exporting and other aspects of application usage. This capability helps you discriminate between valid and invalid login requests and also track user login patterns for future reference. Not only can your Agency now better understand how your apps are being utilized, you can also monitor if users download large amounts of data that might put your agency at risk. In addition, your Agency can also determine if an employee is unnecessarily downloading sensitive customer/citizen information, pinpointing the exact time and location of that event. Event Monitoring is delivered as an API-first feature and there are Salesforce partners with visualization tools available. Use the SOAP API and REST API resources to retrieve event log files that contain information useful for assessing organizational usage trends and user behavior. Because event log files are accessed through the Force.com SOAP API and REST API, you can integrate log data with your own back-end storage and data marts so that you can correlate data from multiple organizations and across disparate systems easily. When using event monitoring, keep the following in mind: - In the unlikely case where no log files are generated for 24 hours, contact Salesforce. - Log data is read-only. You can't insert, update, or delete log data. - Use the EventType field to determine which files were generated for your organization - LogDate tracks usage activity for a 24-hour period, from 12:00 a.m. to 11:59 p.m. UTC time. - An event generates log data in real time. However, log files are generated the day after an event takes place, during nonpeak hours. Therefore, log file data is unavailable for at least one day after an event. - CreatedDate tracks when the log file was generated.

	- Log files, represented by the EventType field, are only generated if there is at least one event of that type for the day. If no events took place, the file won't be generated for that day - Log files are available based on CreatedDate for the last 30 days when organizations purchase User Event Monitoring or one day for Developer Edition organizations. Businesses desire certainty that their data is accurate, complete and reliable, enabling them to meet stringent industry regulations. With Field Audit Trail, customers can track changes at the field level for up to ten years and set different policies for each Salesforce object to ensure data is purged when no longer needed. Life sciences companies running clinical trials in Salesforce, for example, can now maintain a complete audit trail of patient data so they can safeguard the integrity of clinical trial results and comply with FDA regulations. - All event monitoring logs are exposed to the API through the EventLogFile object, however there is no access through the user interface. Event monitoring can be used with 28 different file types: Apex Callout, Apex Execution, Apex SOAP, Apex Trigger, API, Async Report, Bulk API, Change Set Operation, Content Distribution, Content Document Link, Content Transfer, Dashboard, Document Attachment Downloads, Login, Login As, Logout, MDAPI Operation, Multiblock Report, Package Install, Report, Report Export, REST API, Salesforce1, Adoption (UI Tracking), Sandbox, Sites, Time-Based Workflow, URI, Visualforce. Event Monitoring Transaction Security Transaction Security policies give your Agency a way to look through events in your organization and specify actions to take when certain combinations occur. A transaction security policy consists of events, notifications, and actions. Transaction Security monitors events according to the policies that your Agency sets up. When a policy is triggered, you can receive a notification and have an optional action taken. For example, suppose that you activate a policy to limit the number of concurrent sessions per user to three. A user with three login sessions tries to create a fourth session. Your Agency can require a user to end one of their existing sessions before proceeding with the new session. At the same time, you are notified that the policy was triggered.
ServiceNow	The ServiceNow application writes detailed log information that is stored in tables within a customer's instance. As this is customer data in a customer's instance, ServiceNow does not attempt to monitor or view this data unless specifically requested by a customer. As a result the customer is responsible for monitoring the contents of these logs files. The log data is protected in the same manner as all other customer data. Event logs can also be configured to feed into a customer's environment via ServiceNow's Syslog probe allowing the logs to be stored within the customer's environment in a syslog repository or SIEM and retained according to the customer's requirements. ServiceNow's application logging includes verbose transaction logs, these logs are retained within the instance for 30 days. Event logs are stored for seven days and audit histories are retained indefinitely in the instance. Transaction logs represent every click, view, and system event that occurs in an instance and as a result, will grow very large, quickly. They provide a level of detail that is frequently used for troubleshooting issues with an instance. They can also provide detailed intelligence on the behaviors within an instance. These logs can be downloaded to customers' environments, if they need to be retained for longer than 30 days. The event logs on the other hand are less granular; they will include the creation of an incident, or deletion of problem, or any one of the 250 standard events. They may also contain customer

	created events. There are a number of security events as well, including successful login, failed login, security privilege escalation, and viewing of a table. These events can either be monitored manually, generate an Incident based on a parameter or when metric is reached; such as failed logins per minute. The final aspect of logging is the audit history. Audit history may be turned on for any particular table or field. The audit log table then maintains a record of who made changes when to a table or field and what they changed.
QTS	All account activities are logged including account creation, modification, disabling and termination. Logs are monitored and notifications are sent for abnormal activity. Splunk Enterprise is used as the centralized audit log monitoring tool to centrally collect, analyze and reduce the amount of audit logs. As referenced in IT_PRO_07_Audit_and_Accountability_Procedure (v1.0 – 1/20/14), on-site network and security operations monitoring coverage and audit management process; to include analysis, reporting, and alerting into a central repository provided by a highly available Splunk logging service. Splunk logging service supports QTS cloud information systems for organizational–wide situation awareness. Splunk provides built-in capabilities to filter, normalize, and correlate the large amounts of data produced by QTS cloud, and then allows QTS's support staff to use Splunk's built-in capabilities to data mine, log mine, and run pre-developed and ad-hoc reports against the result sets obtained during the data and log mining sessions. Logs are centrally correlated and reviewed from devices across QTS cloud Hosting Environment by QTS's Systems Engineer or designee. Specific report categories include: •Authentication and Authorization Reports • Systems and Data Change Reports •Network Activity Reports •Resource Access Reports •Malware Activity Reports •Failure and Critical Error Reports • Vulnerability Correlations Reports •Anti-Port Correlations Reports •Watch List Correlations Reports
VMware	VMware IaaS Services In accordance with our ISO and SOC commitments, change-related activity, including administrative actions, performed on the management infrastructure layers supporting vCloud Air are monitored and logged to a centralized logging server for a minimum of 1 year. Infrastructure logging is in place for customer interactions with the vCloud Air management and administrative consoles. These logs are only for the management and administrative interfaces. These are not in place for monitoring of individual customer VMs installed within the customer tenant org. Limited logging and activity reporting are available from customer tenant environments, with more detailed reporting, auditing and logging capabilities introduced Q4-2014. VMware AirWatch To enable user accountability, we have full auditing capabilities on all environments in the AirWatch Cloud. Customers can use the built-in event log, customizable dashboards, integrated reporting engine and AirWatch Hub to audit the web console and end-user actions. For the SaaS environment logs, our Information Security Team helps ensure that systems generate audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.
FireEye	FireEye auditing and log review procedures are based on industry best practices and in accordance with regulatory, statutory, contractual and business requirements. Detailed audit

	records (User ID, date, time, type of event, successful/unsuccessful attempts or access secured files and protect the contents of audit trails against unauthorized access, modification or deletion.
VirtueStream	Virtustream offers logging as a managed service to customers as optional solution. The types of services and devices are specified by the customer and a monthly report is delivered to the customer.

8.6.7 Offeror must describe whether it can restrict visibility of cloud hosted data and documents to specific users or groups.

CA	APM	Users of the Portal are divided into two types: Internal users (for publishers of the API) and External users (for developers). There are a number of pre-defined roles for both Internal and External users that inherit functionality in a hierarchical manner. Portal has RBAC built in that allows you to grant access to different functionality for different users. For example, you can assign a user to role that only allows them access to update content, or access apps but not create them.
	MAA	CA utilizes IaaS vendor to host the service with strict access controls in place. CA SaaS InfoSec team manages users and their associations with groups within LDAP Directory and conducts periodic access reviews to conform to governance requirements.
	CA Agile	Our databases are shared but logically segregated. We ensure logical security of access to customer data by implementing access restrictions between subscriptions and roles within those subscriptions to assure adequate segregation of data. There is a plugin available in the unlimited edition that allows the administrator to limit access to the application based on IP address.
	ASM	Only Public Status Page (PSP) data is stored in the cloud, and PSP web pages are accessible by anyone. PSP data is only sent to the cloud if the customer enables this feature, and they can decide which data is made public.
Google	If Google becomes aware of a Data Incident, Google will promptly notify Customer of the Data Incident, and take reasonable steps to minimize harm and secure Customer Data. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address provided by Customer in connection with the Agreement or, at Google's discretion, by direct communication (e.g., by phone call or an in-person meeting). Customer acknowledges that it is solely responsible for ensuring the contact information given for purposes of the Notification Email Address is current and valid, and for fulfilling any third party notification obligations. Customer agrees that "Data Incidents" do not include: (i) unsuccessful access attempts or similar events that do not compromise the security or privacy of Customer Data, including pings, port scans, denial of service attacks and other network attacks on firewalls or networked systems; or (ii) accidental loss or disclosure of Customer Data caused by Customer's use of the Services or Customer's loss of account authentication credentials. Google's obligation to report or respond to a Data Incident under this Section will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.	
AODocs	The AODocs-specific data stored in the Google App Engine Datastore relies on a built-in multi-tenancy feature named "namespace", which define virtual "silos" within the AODocs database. Each customer is assigned a specific namespace (which is in fact the customer's primary Google Apps domain name), and all the customer's data is stored within this namespace.	
Virtru	Key material is encrypted prior to storage, and those keys are backed by HSM. Decryption occurs only for authenticated users	
Salesforce	The multitenant architecture and secure logical controls address separation of customer data. There are no dedicated servers used for individual customers. The Salesforce Services infrastructure is divided into a modular architecture based on "Instance". Each Instance is capable	

	of supporting several thousand customers in a secure and efficient manner. Services are grouped within each Instance; with app, search, and database elements contained. There are appropriate controls in place to ensure that any given customer's org (application) is not compromised. The service has been designed to accomplish this and is robustly tested on an ongoing basis by both Salesforce and its customers.	
ServiceNow	ServiceNow includes built in Role Based Access Control (RBAC) that is based on users, groups and roles. The entitlements granted to users are built from fine grained Access Control Lists (ACLs). ACLs can be built from individual entitlements that include read, write, create, execute and delete as well as a number of other individual attributes. The attributes that are available also vary, depending on the type of object being secured. Customers have full control of the entitlements granted to each of their users and integration with customer side directory service is possible through the use of users, groups and group memberships.	
SAP	Ariba	Within our solution, specific logging takes place that is viewable by the customer administrator or their designee. Audit logs produced through use of the solution are considered customer data and are maintained within the customer's instance of the database. These logs are retained so long as the customer has an active contract with us. As a user control consideration, customers are responsible for monitoring the proper entry of data to the solution and reviewing reports generated by the system.
	Fieldglass	The Fieldglass Audit Trail tracks a date/time stamp for each user as they log in and out of the application. Likewise, Fieldglass tracks a date/time stamp and owner of every transaction that is created, submitted and approved through the application. Similarly, actions that occur within the reporting tool are also tracked, including when reports are created and run and by whom. The audit trail log is visible by the State of Utah program office. Audit trail reports can be created with Fieldglass' ad hoc reporting.
	Hanna	SAP has Security Information and Event Management systems (SIEM) for analysis, reporting and alerting. All critical systems and infrastructure components within the SAP Cloud need to log relevant data, which is stored for a minimum of six (6) months. This is ensured via the security configuration compliance checks and event monitoring. General security monitoring is performed 24x7 for all activities. Resulting warnings and alerts are processed via ticketing system and critical events are handled according to the Incident Management Process.
	Hybris	Log management procedures are in-place for log review for firewall, applications, network devices, including file-integrity management. hybris utilizes technologies from leading security firms for Log Management and File Integrity Management.
	SuccessFactors	The application logs the following for every transaction: Event/transaction Time, Transaction ID, Event/transaction Type, Event/transaction Status (Result of the event; if failure, includes reason), Object Attributes (Describes the object affected by the event), Originator User ID (ID of the user who initiated the event or action), Subject ID, Process User ID, Account Number, Transaction Specific Elements. The application audits changes to the major components. Examples of this are goal auditing and document auditing. The audit trail includes who made the

		change, the date of the change and the ability to see the data as it existed at that point in time. The data in the audit log can be viewed with appropriate permissions. We also provide an optional Audit Framework for additional audit logging capabilities. All audit logs within the application are accessible only by customers. Therefore, the review of application audit logs as well as retention periods for the application audit logs are the customer's responsibility, and can be determined as per requirements. To detect unauthorized information processing activities, systems are monitored and all information security events are recorded. Operator logs and fault logging are used to information system problems are identified. We comply with all relevant legal requirements applicable to its monitoring and logging activities. All system logs are created with "write-once" technology so that they cannot be altered or overwritten. All system logs are maintained for a minimum of 90 days on-line and a minimum of 13 months near-line. Inter host communications are secured by multiple layers of defense including segmented separate VLANS, restricted protocol sharing, multiple levels of stateful firewalls, HOST and NETWORK IDS/IPS and constant vigilant monitoring and testing. In addition, our Operations Team maintains detailed system logs. Our internal system logs successful and unsuccessful requests for access, and our team monitors all system logs for any errors or unusual activity. Activities are logged and reviewed by various mechanisms such as: RSA, SysLog, NIDS, HIDS, OSSIM and database logging. The system logs are not made available to customers but are used to monitor the health of the application and facilitate a high level of performance. Alerts are responded to immediately and logs are analyzed daily for any issues or anomalies. The system level logs are written to servers in the data center then copied to our operations team on an as needed basis. Various logging mechanisms are used to monitor database administration activities. Logging mechanisms include: syslog, alert log and database auditing for the privileged role SYSDBA. All activities are logged under the SYSDBA role which including: start-up and shutdown of the data base, configuration changes to init.ora and also any queries/data extraction. We would be able to identify dba activities by manual review of the logs and database auditing to detect if client data querying has occurred. All audit logs are created with "write-once" technology so that they cannot be altered or overwritten. Controls aim to protect against unauthorized changes and operational problems with the logging facility including: Alterations to the message types that are recorded. Log files being edited or deleted. Storage capacity of the log file media being exceeded, resulting in either the failure to record events or over-writing of past recorded events.
VMware	The vCloud Air Terms of Service and Data Privacy Addendum's establish the line of demarcation between the responsibility of VMware and the customer as it pertains to data protection. In addition, security whitepapers are made available to customers to further illustrate these points or to establish transparency regarding the separation of responsibility between VMware and the customer for compliance programs such as HIPAA or PCI. Subscribers are able to use a VPN connection at multiple layers to maintain data security. For traffic in motion, VPNs can be created for a particular application and also for an entire virtual data	

	center. A site-to-site IPsec-VPN can also be established to securely tunnel the entire virtual data center back to the private data center. For data ""at rest"", subscribers are provided a role-based access control, whereby specified users are not exposed to the entire infrastructure and can be limited to a single or multiple virtual data centers. Further details of the controls in place to limit exposure of these groups to customer data is documented within the ATA 101 and SOC reports, available under NDA. vCloud Air has logically separated networks that restrict Tenant access to only their own private networks. The vCloud Hybrid Service has two offerings: The Dedicated Cloud option provides physically isolated and reserved compute resources from all other vCloud Hybrid Service tenants, as well as a private cloud instance. The Virtual Private Cloud option has a multitenant compute resource mode. Both services have logically isolated networking and storage that ensures secure resource separation. Customers have complete control over the file systems and databases they deploy within the service. Access is technologically enforced and employees are only authorized the level of access to information assets that is required to meet an approved business need or perform prescribed job responsibilities. • Administrative access is limited to only those users that explicitly require privileged access. Customers do not have direct access to the SaaS environment; rather, customers administer the solution via the Web console.
FireEye	Each of the FireEye offerings include strong access controls including role-based access. Only properly authorized individuals on a need to know basis are granted access to data.
VirtueStream	Virtustream does not have access to customer hosted data. Customers control access to their application or system which sits upon the IaaS. Customer would need to create the user in their own Active Directory to allow access by named users of Virtustream for specific system.

8.6.8 Offeror must describe its notification process in the event of a security incident, including relating to timing, incident levels. Offeror should take into consideration that Purchasing Entities may have different notification requirements based on applicable laws and the categorization type of the data being processed or stored.

CA	APM	CA Technologies documents a plan and associated procedures in case of an information security incident. The incident response plan clearly articulates the responsibilities of personnel and identifies relevant parties for notification. All security incidents will be investigated and triaged to understand where the vulnerability exists. Software vulnerabilities will be investigated by CA engineering teams; other vulnerabilities will be addressed by the SaaS Ops team in conjunction with AWS. Affected customers will be notified and given a remediation plan
	MAA	Clients are notified via email of any security incident that resulted in a data breach for that client promptly and no later than 5 days. A root cause analysis is then sent within 30 days. Meeting can be setup upon request.
	CA Agile	We have a defined Incident Handling Guide which outlines the process and responsibilities during breach investigation. Clients are notified via email of any security incident that resulted in a data breach for that client promoptly and no later than 5 days. A root cause analysis is then sent within 30 days. Meeting can be seutp upon request.
	ASM	Clients are notified via email of any security incident that resulted in a data breach for that client promptly and no later than 5 days. A root cause analysis is then sent within 30 days. Meeting can be setup upon request.
Google	Google's focus on security and protection of data is among our primary design criteria. Google data center physical security features a layered security model, including safeguards like custom-	

	designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics, and the data center floor features laser beam intrusion detection. Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are available in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. As you get closer to the data center floor, security measures also increase. Access to the data center floor is only possible via a security corridor which implements multifactor access control using security badges and biometrics. Only approved employees with specific roles may enter. Less than one percent of Googlers will ever step foot in one of our data centers. Google operates a global, multi-tenant environment running the world's second largest IP data network providing customers with a low latency, high performing platform that runs 24x7. Hard Disks are assets that are tracked throughout its lifecycle at Google from arrival to final destruction. These disks are component parts that Google uses to build its own servers from other component parts including motherboards and a harden, highly customized version of Linux. Google uses a proprietary storage and processing mechanism that isolates processing of data in chrooted jails within a physical server. Access permissions restrict the ability for processes to interact between jails. In addition, tenant data is striped in chunks across many different drives with each chunk having its own access control list. This helps ensure that data is logically isolated between customers in storage and during processing. In addition to the inherent processing and storage mechanisms described above, Google's security controls including least privilege rights, logging and auditing have been implemented consistent with FedRAMP requirements
AODocs	Altirnao can use multiple notification channels to communicate incident updates to its customers: the AODocs status page (https://status.aodocs.com) provide status updates on all the AODocs services the AODocs customer mailing list, which can be used to send emails to the technical contacts of all AODocs customers the AODocs support platform, i.e. ZenDesk, which can be used to communicate with specific customers who have opened tickets.
Salesforce	Incident Response If negotiated into a final contract, Salesforce can promptly notify the Customer in the event Salesforce becomes aware of an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by Salesforce support, email to customer's administrator and Security Contact (if submitted by customer), and public posting on trust.salesforce.com. Salesforce maintains an Incident Response Plan and has an established Security Incident Response Process. During a security incident, the process guides Salesforce personnel in management, communication, and resolution activities. Government customers can report security incidents related to their Salesforce products and offerings via security_gov@salesforce.com. Salesforce will respond in accordance with the incident response process described above. Our incident response plan/process was created in accordance with FedRAMP moderate control requirements which include incident response requirements derived from NIST SP 800-53, NIST SP 800-61, and the FedRAMP Incident Communications Procedure.
ServiceNow	Unless notification is delayed by the actions or demands of a law enforcement agency, ServiceNow shall report to Customer the unauthorized acquisition, access, use, disclosure or destruction of Customer Data (a "Breach") promptly following determination by ServiceNow that a Breach occurred. The initial report shall be made to Customer security contact(s) designated in

	ServiceNow's customer support portal. ServiceNow shall take reasonable measures to promptly mitigate the cause of the Breach and shall take reasonable corrective measures to prevent future Breaches. As information is collected or otherwise becomes available to ServiceNow and unless prohibited by law, ServiceNow shall provide information regarding the nature and consequences of the Breach that are reasonably requested to allow Customer to notify affected individuals, government agencies and/or credit bureaus. Customer is solely responsible for determining whether to notify impacted Data Subjects and for providing such notice, and for determining if regulatory bodies or enforcement commissions applicable to Customer or Customer Data need to be notified of a Breach. See the "Data Security Guide" contained within the "Subscription Service Guide" included with this response for additional information.	
QTS	Security Incident handling capability and process is outlined in the following Incident Response related procedures and plans: •FED_PLN_01_Incident_Response_Plan (v1.2 – 4/09/14) •IT_PRO_29_QTS-FC_Incident_Response_Procedure (v1.0 – 1/17/14) •IT_PRO_18_ISSO_IRT_Incident_Response_Guidelines_Procedure (v1.2 – 12/11/13) •OPS_PRO_77_OSC_New_Incident_Creation_Procedure (v1.0 -1/23/14) •OPS_PRO_62_Best_Practices_for_Incident_Handling_Procedure (v1.0 – 12/10/13) •OPS_PRO_72_BPG_OSC_Working_and_Resolving_Incidents_Procedure (v1.0 – 1/22/14) •OPS_PRO_84_BPG_OSC_Major_Incident_Management_Procedure (v1.0 – 1/27/14) As outlined in QTS's IT_PRO_29_QTS-FC_Incident_Response_Procedure (v1.0 -1/17/14) and FED_PLN_01_Incident_Response_Plan (v1.2 – 4/09/14): •Preparation activities, to include: -Ensuring the security of systems, networks, and applications through periodic risk assessments of systems and applications to prevent incidents. -Increasing user awareness of policies and procedures regarding appropriate use of networks, systems, and applications. -Sharing applicable lessons learned from previous incidents (particularly those involving malicious code and violations of acceptable use policies) with users so they can see how their actions could affect the organization. -Training Federal Cloud System Administrators to maintain their networks, systems, and applications in accordance with the organization's security standards. •Detecting activities, to include: -As referenced in QTS's IT_PRO_29_QTS-FC_Incident_Response_Procedure (v1.0 -1/17/14), review and analysis of continuous monitoring tools and related log file(s). -3rd Party monitoring services (Alert Logic): help detect and alert on changes in certain resources (e.g., Web pages) or publicly accessible services, such as Web, Domain Name System (DNS) and FTP servers. -File Integrity Checking Software: help detect any changes to important files caused by incident -IDS are set up for scanning and detection. Detection is achieved either by log analysis, packet capture review or image acquisition and analysis. •Analysis Activities, to include: -QTS IR Team is activated and incident identification is performed -Continued and targeted review and analysis of continuous monitoring tools, related log file, and corresponding applications would be performed. -If an Incident Response Team is required then at least one member of IT Security along with one or more members of QTS's IT Operations organization responsible for the affected system, as well as any necessary representatives from Network	
SAP	Ariba	We can provide a general overview but our full documentation is confidential. All of our security processes and procedures are audited by a third party every six months for ISAE 3402 assurance. We also hold PCI DSS certification. The

		intent of the following is to describe in a broad manner the actions we take in regard to security incidents, their management, tracking and communications in regard to internal policies and procedures. We have an established security incident plan based on internally-developed policies and procedures where documented results of all security incidents occurring during the six month audit period are reviewed and evaluated against the Trust Services Principles of ISAE 3402 and the PCI DSS standards as appropriate. Upon notification of a security incident, a documentation trail is begun by the InfoSec department and an internal ticket is created as the record of reference. The lead security manger calls a meeting including all personnel required to contain and reduce risk and impact appropriate to the nature of the incident. Tasks are assigned with milestones to be met to validate and determine extent of the incident. Communication is made to the Privacy & Security Board to alert principal membership and foster internal cooperation and awareness. An appropriate communication channel to affected customer(s) is determined based on how we were notified of the incident, i.e. from a customer, from an internal report or from a third party report. Communication is made to affected customer(s) to include the nature of the incident, actions taken to contain the incident and potential effects of actions if any, in regard to sustained business process and availability of the system. Any workarounds or hot fixes necessary in the solutions are communicated and scheduled reporting to the customer(s) is established with an identified single point of contact within our company. Based on the nature of the incident, if required, legal counsel present at initial risk & impact meeting, will assist in communicating with law enforcement contacts. The customer is kept informed of the milestones met and at scheduled intervals until the incident is fully contained and no further risk and impact perceived. All incidents are required to be internally managed by InfoSec to include tracking and review on a weekly basis and evaluation of the actions taken in regard to our security concept. All incident reports are presented to and reviewed by the Privacy & Security Board and are formally closed with discussion and evaluation to determine what actions can be taken to prevent similar incidents. Depending on the nature of the incident and impact to customer(s), security incidents are not formally closed by the board until all affected customers are made aware of the incident and appropriate measures to remediate the initial threat are formally communicated.
	Fieldglass	Fieldglass' security team is responsible for managing security incidents and all communication is conducted via the respective account managers to ensure timeliness. The process is defined within the Incident Response Management Standard. Customers are notified of an incident within 48 hours.
	Hanna	SAP will notify via defined communication channels within 36 hours of a confirmed data security breaches to the affected customers. The report will detail the following information: • Details relating to the security incident that has occurred, known at the time of notification. • IT infrastructure and/or application affected by the security incident. • Overview of the performed mitigation actions to restore the security, documented within the incident report form. • All further applicable requirements by country regulations "on obligation to notify" will be met.

	Hybris	Upon a breach that directly affects a customer's environment, hybris would notify the customer as quickly as reasonably possible. Furthermore, hybris follows its information security incident management policy as well as Visa's standard process for responding to a breach. The policy includes procedures such as disclosure of sensitive information, disclosure of system vulnerability, public release of vulnerability information, system vulnerability exploitation as well as incident reporting, contacting of law enforcement and forensic investigation.
	SuccessFactors	We have a comprehensive and approved Incident Management Policy and process. Upon the occurrence of a security incident, initial communication is distributed to the appropriate individuals and an escalation process is followed. Upon becoming aware of the incident, measures are promptly taken by the team to resolve the situation. All affected customers should be informed within at most 36 hours of confirming a potential breach in the privacy of their data. Following incident resolution, follow-up is required to ensure that the incident has been resolved effectively and that the threat is no longer present. We are aligned with ISO 27k standards for event and incident management and have formal incident management policies and processes in place. These policies and procedures are tested in the ISO 27k and SOC 2 audits.
VMware	VMware IaaS Services If VMware determines that there has been unauthorized access to, or use or disclosure of, Your Content, or other incident VMware will use commercially reasonable efforts to notify You, taking into account any applicable law, regulation, or governmental request. VMware will provide security incident response (e.g., detection, severity/threat classification, forensics, and resolution) pertaining to management infrastructure over which VMware has direct, administrative, and/or physical access and control, such as the vCloud Hybrid Service servers, storage, applications, and network devices. Documented escalation procedures and a ticketing system are in place to guide employees in identifying, reporting, and responding to system availability issues and related security incidents. This includes an incident response policy to determine severity of an incident and a breach notification process. All alerting and monitoring at the guest OS\VM level is the responsibility of the customer. In the event of a data breach customers will be notified by VMware vCloud Air Global Support Services via their preferred contact means. VMware will provide security incident response (e.g., detection, severity/threat classification, forensics, and resolution) pertaining to management infrastructure over which VMware has direct, administrative, and/or physical access and control, such as the vCloud Air service servers, storage, applications, and network devices. Notification timeframes are agreed upon between VMware and the customer in standard agreements and contracts. Incidents are handled on a case-by-case basis, but typically occur between 24-48 hours after a breach has been confirmed. VMware will provide security incident response (e.g., detection, severity/threat classification, forensics, and resolution) pertaining to management infrastructure over which VMware has direct, administrative, and/or physical access and control, such as the vCloud Air service servers, storage, applications, and network devices.	
FireEye	FireEye has a developed documented process for reporting client notification for regulatory, legal and contractual issues once a breach has been confirmed.	
VirtueStream	Virtustream shall contact customers in accordance with Service Level Agreements (SLA) and contractual obligations. There are two primary Incident types; Security Incidents, where there is a possible breach in systems or data integrity, and Services, where there is in impacted or affected service. Although there is some overlap, generally any security-related incident should be classified as a Security	

	Incident and the response must be managed using the 'Virtustream Information Security Procedure – Security Incident Response Plan'. The purpose of this security incident response plan is to provide general guidance to Virtustream staff- both technical and managerial – to enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission critical information including sensitive credit card data. The plan is also a guide to sharing information with other stakeholder organizations who might be impacted by such security incidents such as the credit card associations and law enforcement. The Security Incident Response Plan (SIRP) provides guidance to prepare for, respond to, and recover from potential incidents. Policy statements surrounding the IR-Plan are provided to ensure continued upkeep and standardized use. The SIRP guidance at the procedural level defines the roles, responsibilities, communication methods and flows, contact information, types of potential incidents, and immediate actions that are to be taken upon an incident's identification, and elaborates with subsequent recovery steps. Virtustream's Incident Response Policy requires the implementation and testing of a generalized plan that adheres to the International Standards Organization 27002 guidance for incident management and response, but meets specific requirements for compliance such as PCI-DSS. The Plan covers the corporate environment associated with Virtustream's IT assets, the local IT resources and the IT resources at Virtustream's Data Center. It consists of a series of guidelines (Incident Response Guidelines or "IRG") that should generally be followed as appropriate for the circumstances as when a security incident occurs or as part of the ongoing maintenance of this plan. As the incident progresses and has more impact (i.e. severity level increases), the escalation process will be used to engage appropriate resources. Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact, and to keep tight control. The Table below defines the escalation levels with the associated team involvement.

8.6.9 Offeror must describe and identify whether or not it has any security controls, both physical and virtual Zones of Control Architectures (ZOCA), used to isolate hosted servers.

CA	APM	AWS EC2 datacenters annually undergo SOC 3 audits.
	MAA	Physical access mechanisms (e.g., access cards, biometric devices, mantraps and portals) have been implemented and are administered by local operations staff to help ensure that only authorized individuals have the ability to access the data centers. Portals and mantraps have been installed as anti-tailgating measures in most of data center lobbies. Entry to and exit from the data centers is through either a portal or mantrap where present. In data centers without portals or mantraps, the security officer monitors the entrance to prevent tailgating. Where present, the portal/mantrap bypass doors are only used in the event an individual is unable to use the portal or mantrap in case of emergency. Examples include handicap, phobia, or other restrictions on a case-by-case basis. Tours and emergency data center security operations crews will be permitted to use the portal bypass door, when necessary.
	CA Agile	Physical access mechanisms (e.g., access cards, biometric devices, mantraps and portals) have been implemented and are administered by local operations staff to help ensure that only authorized individuals have the ability to access the data centers. Portals and mantraps have been installed as anti-tailgating measures in most of data center lobbies. Entry to and exit from the data centers is through either a portal or mantrap where present. In data centers without portals or mantraps, the security

		officer monitors the entrance to prevent tailgating. Where present, the portal/mantrap bypass doors are only used in the event an individual is unable to use the portal or mantrap in case of emergency. Examples include handicap, phobia, or other restrictions on a case-by-case basis. Tours and emergency data center security operations crews will be permitted to use the portal bypass door, when necessary.
	ASM	Physical access mechanisms (e.g., access cards, biometric devices, mantraps and portals) have been implemented and are administered by local operations staff to help ensure that only authorized individuals have the ability to access the data centers. Portals and mantraps have been installed as anti-tailgating measures in most of data center lobbies. Entry to and exit from the data centers is through either a portal or mantrap where present. In data centers without portals or mantraps, the security officer monitors the entrance to prevent tailgating. Where present, the portal/mantrap bypass doors are only used in the event an individual is unable to use the portal or mantrap in case of emergency. Examples include handicap, phobia, or other restrictions on a case-by-case basis. Tours and emergency data center security operations crews will be permitted to use the portal bypass door, when necessary.
AODocs	N/A because all our data is hosted on the Google Cloud Platform infrastructure.	
Virtru	We require 2 Factor and Private Keys to authenticate and Virtrual Private Clouds for purposes of Inter-machine communication	
Salesforce	A customer's instance (org) of Salesforce is an aggregate of the raw data. The data model is very complicated, normalized, and the rows are identified by base62 encoded keys (primary and foreign). Re-establishing data ownership and a business context for the data would be very difficult to do at the database level. In order to reassemble any given customer's application (org), someone would need access to our source code in order to reassemble the raw data in a manner that could be interpreted and understood, and would need the entire set of tapes or disks/arrays supporting a given Instance, as the data for any one customer is spread across several tapes/disks. Data center engineers with physical access to the servers do not have logical access to the production environment and administrators with logical access to the systems do not have physical access to the data centers.	
ServiceNow	ServiceNow's architecture is built on a ServiceNow fully owned operated private cloud. This private cloud hosts the ServiceNow platform and applications that are offered to its customers under a subscription service model. The ServiceNow private cloud operates out of colocation data centers that provide robust physical and environmental controls, with ServiceNow staff exclusively providing the logical management. Access to the private cloud where customer data is hosted is only granted to ServiceNow staff based on their roles and job requirements. ServiceNow does not outsource any function that would give a third party access to customer data. ServiceNow's private cloud is a highly standardized environment from the identically configured cages in the data centers through to the consistent logical infrastructure. This private cloud is home to just ServiceNow, limiting the private cloud's footprint to only those technologies required to support this service. This allows for highly restricted networking rule sets regarding ingress and egress requirements and facilitates the ability for hardened systems, only allowing for the small number of necessary services, protocols and ports to be enabled. A ServiceNow instance represents an isolated logical environment consisting of application nodes in the web application tier and a dedicated database. Each customer will receive at least two instances, a production High Availability (HA) instance and a sub-production instance without HA. Each instance is accessed via a unique Domain name in the form of 'customername.service-now.com' (for a production instance) and 'customername-dev.service-now.com' as a sub-production example.	

	There is no comingling of any customer data between instances and there is no single shared multi-tenant databases, with data from multiple customers stored therein.	
QTS	QTS cloud employs security controls as needed to protect the confidentiality and integrity of the information being transmitted by utilizing Cisco AnyConnect VPN Client with SSL (TLS and DTLS) and IPSec (Internet Key Exchange Version 2 [IKEv2]). DTLS provides an optimized connection for latency-sensitive traffic, such as VoIP traffic or TCPbased application access, TLS (HTTP over TLS/SSL) ensures availability of network connectivity through locked down environments, including those using web proxy servers. IPSec/IKEv2 provides an optimized connection for latency-sensitive traffic when security policies require use of IPSec and complies with applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance. The QTS Federal Cloud Infrastructure (QTS cloud) is divided into two separate, isolated firewalled environments, each having its own security boundaries, which are physically and logically separated. These are the QTS cloud Hypervisor Management Layer and the QTS cloud Service Delivery Layer. QTS cloud's Hypervisor Management Layer management is made available through dynamic FIPS 140-2 validated L2TP/IPSEC or SSL 3. 0/TLS 1. 0 encrypted VPN tunnels, which are authenticated against the RSA SecurID multi-factor authentication security appliances. Once fully authenticated, only a limited RDP session to the physical bastion host (which is also protected by the RSA SecurID multi-factor authentication security appliances) via jump domains is allowed, which prevents the presentation of information systems management related functionality at an interface for general users. QTS cloud's Service Delivery Layer management is also made available through FIPS 140-2 validated L2TP/IPSEC or SSL 3.0/TLS 1. 0 encrypted VPN tunnels, which are authenticated against the RSA SecurID multi-factor authentication security appliances. Connection to the QTS cloud Service Delivery Layer is only available through dedicated site-to-site 140-2 validated L2TP/IPSEC or SSL 3. 0/TLS 1. 0 encrypted VPN tunnels or Trusted Internet Connection (TIC) monitored dedicated datelines to federal customer datacenters, which prevents the presentation of information systems management related functionality at an interface for general users. QTS cloud's Hypervisor Management Layer management is made available through dynamic FIPS 140-2 validated L2TP/IPSEC or SSL 3. 0/TLS 1. 0 encrypted VPN tunnels, which are authenticated against the RSA SecurID multi-factor authentication security appliances.	
SAP	Ariba	The Cisco Secure ASA5555 Firewall is a dedicated firewall appliance that delivers strong security and performance and creates almost no network performance impact. The product enforces secure access between an internal network and Internet, extranet, or intranet links. Ariba uses Cisco Secure ASA5555 Firewall hardware and Cisco Router access lists to control the traffic to and from the Internet, between Ariba Corporate and the Ariba system, and between servers in Ariba. The firewall servers are configured for Fail-Over/Hot Standby Setup. Additionally, Ariba uses internally developed Ariba SafeGuard software to protect customer data from unauthorized Ariba Corporate users, allowing only Ariba Operations personnel access for limited periods of time. Specifically, firewall servers are used in each level of data communication within Ariba: Between the Internet and web servers Between the web servers and the application servers Between the application servers and the database servers

		These ASA5555 Firewall servers allow Ariba Operations to rigorously protect Ariba from unauthorized access, providing full firewall security protection. The Equinix Data Center utilizes an array of security equipment, techniques, and procedures to control, monitor, and record access to the facility, including customer cage areas. All areas of the center are monitored and recorded using CCTV, and all access points are controlled. The Data Center is staffed with 24-hour security officers. Visitors are screened upon entry to verify identity, and escorted to appropriate locations. Access history is recorded for audit purposes.
	Fieldglass	Please see the Fieldglass Security and Hosting Overview provided in the Supplemental Information section of this response.
	Hanna	The fundamental security architecture of the SAP Cloud infrastructure is the principal of a private cloud. Customers receive an isolated, logical grouping of several virtual machines and physical systems in dedicated customer private networks. Customer private networks are segregated from each other using virtual local area networks (VLAN) technology. Customer systems are deployed in the respective customer private network. Though customers are only able to view or access systems within their assigned customer private network. Design of customer private networks has to be defined in a workshop between SAP and the customer. Multiple customer private networks might be required to separate different tier levels or to implement customer data flow restrictions. SAP HANA Enterprise Cloud administrative tasks will be done using management networks. Administrative access to the management networks from the SAP internal networks is only possible using dedicated jump hosts with strong authentication. Security of the SAP internal network including SAP end user equipment is ensured using solutions like network admission control, Intrusion Prevention Systems, network filtering, strong authentication for remote access, internet content filtering, anti-virus scanner.
	SuccessFactors	We serve our customers and end users from secure data centers around the world. Physical security features at these facilities include a 24x7x365 manned security station and biometric and man-trap access controls. The systems at these facilities are protected by firewalls and encryption technology. Operational redundancy features include redundant power, on-site backup generators, and environmental controls and monitoring. We employ a wide range of security features, including two factor authentication, data encryption, encoded session identifications and passwords. Our hosting providers conduct regular security audits of our infrastructure. We also employ outside vendors for 24x7x365 managed network security and monitoring. Every page we serve is delivered encrypted to the end user via a Transport Layer Security or TLS. We also use encryption technology in our storage systems. We continuously monitor the performance of our cloud offerings using a variety of automated tools. The architecture is designed with built-in redundancy for key components. We load balance at each tier in the network infrastructure. We also designed our application server clusters so that

		servers can fail without interrupting the user experience, and our database servers are clustered for failover. We regularly back up customer data. We have implemented a multi-tiered architecture leveraging a strategy of "defense in depth" with 6 tiers of virtual networks (VLAN) for separation at each delivery layer. Network traffic is logged and monitored with live monitoring through an Intrusion Detection System (NIDS), and controlled through a series of switches and routers whereas data must pass through each tier in order to get to the next tier. In addition to Physical (site) security, the logical network stratification includes the following: Tier 1 (External VLAN/firewall) - The first tier consists of the external network and perimeter firewalls. These provide an initial layer of defense and protect the following layers from unauthorized access. Note that port 443 (HTTPS for web traffic) is the only port open. Tier 2 (Internal VLAN/firewall) - A de-militarized zone (DMZ) exists with load balancers. The DMZ provides a second line of defense while the load balancers are the first layer of scalability for the service delivery. The DMZ functions as a ""neutral zone"" between the network and the outside public network. Tier 3 (Web VLAN) - The Web tier presents the User Interface to the application, and separates the application, reporting and utility servers from the other tiers. Tier 4 (Application VLAN) - The Application tier contains the business logic and transaction servers, and is managed through clustered, high availability (HA) servers. Pre-configured as "Pods", additional servers can be added as needed to provide scalability and performance. Tier 5 (Database VLAN) - The database tier is protected by an additional set of perimeter firewalls. The database processing is executed on database servers leveraging a multi-tenant, fully qualified database schema. Tier 6 (Storage VLAN) - Data is persisted to disks with include a Storage Area Network (SAN). Prior to store, data is encrypted by way of data appliance with AES-256 bit encryption.
VMware	VMware IaaS Services At the tenant level firewall services are provided via the vCloud Networking & Security Edge Gateways for customers to configure and maintain. Firewall policies can be used to restrict and manage public/Internet-based traffic and create DMZ zones for multi-tier applications. Firewall policies can also be used to configure access policies between internal IP networks and VxLAN segments. Stateful inspection firewalling can be applied on the external interface of the vCNS Edge Gateway. VMware architects, provisions, monitors and manages the vCloud Hybrid Service infrastructure and surrounding components. As described in the AT 101 (ISO 27001) report, access points such as delivery and loading areas and other points where unauthorized persons may enter the premises are controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. The details of this control are not disclosed publicly. VMware AirWatch We implement multiple security measures to protect hosted servers, including physical and logical controls. Due to FOIA requirements and the competitive EMM marketplace, we cannot provide specific architecture details at this time.	

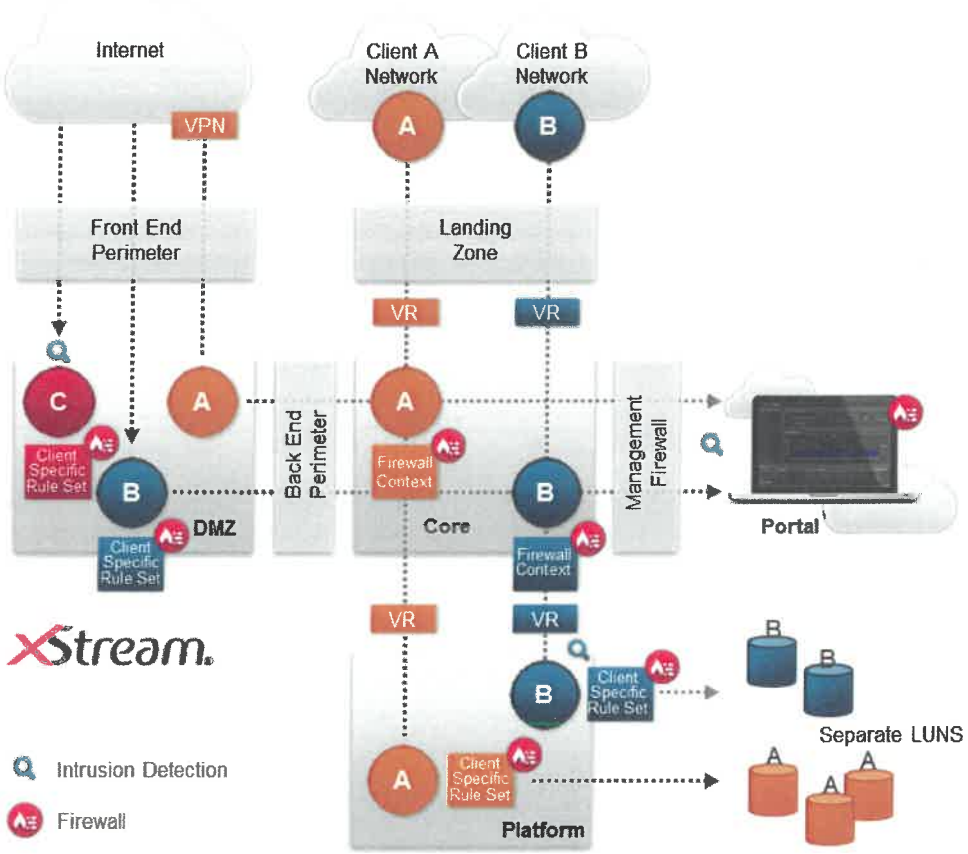
FireEye	High-level architecture diagrams following industry best practices utilizing both virtual and physical controls are available and contained in the SOC 2 report.
VirtueStream	Virtustream utilized a virtual local area network (VLAN) and virtual route forwarding (VRF) to logically segregate all customers in the IaaS environment. Every customer chooses their own IP Address range, as there is no ability to overlap IP Addresses between customers. In addition, every customer is logically separated with Firewall Context with their own rule, where by default everything is denied except specific rule.

8.6.10 Provide Security Technical Reference Architectures that support Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS).

CA	APM	Only SaaS is provided, network diagram can be provided upon signing NDA
	MAA	Only SaaS is provided, network diagram can be provided upon signing NDA
	CA Agile	These can be provided when a NDA is in place.
	ASM	Only SaaS is provided, network diagram can be provided upon signing NDA
Salesforce	Salesforce offers market leading PaaS and market leading SaaS solutions. Salesforce does not provide IaaS as a direct service offering to our customers, it is an underlying part of our PaaS and SaaS offerings. The Salesforce Platform is built for cloud computing, with multitenancy inherent in its design. To meet the high demands of its large user population, Force.com's foundation is a metadata-driven software architecture that enables multi-tenant applications. Force.com combines several different persistence technologies, including a custom-designed relational database schema, which are innately designed for clouds and multitenancy—no virtualization required. Force.com's core technology uses a runtime engine that materializes all application data from metadata—data about the data itself. In Force.com's well-defined metadata-driven architecture, there is a clear separation of the compiled runtime database engine (kernel), tenant data, and the metadata that describes each application. These distinct boundaries make it possible to independently update the system kernel and tenant-specific applications and schemas, with virtually no risk of one affecting the others. Every logical database object that Force.com exposes is internally managed using metadata. Objects, (tables in traditional relational database parlance), fields, stored procedures, and database triggers are all abstract constructs that exist merely as metadata in Force.com's Universal Data Dictionary (UDD). For example, when you define a new application object or write some procedural code, Force.com does not create an actual table in a database or compile any code. Instead, Force.com simply stores metadata that the system's engine can use to generate the virtual application components at runtime. When you need to modify or customize something about the application schema, like modify an existing field in an object, all that's required is a simple non-blocking update to the corresponding metadata. Because metadata is a key ingredient of Force.com applications, the system's runtime engine must optimize access to metadata; otherwise, frequent metadata access would prevent the service from scaling. With this potential bottleneck in mind, Force.com uses massive and sophisticated metadata caches to maintain the most recently used metadata in memory, avoid performance-sapping disk I/O and code recompilations, and improve application response times.	

	The multitenant architecture and secure logical controls address separation of Customer Data. The Salesforce infrastructure is divided into a modular architecture based on "instances". Each instance is capable of supporting several thousand customers in a secure and efficient manner. Salesforce uses the instance architecture to continue to scale and meet the demands of our customers. There are appropriate controls in place designed to prevent any given customer's Salesforce instance from being compromised. This functionality has been designed and undergoes robust testing through an on-going process by both Salesforce and its customers.	
QTS	The QTS cloud makes use of unique managed service provider architecture layer(s). Information systems, particularly those based on cloud architecture models, are made up of different service layers. The layers of the QTS cloud that are defined in its System Security Plan, and are not leveraged by any other Provisional Authorizations, are: Infrastructure as a Service (IaaS). Note: Please refer to NIST SP 800-145 for information on cloud computing architecture models.	
SAP	Ariba	Ariba recognizes that security is a critical component of effective electronic commerce architecture and takes necessary security measures to protect any information passed between buyers and suppliers. Ariba implements security using a variety of hardware, software, and procedural best practices. Full details about our security mechanisms and procedures are available in Chapter 3 of the Ariba Cloud Technical Infrastructure Whitepaper.
	Hanna	N/A, HANA Enterprise Cloud is a private managed cloud
	SuccessFactors	We understand the critical importance of information protection and recognize the contribution that information security makes to an organization's strategic initiatives and overall risk management. We have implemented security controls and practices designed to protect the confidentiality, integrity, and availability of customer information. We continually work to strengthen and improve those security controls and practices as well. The current best practices associated with information security involve a layered approach, what the industry calls "defense in depth." Regardless of the software delivery model, security cannot be implemented at a single "make or break" point. For a SaaS provider to facilitate data security for sensitive information, it must have a comprehensive, multifaceted security program in place. We take a holistic approach to information security, implementing a multilayered defense at all the touch points in the information flow—both the physical and logical, applied across the database, middleware, application, and network and communication layers—to offer complete data privacy, transparency, and audit controls.
VMware	Compliance Reference Architecture Framework (RAF) that provides a consistent method for VMware, its partners, and customers to assess and evaluate the impact of regulations on virtual and cloud environments. The intent of the RAF is to provide a single framework for VMware, its partners, and organizations to address a variety of compliance requirements across an IT infrastructure. This includes: Product Applicability Guide (PAG), Architecture Design Guide (ADG), and a Validated Reference Architecture (VRA).	
FireEye	High-level architecture diagrams following industry best practices utilizing both virtual and physical controls are available and contained in the SOC 2 Type 2 report.	
VirtueStream	Virtustream Cloud Platform Security (for the Infrastructure-as-a-Service environment) is designed, built, and operated to provide highest level of infrastructure security available. **Proposed State of Utah Security Architecture**	

Figure 1. xStream Enterprise Architecture



State of Utah end users would access the hosted SAP environments via a MPLS connection (Provided by State of Utah). Additionally a VPN connection has been sized at 100Mbps however this can be decreased or increased depending on the exact requirements.

State of Utah end users accessing our enterprise platform would first hit the landing zone in a dedicated virtual local area network (VLAN) and dedicated virtual route forwarding (VRF). The next hop into the enterprise platform is a dedicated firewall (FW) context on a Cisco Firewall services module. After traversing the core, traffic hits another dedicated VRF and drops into the platform network and compute (CPU and Memory essentially a blade server) layer. All traffic is VLAN separated. At each compute host, a hypervisor based firewall and intrusion protection system (IPS) provides a dedicated client rule set to further ensure network security. All traffic transitioning from one zone to another are monitored by Intrusion Detection and Intrusion Prevention systems.

Traffic coming in via the internet hits the front-end perimeter with load balancing modules and multi-context Cisco firewalls. All traffic then passes through intrusion detection system and intrusion protection systems. As in the enterprise compute layer, every host in our demilitarized zone (DMZ) has a hypervisor-based firewall and IPS with dedicated client rule sets. Again, all traffic is VLAN separated as well.

Traffic that needs to traverse from DMZ to the enterprise runs through another dedicated FW context and IDS/IPS.

All of the State of Utah environments and data will be hosted in Virtustream's data centers within the continental United States.

Standard Services used in Virtustream's management environment and in all client environments including the following:

- All Virtustream employees use Mandatory Strong 2 factor authentication (2FA OTP) Administrative Access to all systems.
- Dedicated VLAN network segmentation and dedicated Virtual Route Forwarding (VRF) are used extensively to segregate environments and zones.
- Perimeter Firewalls are used to segment internal and external environments as well as segregate security zones. Configuration, monitoring, auditing and logging are included.
- Virtual Machine-based Firewall and Intrusion Prevention System (IDS) is installed on every virtual machine in the environment and is protected with Juniper's Security Gateway virtual firewall application and monitored service.

Security Services that are standard components for Virtustream's management environment and are Optional Services for client environments including the following:

- Managed Two-Factor Authentication ("2FA") is in use for all application systems.
- Intel TxT Enabled Servers and Trusted Boot/Bios monitoring with Attestation Server and OS and VM support, including Geolocation and Geofencing according to NIST 7904 guidelines.
- Secure operating system (OS) builds based on DoD Secure Technology Implementation Guide (STIG) guidelines are used to build Virtustream's Management and Administration Servers.
- Server/File Integrity Monitoring (FIM) is installed in the PCI and VFC clouds.
- Patching Regimen: Virtustream patches host servers, network devices, security devices, servers and related services in the Management Network on a specified routine (monthly or quarterly, depending on release schedules), or when there is a CERT or other authorized source of patch that requires immediate attention. Based on urgency and risk of the issue we will schedule the patch as appropriate and use change control.
- Scanning regimen: vulnerability scanning is done on a monthly basis with additional 3rd party vulnerability scans done monthly. Additional scans are done when made aware of new vulnerabilities. Issues are classified and addressed according to Risk Classifications and are addressed with ITIL v3 change control processes.
- Managed IDS signatures are routinely updated and the logs are monitored.
- Anti-Virus is managed on all Management servers in Enterprise, PCI and, VFC clouds.
- Logging Service of all servers, network devices, and security devices to a centralized log server system.
- Governance Risk Compliance: We use a complete Enterprise Risk Management toolset to manage compliance reporting and continuous monitoring to all of our supported compliance frameworks.

Virtustream's facility monitoring systems are complete as per specifications in NIST 800-53r3/4. We use site assessment methodologies and checklists as detailed in NIST 800-42. Our systems and facilities are monitored 24/7 for any exceptions or trends. Our tools, processes and CONUS (Continental USA) personnel monitor network, power, cooling, humidity, water leakage, fire suppression, power systems (utility power, UPS systems and generators) and site access. Virtustream's Physical Access Control Security is designed to protect the confidentiality, integrity, and availability ("CIA") of the cloud platform system and its data with the following security components:

- Limited and controlled room access.
- Logged and monitored access of all access control events.
- Video surveillance and review of all access control events.
- Biometric access control required to gain access to the Data Center.
- US Data Center staff is limited only to US Citizens.

	• Locked racks and rooms with key log out/in process. • Data destruction policies and procedures. • Asset in/out policy and procedures. Physical access by authorized staff is controlled by badge systems and biometric access systems. All access of any kind is recorded and logged. Access lists are reviewed every 90 days. Employees that do not have a reason to have physical access are removed from our access management systems. Multiple high resolution and IR enhanced CCTV Cameras monitor our datacenters at all egress and ingress points as well as other sensitive areas. Security video footage is stored in a secure area for 90 days. Approved Visitor Access requires VISITOR Badges and bright lanyards that are specifically different from employee badges. Visitors are required to produce and surrender a state or government issued photo ID during the visit, have a pre-approved reason for the visit, and have the escort witness the sign in and out procedure. Visitors are escorted continuously through approved areas of the facility. Visitors are not allowed access to following areas of the data center under any circumstances: • Cloud hosting areas. • Networking and telecommunication areas. • Guard areas. • Power vaults.

8.6.11 Describe security procedures (background checks, foot printing logging, etc.) which are in place regarding Offeror's employees who have access to sensitive data.

FireEye	Background verification for employment candidates is a mandatory component of FireEye's hiring process. All personnel are required to sign a confidentiality and non-disclosure agreement agreeing not to disclose proprietary or confidential information including client information to unauthorized parties. Security awareness training program is in place to maintain the skill level of personnel regarding security and privacy expectations and best practices. All FireEye personnel at all levels are trained and notified of information security and privacy requirements and personnel responsibilities.
VirtueStream	Virtustream employees who are assigned to IaaS must pass a Virtustream background investigation. In addition, Virtustream employees assigned to the IaaS must adhere to any requirement by customers to pass federal, state, or local background investigations if they are to provide managed services to the customer zone which includes access to sensitive data.

8.6.12 Describe the security measures and standards (i.e. NIST) which the Offeror has in place to secure the confidentiality of data at rest and in transit.

CA	At CA Technologies, we comply with a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. We ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks and adhere to the highest industry compliance and security policies. CA offers a variety of SaaS solutions, details for each offering has been provided in Exhibit 1 and 2 of this proposal.
Google	All connections from customer end point devices to Google's Front End Servers are encrypted with enforced HTTPS sessions using Forward Secrecy. Google websites and properties use robust public key technologies: 2048-bit RSA or P-256 ECDSA SSL certificates issued by a trusted authority (currently the Google Internet Authority G2).

	All data in transit between Google's Data Centers traverses across Google's private fiber network using a customized, proprietary encryption technology. Google hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect data at rest. These methods of encryption are fully managed by Google and Google's Key Management Servers based on 128-bit or stronger Advanced Encryption Standard (AES). Encryption Keys and Ciphers Supported by Google Protocols TLS 1.2 TLS 1.1 TLS 1.0 SSL 3.04 QUIC Cipher suites ECDHE_RSA with AES ECDHE_RSA with 3DES ECDHE_ECDSA RSA with AES RSA with 3DES Signing keys RSA 2048 ECDSA P-256 Hash functions SHA384 SHA256 SHA1 MD5
Salesforce	Government Cloud Encryption Capabilities: As part of the Salesforce Government Cloud, Salesforce is capable of responding to FIPS 140-2 cryptographic implementations for data being transferred between the State's web browser and Salesforce. Data that resides within Salesforce's protected boundary does not use FIPS 140-2 validated encryption as compensating/mitigating controls are in place to protect data. Additional information is provided below. Data In Motion: Salesforce employs cryptographic mechanisms to protect information during transmission. All transmissions between the user and Salesforce are encrypted by default with a 2048- bit Public Key. Our service uses International/Global Step Up certificates. We support one- way TLS, in which customers create secure connections before sharing private data. Secure routing and traffic flow policies ensure that customer traffic is encrypted entering Salesforce until the load balancer decrypts the traffic. The load balancers decrypting the traffic are FIPS 140-2 compliant and are located inside of the Salesforce Government Cloud isolation boundary. Data At Rest: NIST SP 800-53 Rev. 4 states in SC-28, "Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system." SC-28 also states, "Organizations may choose to employ different

	mechanisms to achieve confidentiality and integrity protections, as appropriate." All secondary storage media (hard drives, disk drives, and tapes) containing customer data are maintained within Salesforce's secure production data centers until the media has been sanitized and destroyed. Salesforce relies on physical access controls as a compensating control to protect the data. For primary data storage, Salesforce provides customers with a built-in capability to apply field-level encryption, using 128-bit keys with AES encryption, for a selection of custom fields included in the Force.com Platform and Salesforce Services. Field-level encryption ensures the data associated with designated fields is encrypted in storage.	
SAP	Ariba	Sensitive data elements, including PCI Primary Account Numbers and system account parameters for internal application communications, are stored in Ariba databases encrypted by the AES (Advanced Encryption Standard) and Triple DES (Data Encryption Standard) encryption algorithms with a minimum key length of 128 bits. Encryption technology is also applied for the client connection to the Web site and to the hosted application passwords in storage. Customer user passwords are one way hashed using SHA256 and salted with random data. Limited Ariba Operations personnel have data query access and monitoring rights for the Ariba Hosting program.
	Fieldglass	
	Hanna	SAP provides for enterprise-grade and industry-standard security. SAP HANA Enterprise Cloud datacenters are enterprise-class security with enterprise-class protection including data encryption, network encryption, firewalling, network isolation, and intrusion detection. HANA data is protected in multiple different ways. SAP HANA Enterprise Cloud is a managed cloud service that employs either a VPN or MPLS connection for transit. By default VPN is encrypted and MPLS can be encrypted. The customer procures the method of connection. At installation, HANA data can be encrypted using a feature called Data Volume Encryption. This encryption protects data in the persistence layer. Storage volume access is restricted to the customer account that created the volume, thus denying all other customer accounts the permission to view or access the volume that includes data isolation, masking, zoning and Logical Unit (LUN) binding. Strict user and access management, authorization management according to the need-to-know principle for administrative accounts, and security logging and security monitoring for critical activities or access, also protect data stored in HANA.
	Hybris	The Hybris platform uses SSL (https) for both the web application tier (browsers and WebService APIs) as well as communicating with back office systems. Data at rest is something that has to be taken into consideration in the application requirements by the partner/customer or PS teams. If encryption is required the application teams need to work on implementing the methods to encrypt and secure the data, for example encrypting data fields in the database.
	SuccessFactors	Each customer's data is maintained in a separate database schema eliminating data segmentation breaches. Each schema has separate authentication credentials and assigned resource profile to restrict access rights and resource consumption. Encryption for data at rest uses the AES256 cipher. All application access is encrypted-in-transit over HTTPS with 128-bit TLS encryption.

FireEye	At rest: Data are collected using automated batch and real-time processes and by manual personnel-driven actions via an Analyst facing Portal. Any information that is collected may be stored temporarily within appliances attached to our customers' networks and may subsequently be transmitted back to one or more FireEye datacenters. Data transmitted from a customer's network to a datacenter travels over a strong encryption Virtual Private Network ("VPN") established by the appliances. At transit: FireEye's network sensors are configured to collect full packet capture of customer network streams, including those originating from or destined to potentially malicious IP addresses, matching signature-based network indicators of compromise, results of domain name lookups, and full e-mail messages including headers, content and attachments. This information is primarily stored on-site on the appliances and only meta data matching FireEye / Mandiant indicators of compromise are sent to FaaS.
VirtueStream	Virtustream's use of Intel® Trusted Execution Technology (Intel® TXT), a hardware-root of trust security feature, and Intel® AES-NI encryption acceleration helps secure and protect virtualized environments against malware and provides more of the critical infrastructure and data protection assurances needed to enable trusted multi-tenancy in the cloud. Virtustream offers solution for data-at-rest and data-in-transit encryption solution for our customers as optional service, as most of our customer environment is only accessible via private network and only to the internal users of the customer. Solutions available to our customer as follows. 1. IPSEC VPN Tunnel for data-in-transit and 2. VM level encryption for files and databases 3. Encrypted Backup (all backups are encrypted by default) The technologies of encryption available throughout the entire data lifecycle and all are FIPS 140-2 compliant. a) DB and File System Encryption b) Encrypts file system and volume data transparently to: i) Applications ii) Databases iii) Storage Infrastructure c) Integrated Key Management d) High Efficiency Encryption i) Centralized Key Management ii) Policy Management iii) Detailed Auditing iv) Highly Available v) FIPS 140-2 Certified Hardware Appliance vi) Very Low Encryption Penalty due to Intel AES-NI enabled chip sets used e) Encryption of Virtual Machine, OS and App i) Integration of SafeNET Protect-V ii) Logging of all image access f) Encryption in Archive g) Implements Encryption, Access Control, Auditing on Host (LUW) h) Kernel Level Driver – Win i) File System – Unix/Linux j) Support for file systems and raw partitions k) Highly efficient block encryption

8.6.13 Describe policies and procedures regarding notification to both the State and the Cardholders of a data breach, as defined in this RFP, and the mitigation of such a breach.

CA	CA Technologies abides to contractual requirements for notification, in addition to working with legal to ensure compliance with regulatory requirements. There may be cases where incident analysis completion is a requirement for confirming the breach, and / or its impact and data leakage boundary. Prior to completion of this activity, CA may not have the needed conclusions for customer communication. Once subscriber data has been identified as part of the investigation, said subscribers will be notified as soon as possible and not longer than 5 days. A report of the incident will be available and distributed to clients within 30 days. Please note that none of the offerings proposed as considered payment products and are not intended for use of storage of cardholder data.	
Google	Google will take and implement appropriate technical and organizational measures to protect Customer Data against accidental or unlawful destruction or accidental loss or alteration or unauthorized disclosure or access or other unauthorized processing. If Google becomes aware of a Data Incident, Google will promptly notify Customer as permitted by law of the Data Incident, and take reasonable steps to minimize harm and secure Customer Data. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address provided by the Purchasing Entity in connection with the Agreement or, at Google's discretion, by direct communication (e.g., by phone call or an in-person meeting).	
Salesforce	Salesforce will promptly notify the State (within 48 hours, reflected in a negotiated agreement between the parties) in the event Salesforce becomes aware of an actual or reasonably suspected unauthorized disclosure of Customer Data. Notification may include phone contact by Salesforce support, email to the State's administrator and Security Contact (if contact is submitted by State and contact information is kept up to date), and public posting on trust.salesforce.com.	
SAP	Ariba	Ariba has developed a computer security incident response team. Following policies and procedures, this team responds to suspected security incidents to mitigate risks and damage. The team conducts response and forensic analysis of systems and network traffic. This information can be used to assist with prosecution if a security breach is detected and the offender caught.
	Fieldglass	SAP Fieldglass' security team is responsible for managing security incidents and all communication is conducted via the respective account managers to ensure timeliness. The process is defined within the Incident Response Management Standard. Customers are notified of an incident within 48 hours.
	Hanna	SAP will notify via defined communication channels within 36 hours of a confirmed data security breaches to the affected customers. The report will detail the following information: • Details relating to the security incident that has occurred, known at the time of notification. • IT infrastructure and/or application affected by the security incident. • Overview of the performed mitigation actions to restore the security, documented within the incident report form. • All further applicable requirements by country regulations "on obligation to notify" will be met.
	Hybris	Since we do not allow for CC data to be transmitted, stored or processed in our environment, we regularly scan the customer environment in case this is done without our consent. However, we do have a CSIRP in place, in which we would notify the customer and our internal Forensics team in the event that a customer environment should be breached.
	SuccessFactors	Upon the occurrence of a data breach, initial communication is distributed to the appropriate individuals and an escalation process is followed. Upon

		becoming aware of the incident, measures are promptly taken by the team to resolve the situation. All affected customers should be informed within at most 36 hours of confirming a potential breach in the privacy of their data. Following incident resolution, follow-up is required to ensure that the incident has been resolved effectively and that the threat is no longer present. We are aligned with ISO 27k standards for event and incident management and have formal incident management policies and processes in place. These policies and procedures are tested in the ISO 27k and SOC 2 audits.
FireEye	FireEye has a documented policy for incident management that has been approved by management and communicated to appropriate constituents and owners. It is continuously maintain and reviewed annually. The plan has a reporting structure and escalation path. An incident response team with defined roles and response related qualifications are available 24x7x365. The team maintains chain of custody for evidence during the incident investigation. There is a process for reporting client notification for regulatory, legal and contractual issues after a breach if a breach were to be confirmed. If a confirmed breach were to occur a management team would review all the factors and develop a remediation plan to mitigate.	
VirtueStream	There are two primary Incident types; Security Incidents, where there is a possible breach in systems or data integrity, and Services, where there is in impacted or affected service. Although there is some overlap, generally any security-related incident should be classified as a Security Incident and the response must be managed using the 'Virtustream Information Security Procedure – Security Incident Response Plan'. The purpose of this security incident response plan is to provide general guidance to Virtustream staff- both technical and managerial – to enable quick and efficient recovery from security incidents; respond in a systematic manner to incidents and carry out all necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission critical information including sensitive credit card data. The plan is also a guide to sharing information with other stakeholder organizations who might be impacted by such security incidents such as the credit card associations and law enforcement. The Security Incident Response Plan (SIRP) provides guidance to prepare for, respond to, and recover from potential incidents. Policy statements surrounding the IR-Plan are provided to ensure continued upkeep and standardized use. The SIRP guidance at the procedural level defines the roles, responsibilities, communication methods and flows, contact information, types of potential incidents, and immediate actions that are to be taken upon an incident's identification, and elaborates with subsequent recovery steps. Virtustream's Incident Response Policy requires the implementation and testing of a generalized plan that adheres to the International Standards Organization 27002 guidance for incident management and response, but meets specific requirements for compliance such as PCI-DSS. The Plan covers the corporate environment associated with Virtustream's IT assets, the local IT resources and the IT resources at Virtustream's Data Center. It consists of a series of guidelines (Incident Response Guidelines or "IRG") that should generally be followed as appropriate for the circumstances as when a security incident occurs or as part of the ongoing maintenance of this plan. As the incident progresses and has more impact (i.e. severity level increases), the escalation process will be used to engage appropriate resources. Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact, and to keep tight control. The Table below defines the escalation levels with the associated team involvement.	

8.7 Migration and Redeployment Plan

8.7.1 Offeror must describe how it manages the end of life activities of closing down a service to a Purchasing Entity and safely deprovisioning it before the Offeror is no longer contractually obligated to maintain the service, include planned and unplanned activities. An Offeror's response should include detail on how an Offeror maintains security of the data during this phase of an SLA, if the Offeror provides for redundancy during migration, and how portable the data is during migration.

The end of life activities for each Purchasing Entity will vary based on the type of service they are currently using and the service that they will be moving too. All Purchasing Entities will be notified in advance of any end of life service so that the Purchasing Entity can work with Carahsoft and the service providers to develop a plan exporting and transitioning data.

8.7.2 Offeror must describe how it intends to provide an orderly return of data back to the Purchasing Entity, include any description in your SLA that describes the return of data to a customer.

At all times during the course of the Service, the Purchasing Entities will have access and ownership of their data. The Purchasing Entity is free to download or access the data through a variety of means based on the service at any time during their service period.

8.8 Service or Data Recovery

8.8.1 Describe how you would respond to the following situations; include any contingency plan or policy.

a. Extended downtime.

CA	APM	If unable to resolve in a timely manner, all customers will be notified via email to the registered admin
	MAA	Customers are kept abreast with progress during incidents, including outages. CA utilizes best-of-breed notification system which enables customer contacts to self-subscribe to different types of notifications that they would be interested in. A DR plan has been created should the extended down time result in DR declaration.
	CA Agile	We would failover to our warm data center in order to restore access to the application as quickly as possible. This is done according to our Disaster Recovery Plan
	ASM	If unable to resolve in a timely manner, all customers will be notified via email to the registered admin. Failover from the primary to DR site may be utilized if the extended amount of time warrants declaration of DR.
Google	Due the redundant nature of the Google infrastruture there is no expectation of any extended downtime. If a data center in use by any of your end users suffers a catatrophic failure, Google's dynamic health monitoring would just reroute the session to a different data center.	
AODocs	All the AODocs data is hosted on the Google Cloud Platform infrastructure. AODocs does not manage any physical infrastructure. Due the redundant nature of the Google infrastruture there is no expectation of any extended downtime. If a data center in use by any of your end users suffers a catatrophic failure, Google's dynamic health monitoring would just reroute the session to a different data center.	
Virtru	Notify users that Virtru service is unavailable, and recommend that they use their offline encryption tools and backups to perform emergency functions.	
Salesforce	Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (http://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers' trust. To ensure maximum uptime and continuous availability, Salesforce provides the best	

	redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance. Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Live and historical statistics on the Salesforce system performance are publicly published at http://trust.salesforce.com/trust/status. The persistence layer underlying Salesforce Platform is proven database technology that powers all of Salesforce's products today, serving more than 150,000 organizations and over 4 billion transactions per day with an average request response time of less than .25 seconds, all with an average up time of 99.9+ percent.
ServiceNow	ServiceNow's data centers and cloud-based infrastructure have been designed to be highly available. All servers and network devices have redundant components and multiple network paths to avoid single points of failure. At the heart of this architecture, each customer application instance is supported by a multi-homed network configuration with multiple connections to the Internet. Production application servers are load balanced within each data center. Production database servers are replicated in near-real time to a peer data center within the same geographic region. ServiceNow leverages this Advanced High Availability (AHA) architecture for customer production instances in several ways: •In the event of the failure of one or more infrastructure components, service is restored by transferring the operation of customer instances associated with the failed components to the peer data center. •Before executing required maintenance, ServiceNow can proactively transfer operation of customer instances impacted by the maintenance to the peer data center. The maintenance can then proceed without impacting service availability. This approach means that the transfer between active and standby data centers is being regularly executed as part of standard operating procedures – ensuring that when it is needed to address a failure, the transfer will be successful and service disruption minimized. RTO is 2 hours. RPO is 1 hour. See the "ServiceNow Security, Operations, and Compliance White Paper" included with this response for more information.
QTS	In the rare instance of failure of the commercially-delivered electrical power, back-up systems at each QTS data center start instantaneously. Batteries provide power for the first 12-15 seconds while on-site diesel generators spin up to synchronize their output with the battery-supplied feed. Once on-line, the generators can supply power indefinitely, and the IT equipment on the data floor as well as critical infrastructure components are all unaffected. While the basics of reliable power seem simple, none of this is taken for granted. Battery banks are sized to provide 15 minutes of power, well beyond the 15 seconds that it typically takes generators to come on line. Inspections are conducted daily and quarterly to ensure that the battery banks are prepared at all times. The diesel generators are inspected by running them each month to circulate and condition the fuel, then running them annually under the full simulated load of the current IT equipment on the data center floor. Factory technicians inspect and maintain the generators semi-annually. Quantities of fuel sufficient to support 48-72 hours of

	operation without resupply are stored on-site, and re-supply contracts are in place with multiple providers to have fuel delivered as soon as the generators come on line.	
SAP	Ariba	Ariba has implemented two sites within each region. In North America the sites are currently located in San Jose, California and Sterling, VA. In Europe the sites are located in St. Leon-Rot, Germany and Amsterdam, Netherlands. The act of failing over from one site to another has a design goal for its Recovery Time Objective (RTO) of no more than four hours. The design goal for the Recovery Point Objective (RPO) is five minutes. Disaster recovery options are included for all Ariba Cloud Services. In the event of a fail-over to the disaster recovery site, no customer changes are required as all URLs that customers use to reach the applications will continue to work. Ariba will notify customers via their email addresses in the event of unplanned downtime. Internally, Ariba uses a documented system recovery plan that outlines the approach and steps for recovering the applications. This document defines roles and responsibilities in the event of disaster: Local Ariba staff maintains the hardware remotely. Ariba maintains the application software. Processes are in place to keep database and fileservers in sync between primary and backup data centers. The failover process of all parts of the infrastructure is automated. In the event of a catastrophe, Ariba will declare the primary data center "down" and locally the script will be run to switchover and start the applications at the remote data center. Ariba tests power outage backup scenarios and the Disaster Recovery Plan on a periodic basis to ensure it is up-to-date, successful, and effective.
	Fieldglass	Customers are notified of unscheduled downtime immediately via email. Updates are frequently emailed out until the issue has been resolved. Customers are notified of scheduled downtime 5 days prior via email.
	Hanna	In case of a disaster depending on the infra & technical architecture defined during HEC technical assessment workshop, systems could fail over to HA node. If DR (optional offering) is selected, the systems could move to secondary DC that where contracted with a DR option & HEC declaring DR. Regular system downtime for patching etc. is planned in advance with the customer and typically follows customers maintenance schedules.
	Hybris	SAP Hybris offers continuous 24/7 systems monitoring in-place, which automatically notifies you, SAP Hybris support and optionally your designated implementation partner in the event of any monitored system problem. Tools used for monitoring include HP Sitescope and Nagios. This service ensures quick response times to emergency problems. Standard monitors are in place for basic site availability. Customer can utilize additional 3rd party monitoring services should it wish to add additional monitoring. Upon request, monthly or quarterly reviews are offered to review performance over the period. When a system problem occurs, in addition to monitor alerts sent to the customer, SAP Hybris support may send emails to a designated customer notification email address to provide status, updates or further detailed information. In addition, a support ticket would be created which would include such information.
	SuccessFactors	Our infrastructure architecture is designed with high availability in mind, and engineered for resiliency. All major components are redundant, including power, HVAC, fire suppression, and the physical components of our network. Production data centers have strict access controls, and are continuously

		staffed and monitored to help prevent acts of sabotage or vandalism. All production data centers are ANSI/EIA/TIA-942Tier III/IV facilities, and are ISO 27001 certified. Production data centers are also geographically dispersed to help prevent a single event from affecting more than one data center. In the event a production data center has an outage we failover to an alternate data center in the same geographic region to minimize impact to customers. Our Cloud Operations teams are also geographically dispersed, working in offices in the US, Europe, South America, and India. Should an office be impacted by an environmental event or pandemic, other offices can continue operations. Aspects of the plan are described in the SOC reports, Disaster Recovery Plan ("DRP") and Business Continuity Plan ("BCP") solutions are dependent on several factors. The customer may be responsible for parts of the recovery/continuity activities.
VMware	VMware vCloud Air leverages proven VMware High Availability technology to minimize the risk of extended downtime. In the unlikely event that an extended outage does occur, VMware will support guide the customer's efforts to restore services to an alternative vCloud Air or vCGS datacenter. We will also provide remedies in the form of service credits as outlined in the following VMware vCloud Air, vCGS, Vmware AirWatch and VMware Identity Manager SLAs.	
FireEye	FireEye has a mature and documented Business Continuity Plan and Disaster Recovery Plan that follows industry best practices that is reviewed and tested annually. The BCP/DRP plan has RPO/RTO timing criteria and other critical business requirements that is available for review if requested in the future.	
VirtueStream	In the event of extended downtime affecting production systems, Virtustream and customer would jointly evaluate the situation and mutually decide on failover declaration, whereby Virtustream would then execute the failover plan to restore customer operations to the secondary data center.	

b. Suffers an unrecoverable loss of data.

CA	APM	Customer data is isolated within dedicated schemas with nightly backups. The maximum data loss would be the previous 24hrs.
	MAA	MAA data is backed up fully daily. The maximum data loss would be the previous 24hrs.
	CA Agile	We have implemented a physical standby database in both hot/Live site as well as warm/standby sites using Oracle Data Guard with real-time apply to achieve the stated recovery objectives.
	ASM	Customer data is isolated within dedicated schemas with nightly backups. The maximum data loss would be the previous 24hrs.
Google	Google performs real time data replication to avoid unrecoverable data loss. Customers that configure the retention policies in Google Apps Vault can ensure that end users can not inadvertently or maliciously delete email in advance of any defined retention schedules.	
AODocs	AODocs data are stored in Google AppEngine and Google Drive: - The data stored in Google AppEngine are backed up every day. The application is hosted on Google Cloud Platform infrastructure and benefits from the network security described in this whitepaper: https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf - Data stored in Google Drive is managed by Google within its multiple servers location. Altirnao does not manage this infrastructure. Google Drive can be backed up by third party tool such as Backupify.	

Virtru	Notify users that data within Virtru is unavailable, and recommend that they use their offline encryption tools and backups to perform emergency functions.	
Salesforce	To maximize availability, the service is delivered using multiple world-class data centers supporting primary and replicated disaster recovery instance, plus a separate production-class lab. The infrastructure utilizes carrier-class components designed to support millions of users. Extensive use of high-availability servers and network technologies, and a carrier-neutral network strategy, help to minimize the risk of single points of failure, and provide a highly resilient environment with maximum uptime and performance. The Salesforce services are configured to be N+1 redundant at a minimum, where N is the number of components of a given type needed for the service to operate, and +1 is the redundancy. In many cases, Salesforce has more than one piece of redundant equipment for a given function.	
ServiceNow	Please see our response for 8.8.1a	
QTS	QTS cloud developed a OPS_POL_54_QTS-FC_Contingency_Planning_Policy (v1.2 – 2/6/14), detailing the policies, procedures, roles and responsibilities of key personnel in the event of an emergency and/or disaster.	
SAP	Ariba	Our SLA provides tenant remuneration for losses they may incur due to outages within the infrastructure.
	Fieldglass	The maximum data loss timeframe is guaranteed to be less than three hours; however, offsite backups are performed every 15 minutes so the timeframe is actually much shorter.
	Hanna	Data loss is defined by RPO & RTO. HEC has a maximum RPO of 30 mins & RTO of 12 hours.
	Hybris	For a cloud solution, data backup and restore is handled by SAP. SAP shall follow its archiving procedures for Customer Data as set out in the SAP Hybris Commerce, cloud edition Services Description. In the event of any loss or damage to Customer Data, SAP shall use commercially reasonable efforts to restore the lost or damaged Customer Data from the latest back- up of such Customer Data maintained by SAP in accordance with the archiving procedure described in its SAP Hybris Commerce, cloud edition Services Description. SAP shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by any third party, (except those third parties sub- contracted by SAP to perform services related to Customer Data maintenance and back-up).
	SuccessFactors	Our SLA provides tenant remuneration for losses they may incur due to outages within the infrastructure.
VMware	VMWare IaaS Services As discussed in detail in section 8.8.2.1.a below, VMware IaaS services are architected to minimize the risk of unrecoverable data loss. In addition option services such as vCloud Air Data Protection can be leveraged to further mitigate any risk. VMware's vCloud Air policy regarding data loss can be found in the vCloud Air Terms of use. VMware's vCloud Government Service policy regarding data loss can be found in the vCloud Government Service Terms of Service AirWatch Hosted Services AirWatch Business Continuity and Disaster Recovery strategies include data and hardware redundancy, network configuration redundancy and backups, and robust, regular testing exercises. AirWatch features active-passive configurations for high availability and redundancy with all components made to failover with minimal downtime. Load balancing capabilities are deployed across multiple data centers to ensure timely server recovery. AirWatch also incorporates replication technology featuring SQL log shipping or network SAN byte replication to prevent data loss.	

	• Due to FOIA restrictions and the competitive nature of the EMM marketplace, we cannot provide specific details regarding recovery strategies or timelines.
FireEye	FireEye has a mature and documented Business Continuity Plan and Disaster Recovery Plan that follows industry best practices that is reviewed and tested annually. The BCP/DRP plan has RPO/RTO timing criteria and other critical business requirements that is available for review if requested in the future.
VirtueStream	Multiple copies of customer data exist in multiple datacenters – in the primary datacenter, there is the production copy and a local backup. The local backup is replicated to a secondary datacenter and the production datastores associated with coreVM's are also replicated at regular intervals to the secondary datacenter. If NASPO feels that additional steps/redundancy are required to maintain recoverability, Virtustream is open to discussion.

c. Offeror experiences a system failure.

CA	APM	Disaster to the CA Technologies corporate network in New York will not affect customers' service. Secondary services, such as domain name services will be routed through the secondary CA Technologies network in Illinois. CA has a BCP plan in place to direct its services. The SaaS environment is separate from the CA corporate network and a service specific disaster recovery plan is in place.
	MAA	Customers would be notified in advance, and given ample time to retrieve their data.
	CA Agile	We enable all of our employees with the ability to be able to work remotely and provide remote network access to ensure business functions can continue. All corporate infrastructure has redundate systems that can be utilized in the event of failure.
	ASM	Customers would be notified in advance, and given ample time to retrieve their data manually or via the ASM API.
Google	Google's corporate network is separate from it's production infrastructure. Google is a global organization that has support personnel located at key office installations and tests our business continuity programs annually. These tests are to validate that if corporate headquarters is off the grid that criticial business functions can be picked up by other staff.	
AODocs	AODocs runs 100% over Google's Cloud Platform infrastructure that is naturally redundant, and all AODocs internal systems such as technical support, email, collaboration, source code hosting, etc are run on cloud based services. AODocs personnel can work from any physical location without any business disruption and they do work from remote locations on a regular basis. If one of the AODocs facilities were to be temporarily unavailable due to a natural disaster, AODocs personnel would be able to perform their work without significant interruption.	
Virtru	Notify users that Virtru is or will be permanently unavailable, and recommend that they use their offline encryption tools and backups to perform emergency functions.	
Salesforce	Please see response to items a. and b. above and d. and e. below. Salesforce has documented Disaster Recovery and Business Continuity plans for critical business functions. The Disaster Recovery and Business Continuity plans are tested at least annually. A post mortem documenting the results of the disaster recovery tests can be provided to customers with a signed NDA in place. Business continuity plans are updated each year, including the list of business processes, recovery time objectives, and key resources. Senior management is included in this process. Business continuity plans are exercised on an annual basis. Action items and lessons learned are tracked from each incident and exercise conducted. Action items are prioritized and tracked until	

	closed. Salesforce has developed additional procedures, processes and plans, including a Pandemic plan. Salesforce also recommends customers also devise their own backup strategy for their data, as there is a fee for customers to request for restoration from Salesforce backups. Salesforce provides multiple ways for our customers to obtain periodic backups of its data. We offer a weekly export service (WES) for those customers requiring a local backup copy of their data or a data set for import into other applications (such as an ERP system). Salesforce also supports data replication, which allows customers to store and maintain a local, separate copy of their organization's Salesforce data including the META data (logins, etc.) for specialized uses, such as data warehousing, data mining, custom reporting, analytics, and integration with other applications. Data replication provides customers with local control and the ability to run large or ad hoc analytical queries across the entire data set.	
ServiceNow	Please see our response for 8.8.1a	
QTS	QTS has established an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions within [Assignment: organization-defined time period consistent with recovery time objectives] when the primary processing capabilities are unavailable. The QTS cloud hosting facilities in Richmond, VA (RIC1) and Atlanta, GA (ATL1) have agreements with each other to restore services in the event that one of the sites becomes unavailable. Both facilities are QTS managed facilities and are always available to meet the recovery time and recovery point objectives for the system. Agreements are in place to allow QTS to access resources at the alternate processing site physically and via the QTS client network. Richmond and Atlanta Datacenters are independently operated datacenters that offers disaster recovery services to customers. The contingency approach ensures that hardware and software components needed for recovery efforts are already at the alternate facility. QTS ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption. Network circuits, networking infrastructure, storage, virtual servers, and management components required to resume operations are available and configured at the alternate site.	
SAP	Ariba	"Ariba modules automatically persist object state to the underlying relational database as users work. When a user performs a significant action, for example, adding an item to an order, performing an approval, etc., the Ariba application tier is aware of the change and automatically saves the relevant object state to the database. This provides transparent persistence of the user's work without the user having to "save" or "submit" changes to avoid losing work in the event of failure or session timeout. This in turn means that the loss of any connections between the tiers or failure of one of the tiers will not leave data in an inconsistent state. While object data is cached in the middle tier for performance, the official record is stored in the database to avoid any potential data loss or corruption. This means that recovery for Ariba modules is implicit and automatic. When the modules start, they retrieve the state of the various business objects from the underlying database as needed for user sessions. If an Ariba module fails, there is no special application recovery process other than restarting the module. The Ariba module will automatically connect to the database and as clients login and commence working, all required business object data will be retrieved from the database."

	Fieldglass	Fieldglass' business continuity program (BC Program) was established to ensure that, after a complete disruption of its Chicago and/or Naperville, Illinois offices, all employees and the functions for which they are responsible, are capable of continued operations in less than one business day. This includes office space as well as all equipment and supplies needed to continue its operations without an interruption in customer services. Fieldglass' BC Program is integrated into all facets of the company due to the criticality of the product that it sells and supports. As such, representatives from all areas of the company are responsible for ensuring that they are familiar with their duties and responsibilities during a disruption and how to recover their areas after the disruption occurs.
	Hanna	Service Level Credits Where SAP fails to meet a Service Level, SAP will be liable to Customer for the corresponding Service Level Credit as set out in this section. The Service Level Credit is calculated as the sum of the Service Level Credits for both DEV/QAS and PRD for the TA Service Level defined in section 5.1 above. SAP will deduct the amount of any Service Level Credits owed to Customer from the next invoice (or, if there is no such invoice, by bank transfer to such bank account as Customer may specify in writing). Customer agrees that under no circumstances will the total maximum Service Level Credits: (i) for any one month, exceed 100% of the Service Fee for that month; and, (ii) for any given contract year, exceed in the aggregate an amount equal to one- third of the annual Service Fee charged for the contract year (or one third of the total Service Fee charged if the Term as defined in the applicable Order Form is less than one (1) year). Customer acknowledges that the Service Level Credits defined hereunder are the sole remedy for SAP's failure to meet the specified Service Level. 5.6 Termination for Service Level Failure Customer may terminate the applicable Order Form with thirty (30) day's termination notice in writing to SAP, if SAP misses a Service Level as specified in this Supplement for three (3) months in sequence. Customer may exercise this termination right only within thirty (30) days after receipt of the respective Service Level report that documents the applicable Service Level failure that would cause such termination right to accrue in Customer.
	Hybris	SAP isn't likely to go out of business in the near future. However, our contract states the following: Upon expiration or termination of the Agreement, SAP may destroy or otherwise dispose of any of Customer Data in its possession unless SAP (i) is requested by Customer to extend the term of the Order Form as permitted in the Order Form to allow Customer to retrieve Customer Data, or (ii) receives, no later than thirty (30) days after the effective date of the termination of this Agreement, a written request for the delivery to Customer of the then most recent back-up of the Customer Data. SAP shall use reasonable commercial efforts to deliver the back-up to Customer within thirty (30) days of its receipt of such a written request, provided that Customer has, at that time, paid all fees and charges outstanding and owed at termination. Customer shall pay all reasonable fees and expenses incurred by SAP in returning or disposing of the Customer Data.

VMware	AirWatch Hosted Services AirWatch Business Continuity (BC) strategies include clear policies and procedures as well as robust, regular testing exercises. Our BC recovery strategies for support and maintenance include provisions for workforce mobility, secondary support locations, and defined leadership roles and responsibilities for all recovery staff. • Multiple Support Locations – AirWatch maintains a Global Support Team, which spans multiple offices around the world. This ensures that if a disaster occurs at one of our offices, our remaining Support Team members can provide assistance to our customers. • Mobile Workforce – Should an AirWatch office become inaccessible, all AirWatch employees are equipped with laptops and can access necessary internal resources. • Defined Leadership – During a disaster, roles and responsibilities are assigned to key personnel, and a recovery manager provides leadership and documents the continuity process. Additionally, emergency contact numbers for key personnel are provided for all vendors and support staff.
FireEye	FireEye has a mature and documented Business Continuity Plan and Disaster Recovery Plan that follows industry best practices that is reviewed and tested annually. The BCP/DRP plan has RPO/RTO timing criteria and other critical business requirements that is available for review if requested in the future.
VirtueStream	Virtustream has built redundancy into all layers of the physical infrastructure in order to deliver SLAs up to 99.999% and mitigate the risks of a system failure. Additional levels of protection include regular system backups (stored locally and replicated offsite) as well as automatic storage replication to a secondary data center to facilitate the ability to restore operations in the event of a system failure.

d. Ability to recover and restore data within 4 business hours in the event of a severe system outage.

CA	APM	CA provides an SLA of 99.8% uptime, which can result in unforeseen outages of ~1.5 hours per month. In the event of a failure to meet a SLA threshold , Customer is entitled to a number of days of credit.
	MAA	Using DB clustering technologies, multiple copies of data are maintained helping in recovery of the data.
	CA Agile	We can meet this requirement.
	ASM	Data is replicated from the primary (production) to secondary (DR) continuously. In the event of catastrophic loss of live data a failover to the DR site would be necessary.
Google	Google's RTO is zero.	
Virtru	See 'Virtrù Incident & Breach Policy'	
Salesforce	Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, and backed up at the primary data center. Backups are performed daily at primary data center facility without stopping access to the application. For business continuity purposes, Salesforce supports disaster recovery with a dedicated team and a 4 hour recovery point objective (RPO) and 12 hour recovery time objective (RTO). Additional details can be provided with the execution of an NDA between Salesforce and your Agency.	
ServiceNow	Please see our response for 8.8.1a	
QTS	As defined in QTS OPS_POL_54_QTS-FC_Contingency_Planning_Policy (v1.2 – 2/6/14), QTS cloud has identified the following potential accessibility problems: • Network Outage – Short Term • Network Outage – Long Term • Facility Power or Environmental Outage – Short Term	

	• Facility Power or Environmental Outage – Long Term • Serious Facility Damage – Short Term • Serious Facility Damage – Long Term or Permanent Both the RIC2 and ATL1 QTS cloud Infrastructure is an Active/Active system and can operate independently of each other indefinitely. If QTS cloud determines that any single event (network, power, facility damage) presents a long-term threat, QTS immediately conducts an emergency meeting and plan to remedy or relocate infrastructure to a viable facility."	
SAP	Ariba	Ariba has implemented two sites within each region. In North America the sites are currently located in San Jose, California and Sterling, VA. In Europe the sites are located in St. Leon-Rot, Germany and Amsterdam, Netherlands. The act of failing over from one site to another has a design goal for its Recovery Time Objective (RTO) of no more than four hours. The design goal for the Recovery Point Objective (RPO) is five minutes.
	Fieldglass	Fieldglass offers the following: • RTO = No more than 48 hours • RPO = No more than 6 hours. Warm site replica with 100% processing power of original site. Disaster recovery site can run without need from resumption.
	Hanna	See our RTO and RPO info below
	Hybris	For a cloud solution, data backup and restore is handled by SAP.SAP shall follow its archiving procedures for Customer Data as set out in the SAP Hybris Commerce, cloud edition Services Description. In the event of any loss or damage to Customer Data, SAP shall use commercially reasonable efforts to restore the lost or damaged Customer Data from the latest back- up of such Customer Data maintained by SAP in accordance with the archiving procedure described in its SAP Hybris Commerce, cloud edition Services Description. SAP shall not be responsible for any loss, destruction, alteration or disclosure of Customer Data caused by any third party, (except those third parties sub- contracted by SAP to perform services related to Customer Data maintenance and back-up). Both IDS and IPS are included the SAP Hybris Commerce, Cloud Edition The security infrastructure includes firewall security and hardened security policies on all servers. Log management procedures are in-place for log review for firewall, applications, network devices, including file-integrity management. SAP Hybris utilizes technologies from leading security firms for Log Management and File Integrity Management. SAP Hybris employs two-factor authentication across its network. SAP Hybris undergoes vulnerability and penetration testing. SAP Hybris validates against requirements for PCI DSS 2.0. The infrastructure also includes Web Application Firewalls and DDoS Mitigation Services. In addition, security policies and change management policies are in-place ensuring that all access and changes to customer systems and information is accessible only by SAP Hybris staff with access authorization. Security of the software application which is controlled by the Customer (or its implementation partner) remains the responsibility of the Customer. Upon expiration or termination of the Agreement, SAP may destroy or otherwise dispose of any of Customer Data in its possession unless SAP (i) is requested by Customer to extend the term of the Order Form as permitted in

		the Order Form to allow Customer to retrieve Customer Data, or (ii) receives, no later than thirty (30) days after the effective date of the termination of this Agreement, a written request for the delivery to Customer of the then most recent back-up of the Customer Data. SAP shall use reasonable commercial efforts to deliver the back-up to Customer within thirty (30) days of its receipt of such a written request, provided that Customer has, at that time, paid all fees and charges outstanding and owed at termination. Customer shall pay all reasonable fees and expenses incurred by SAP in returning or disposing of the Customer Data.
	SuccessFactors	RPO and RTO are defined in the general terms and conditions
VMware	VMware Response: VMware IaaS Services VMware DR service. We can discuss specific recovery information under NDA to participating entities during task order negotiations as required. AirWatch Hosted Services We can discuss specific recovery information under NDA to participating entities during task order negotiations as required.	
FireEye	FireEye has a mature and documented Business Continuity Plan and Disaster Recovery Plan that follows industry best practices that is reviewed and tested annually. The BCP/DRP plan has RPO/RTO timing criteria and other critical business requirements that is available for review if requested in the future.	
VirtueStream	Basic Plus microVM's are designed for mission-critical workloads and for systems that require DR, addition of reserved compute capacity in a secondary datacenter (i.e. Reserve uVM) and automatic storage replication to facilitate the ability to restore operations in the event of an outage at the primary data center. RPO and RTO for core microVM's are 15 minutes and 2 hours respectively.	

e. Describe your Recovery Point Objective (RPO) and Recovery Time Objective (RTO).

CA	APM	Recovery Point Objective (RPO): Maximum data loss: 24 hours Data that is uploaded, but not backed up within the 24 hours may have to be re-entered Recovery Time Objective (RTO): 72 hours
	MAA	Recovery Point Objective (RPO): Maximum data loss: 24 hours Data that is uploaded, but not backed up within the 24 hours may have to be re-entered Recovery Time Objective (RTO): 72 hours
	CA Agile	RTO: 2 hours RPO: 12 hours
	ASM	Recovery Point Objective (RPO): Maximum data loss: 24 hours Data that is uploaded, but not backed up within the 24 hours may have to be re-entered Recovery Time Objective (RTO): 24 hours
Google	RPO/RTO objectives are zero hours.	
AODocs	AODocs is hosted on Google App Engine which is designed to be highly available. Our standard SLA is 99.5% . Specific financial penalties can be discussed as part of the AODocs license contract. Google App Engine is running in multiple datacenters on multiple continents.	

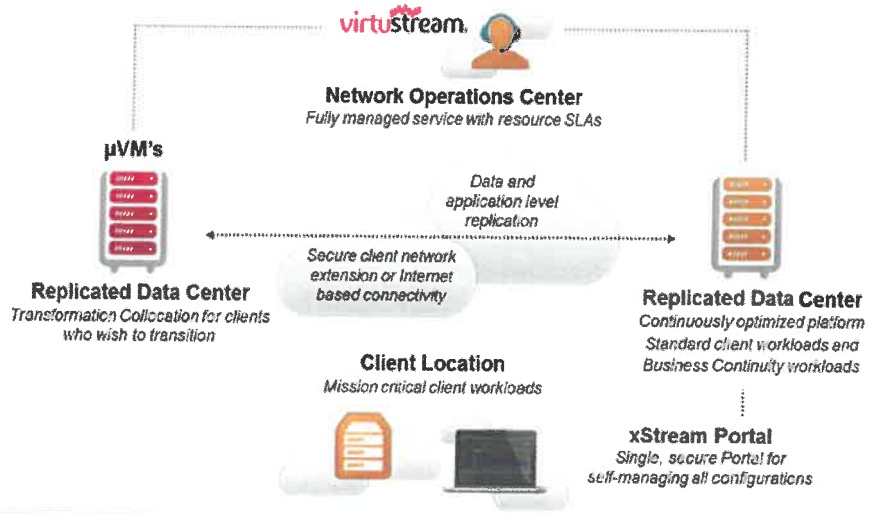
	AODocs data is backed up on a daily basis, and backups are stored on the highly redundant Google Cloud Storage. Backups are retained for at least 90 days	
Virtru	See 'Virtru Incident & Breach Policy'	
Salesforce	For business continuity purposes, Salesforce supports disaster recovery with a dedicated team and a 4 hour recovery point objective (RPO) and 12 hour recovery time objective (RTO). Additional details can be provided with the execution of an NDA between Salesforce and your Agency.	
ServiceNow	Please see our response for 8.8.1a	
QTS	QTS DRaaS will support all of your mission-critical application needs and enables you to achieve a RTO within minutes and RPO of just seconds.	
SAP	Ariba	See above
	Fieldglass	Fieldglass offers the following: • RTO = No more than 48 hours • RPO = No more than 6 hours. Warm site replica with 100% processing power of original site. Disaster recovery site can run without need from resumption.
	Hanna	For disaster Recovery, SAP HEC offers the following RTO & RPO 1. HANA Database RTO - 12 hours, RPO - 30 minutes 2. Sybase ASE Database RTO - 12 hours, RPO - 30 minutes
	Hybris	In the case of catastrophic failure to your primary production data center, we offer anywhere from best efforts to enhanced DR solutions. Enhanced DR options translates to either RTO of 8 hours and RPO of 1 hour for a warm standby solution, or RTO of 30 minutes to RPO of 30 minutes for a hot-site. Customers have 3 choices in DR sites: • as part of our base offering, best effort DR, we would bring your site back up in an alternate datacenter which is a minimum of 500 miles away from the primary datacenter. We would actually push your project server images to the alternate datacenter, but we would still need to set up your various interfaces, 3rd party services, etc, which could day a few days. • 2nd would be to have your DR site managed by hybris Managed Services. • 3rd would be to use your own DC as a DR site, We would need to set up a technical call with our combined teams to synch up on the replication strategies. • Our DR services utilizes VMware Site Recovery Manager with storage-based replication. • For enhanced DR, we would include one annual DR test, but more can be added if required. It also includes a customer specific DR and Business Continuity plan.
	SuccessFactors	Within the contract/subscription agreement, there are provisions for data recovery in the event of disaster. SLA's for RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are defined in the contract. We will prioritize data recovery based upon our contractual obligations for each customer, concerning RTO and RPO.

VMware	VMware IaaS Services Provide the RPO and RTO for DR, point to SLAs for others. RTO – 4 hours or less RPO – 15 minutes to 24 hours – time is configurable by user but there is a bandwidth consideration for shorter replication times. VMWare AirWatch AirWatch Business Continuity (BC) and Disaster Recovery (DR) strategies include data and hardware redundancy, network configuration redundancy and backups, and robust, regular testing exercises. • Business Continuity – Our BC recovery strategies for support and maintenance include provisions for workforce mobility, secondary support locations, and defined leadership roles and responsibilities for all recovery staff. o Multiple Support Locations – AirWatch maintains a Global Support Team, which spans multiple offices around the world. This ensures that if a disaster occurs at one of our offices, our remaining Support Team members can provide assistance to our customers. o Mobile Workforce – Should an AirWatch office become inaccessible, all AirWatch employees are equipped with laptops and can access necessary internal resources. o Defined Leadership – During a disaster, roles and responsibilities are assigned to key personnel, and a recovery manager provides leadership and documents the continuity process. Additionally, emergency contact numbers for key personnel are provided for all vendors and support staff. • High Availability and Disaster Recovery – AirWatch features active-passive configurations for high availability and redundancy with all components made to failover with minimal downtime. Load balancing capabilities are deployed across multiple data centers to ensure immediate server pick up, ensuring zero end user downtime. AirWatch also incorporates replication technology featuring SQL log shipping or network SAN byte replication to prevent data loss. Due to FOIA restrictions and the competitive nature of the EMM marketplace, we cannot provide specific details regarding recovery strategies or timelines.
FireEye	FireEye has a mature and documented Business Continuity Plan and Disaster Recovery Plan that follows industry best practices that is reviewed and tested annually. The BCP/DRP plan has RPO/RTO timing criteria and other critical business requirements that is available for review if requested in the future.
VirtueStream	Virtustream's solution will have a Recovery Point Objective (RPO) of 2 Hours and Recovery Time Objective (RTO) of 30 Minutes for all disaster recovery enabled workloads. The Virtustream Cloud has been designed to deliver continuous operations. The platform is architected to be highly available, with SLAs as up to 99.99%. All infrastructure systems are run in at least an N+1 model and have been designed with no single points of failure. All of the data center facilities and infrastructure has redundant power supplies connected to separate circuits from separate power feeds. Every device is connected via redundant pathways at a LAN/SAN/WAN layer. State of Utah can choose any of our FedRAMP Data Centers to host their applications and the DR location. For illustrative purposes, we have assumed the primary data center will be USDC02 and DR data center would be USDC01. The State of Utah solution has been designed with all workloads running in our San Francisco (USDC02) data center. In the unlikely event of a disaster at the USDC02 facility, State of Utah's production services will be brought back online in the secondary data center located in Northern Virginia (USDC01). The target RPO is 30 minutes for virtual machines with a 2 hour RTO. All production workloads in the primary node will have reserved compute capacity in the secondary node when deployed using Reserve µVMs and replicated storage. All virtual machine disaster recovery services are based on storage replication. The primary and secondary data centers are interconnected by diverse private 10 Gbps Sonet rings from separate Tier 1 providers – AboveNet and Level 3. Data is replicated asynchronously and continuously between the two data centers.

Virtustream also performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by State of Utah per landscape and will be documented during the on-boarding process.

Figure 2. Integrated Disaster Recovery

Virtustream's cloud platform includes integrated disaster recovery (30 Min RPO & 2 Hr RTO) and backup.



8.8.2 Describe your methodologies for the following backup and restore services:

a. Method of data backups

CA	APM	Backups are stored on disk only
	MAA	Backups are stored on disk only, sync'd between data centers for DR purposes.
	CA Agile	Full database backups are taken once per week, both to onsite and offsite (our warm data center, not a separate 3rd party) systems. Incremental backups are run nightly. Backups are retained for 21 days after which time they are simply aged out and over-written. In addition, snapshots of database transactions are taken every hour to an disaster recovery site allowing for emergency disaster recovery with maximum of 1.5 hours of data loss due to catastrophic onsite failure (fire in cage, natural disaster, etc. at data center). Backups are tested monthly and a full disaster recovery process to the offsite application cluster is tested semi-annually.
	ASM	Backups are stored on disk only, sync'd between data centers for DR purposes.
Google	Keeping in mind that Google stores customer data in encrypted chunks or shards on several servers at several data centers backups should not be considered customer specific. Daily backups of each server are performed to encrypted tapes at each data center.	
Virtru	We perform live database replication to a separate redundant database in Oregon and offline as well in a separate Amazon AWS Region	
Salesforce	Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, backed up at the primary data center, and then cloned to the disaster recovery data center. Disaster recovery tests verify our projected recovery times and the integrity of the customer data.	

	Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Tapes never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process. The backup retention policy is 90 days (30 days for sandboxes). Deleted / modified data cannot be recovered after 90 days (30 days for sandboxes). If customers want a longer retention, they can use the weekly export feature available in the system.	
ServiceNow	While Advanced High Availability as described in 8.8.1 is the primary means to recover data and restore service in the case of a service disruption, in certain cases it is desirable to use ServiceNow's more traditional data backup and recovery mechanism. This data backup and recovery system works in concert with AHA and acts as a secondary recovery mechanism. ServiceNow stores production instances in two geographically separate regional data centers, with sub-production instances hosted in a single data center. Backups of the two production databases and the single sub-production database are taken everyday for all instances throughout the private cloud infrastructure. The backup cycle consists of four weekly full backups and the past 6 days of daily differential backups that provide 28 days of backups. All backups are written to disk, no tapes are used and no backups are sent off site. All the controls that apply to live customer data also apply to backups. If data is encrypted in the live database then it will also be encrypted in the backups. Regular, automated tests are run to ensure the quality of backups. Any failures are reported for remediation within ServiceNow.	
QTS	QTS operates and manages high-performance, multi-tenant platforms on which customer system and data file backups can be created and retained for rapid restore of files/volumes. Data can be stored on tape or disk, depending on QTS location, and can reside locally in a QTS data center or off-site. If there is a need for off-site data retention, the backup medium is tape. QTS can also replicate the backed up data from the primary site to a secondary (remote) site to address geographically remote storage and DR requirements. Secure: QTS utilizes a separate, secure gigabit backup network with private VLAN security. Physical security is monitored using a priority badge access system to limit access to the tape libraries, disk arrays, servers, and network infrastructure. From the application, the backup software controls access to the data stored on tape, and access security is limited to QTS staff only. Scalable: QTS backup systems are highly scalable, and capacity can be quickly added as needed.	
SAP	Ariba	Our primary data center is Equinix, in San Jose; CA. Ariba's backup data center is CenturyLink in Sterling, VA. We make many copies of our data to insure no data loss happens: Data is stored in databases on high-availability storage disk-based system in primary datacenter Data is copied as backup to high-availability disk storage in the primary datacenter Data is copied to tape and kept in the primary data center Data is copied to tape and kept in an off-site tape storage facility (Iron Mountain) in Union City Data is replicated to databases high-availability storage disk-based system in the backup datacenter Data is copied as backup to high-availability disk storage in the backup datacenter Data is copied to tape and kept in the backup datacenter

		Data replication to the remote datacenter happens in near-real time. Data is backed up to the backup disks multiple times a day (in each location) Data is written to tape once a day (in each location) These processes and procedures are audited against the ISAE 3402 standard. Our auditor verifies we can restore from these backup methods.
	Fieldglass	All data in the Fieldglass system is stored within our clustered databases. Full backups daily, 15 minute incremental backups, and replication from center to center of backup data continuously.
	Hanna	The backup of SAP systems in HEC is executed on EMC DataDomain deduplication storage. This is done using EMC Networker for backup and administration. The backups on Site A are also replicated to remote Site B.
	SuccessFactors	Data backup is undertaken as follows: storage system snapshots every 24 hours, nightly incremental database backups, and weekly full database backups. These are all standard and provided as part of our hosted service. All backups are stored on disk in the primary and backup data center facilities for 30 days. Database backups are encrypted and stored at a customer's "primary" location, as well as the "alternate" warm-site location for redundancy and disaster recovery purposes. If the customer's primary location is defined as the data center in Amsterdam, NL, then copies of their database would be encrypted and streamed in a secure manner to the data center based in St Leon-Rot, DE, and vice versa. The backup is stored on Storage Area Network systems encrypted with AES-256 bit by encryption appliance. Backups are retained for 30 days. Our Log File Retention Policy is designed to meet or exceed the most stringent industry standards. Archiving of data is the customer's responsibility.
VMware	VMware will provide the following services to participating entities with respect to Data Recovery: •Data protection, such as routine backups, for the vCloud Air infrastructure, including top-layer management and user-management interfaces owned and operated by VMware. •Data and infrastructure restoration for the vCloud Air infrastructure, including top-layer management and user-management interfaces owned and operated by VMware. Participating entities will be responsible for the following services with respect to Data Recovery: •Data protection, such as routine backups, for the data and content accessed or stored on vCloud Air virtual machine's or storage devices, configuration settings, etc. •Data, content, virtual machine and configuration restorations for assets accessed or stored on your vCloud Air account. Data Protection is an optional service that provides secure, image-based backup and recovery capabilities that enable you to protect important virtual machine data and content hosted in your vCloud Air IaaS environment. Through the Data Protection administration interface available in the vCloud Air Console, vApps and their virtual machine members can be selected for policy-based backup and recovery operations. Data Protection feature subscription and activation may be requested via My VMware and is subject to additional service fees based on the amount of backup data capacity. Backup data capacity for the service is measured in front end terabytes (FETB). Once activated, vApps and their virtual machine members may be registered and unregistered with Data Protection features on a self-service basis through the vCloud Air Console. As part of this service, VMware will: •Implement and maintain central service components (backup software appliances, backup and archival storage media and associated network topologies) needed to support Data Protection features. •Perform routine configuration, maintenance and optimization services on behalf of the Data Protection environment and in conformance with industry best practices.	

	•Allocate requisite backup storage based on capacity selections made at the time of subscription enrollment. •Guarantee storage locality per geographical region for all backup data. •Provide necessary Data Protection service reporting as it is requested. Participating entities will be responsible for: •Subscribing to Data Protection as an add-on feature via My VMware and selecting an amount of backup storage capacity commensurate with your requirements. •Creating custom backup protection policies that may include, but are not limited to: affinity settings per VDC, scheduling, and retention periods. •Registering and unregistering individual vApps and their virtual machine members for scheduled backups using Data Protection. •Performing any on-demand backups per vApp and its virtual machine members. •Performing in-place or out-of-place restores per vApp and/or individual virtual machine. •Managing any in-guest recovery tasks, including restore operations at the operating system, file systems and/or any application level. •Managing backup storage capacity and consumption that may include, but is not limited to: activity reporting, ordering additional storage capacity via My VMwareTM and deleting any backup data in inventory to free up space.
FireEye	All backup and restore procedures are in compliance with SOC 2 specifications. Data and server images are backed up digitally and replicated to datacenters in geographically different locations.
VirtueStream	Virtustream performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by State of Utah per landscape and will be documented during the on-boarding process. Virtustream provides OS level files are protected with a File System backup and then protect the application with an integrated solution. Some of the databases would dump to a flat file format and those files would be protected with the standard file system backup.

b. Method of server image backups

CA	APM	N/A
	MAA	Automation tools are used to manage the configuration of MAA internal servers, and can be used for recovery.
	CA Agile	Systems are not backed up as we have determined rebuilding is faster than restoring. We manage systems through Chef and the configuration cookbooks are backed up.
	ASM	Automation tools are used to manage the configuration of ASM internal servers, and can be used for recovery.
Virtru	All images are backed up onto cloud storage on two separate provider systems	
Salesforce	Each server has been allocated a different volume group so it can fail over to its backup server within the instance independently of the others.	
ServiceNow	Please see our response to 8.8.2a	
QTS	Your data storage requirements are growing exponentially and a scalable comprehensive solution for storage and data protection is absolutely necessary in today's marketplace. Implementing and managing this necessary storage infrastructure to meet both your application and compliance requirements can be extremely time consuming and costly. Outsource your storage needs to QTS. With our portfolio of high-performance and cost-effective managed storage services, your data will be secure and guaranteed to be available when you need it. By leveraging market leading hardware and software, coupled with certified processes and personnel, QTS delivers dependable, auditable solutions.	

	Managed SAN (Shared and Dedicated)- a fast, reliable Fibre Channel (FC) and iSCSI SAN attached storage solution that easily scales to meet your business requirements. SAN-to-SAN Replication - provides block level asynchronous replication of your Managed SAN FC service between two of our state-of-the-art data centers for your disaster recovery needs.	
SAP	Ariba	See above
	Fieldglass	Fieldglass does not run server image backups. All systems are designed to be created through a series of templates and scripts.
	Hanna	The defined backup package includes a file system, operating system files, and the database backup. The frequency in which the backup is executed varies for each of the components mentioned above. This depends on the standard HEC service schedules and the service levels agreed on with the customer.
VMware	VMware will provide the following services to participating entities with respect to Data Recovery: •Data protection, such as routine backups, for the vCloud Air infrastructure, including top-layer management and user-management interfaces owned and operated by VMware. •Data and infrastructure restoration for the vCloud Air infrastructure, including top-layer management and user-management interfaces owned and operated by VMware. Participating entities will be responsible for the following services with respect to Data Recovery: •Data protection, such as routine backups, for the data and content accessed or stored on vCloud Air virtual machine's or storage devices, configuration settings, etc. •Data, content, virtual machine and configuration restorations for assets accessed or stored on your vCloud Air account. Data Protection is an optional service that provides secure, image-based backup and recovery capabilities that enable you to protect important virtual machine data and content hosted in your vCloud Air IaaS environment. Through the Data Protection administration interface available in the vCloud Air Console, vApps and their virtual machine members can be selected for policy-based backup and recovery operations. Data Protection feature subscription and activation may be requested via My VMware and is subject to additional service fees based on the amount of backup data capacity. Backup data capacity for the service is measured in front end terabytes (FETB). Once activated, vApps and their virtual machine members may be registered and unregistered with Data Protection features on a self-service basis through the vCloud Air Console. As part of this service, VMware will: •Implement and maintain central service components (backup software appliances, backup and archival storage media and associated network topologies) needed to support Data Protection features. •Perform routine configuration, maintenance and optimization services on behalf of the Data Protection environment and in conformance with industry best practices. •Allocate requisite backup storage based on capacity selections made at the time of subscription enrollment. •Guarantee storage locality per geographical region for all backup data. •Provide necessary Data Protection service reporting as it is requested. Participating entities will be responsible for: •Subscribing to Data Protection as an add-on feature via My VMware and selecting an amount of backup storage capacity commensurate with your requirements. •Creating custom backup protection policies that may include, but are not limited to: affinity settings per VDC, scheduling, and retention periods. •Registering and unregistering individual vApps and their virtual machine members for scheduled backups using Data Protection.	

	•Performing any on-demand backups per vApp and its virtual machine members. •Performing in-place or out-of-place restores per vApp and/or individual virtual machine. •Managing any in-guest recovery tasks, including restore operations at the operating system, file systems and/or any application level. •Managing backup storage capacity and consumption that may include, but is not limited to: activity reporting, ordering additional storage capacity via My VMwareTM and deleting any backup data in inventory to free up space.
FireEye	All backup and restore procedures are in compliance with SOC 2 specifications. Data and server images are backed up digitally and replicated to datacenters in geographically different locations.
VirtueStream	OS level files are protected with a File System backup and then protect the application with an integrated solution where available. Otherwise databases would dump to a flat file format and those files would be protected with the standard file system backup. Additionally, core microVM's are automatically replicated to a secondary datacenter for DR purposes.

c. Digital location of backup storage (secondary storage, tape, etc.)

CA	APM	Backups are securely replicated to an alternate location (within the same geographic location (e.g. N. America))
	MAA	Daily differential and full backups reside in the primacy site with weekly data backups residing offsite.
	CA Agile	Backups are stored in our warm data center.
	ASM	CA has an alternate site approximately 900 miles from our primary site.
Google	Tape	
Virtru	All backup storage is hosten in two separate cloud storage regions	
Salesforce	Backups are performed daily at each data center facility without stopping access to the application. Backup cloning is transmitted over an encrypted network (our MPLS network across all data centers). Tapes never leave our secure data center facilities, unless they are to be retired and destroyed through a secure destruction process.	
ServiceNow	Please see our response to 8.8.2a	
QTS	Managed Tape Rotation and Off-site Storage This service provides off-site storage for data backup, and helps many customers who must store data separately from a primary IT site to comply with various laws and regulations. QTS has contracted Iron Mountain — a nationally recognized leader in off-site data storage services — to move the data storage media (tapes) to and from a secure, off-site location. The service enables data security, integrity, and restoration in the event of an outage. Off-site data storage via tape ensures that a customer's information is securely stored in multiple locations. In the event of an emergency, QTS and Iron Mountain deliver the customer's media back to their IT environment or wherever they request delivery. Secure: QTS staff adheres to storage-industry best practices and security procedures. QTS facilities have earned SSAE16-SOC1 accreditations. All media is maintained in a secure environment and locked in secure media containers during transition from the QTS environment to the off-site storage location. Compliance and Tracking: QTS's partnership with Iron Mountain provides the ability to offer logging and tracking information about the customer's off-site media via the SecureSync Web portal.	
SAP	Ariba	See above

	Fieldglass	Fieldglass houses all backup data vaults within its production data centers. Replicas of the vault are performed continuously across data centers more than 1,000 miles apart.
	SuccessFactors	All data is backed up to the secondary site and can be restored from there in the event of a disaster recovery event at the primary site.
VMware	VMware vCloud Air Data Protection provides backup storage to disk	
FireEye	All backup and restore procedures are in compliance with SOC 2 specifications. Data and server images are backed up digitally and replicated to datacenters in geographically different locations.	
VirtueStream	Virtustream performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by State of Utah per landscape and will be documented during the on-boarding process. Backup data is stored on local enterprise class disk storage systems and can be replicated to systems in a secondary Virtustream datacenter. All of Virtustream backup is disk based solution. Encryption keys are generated at the time of backup application install on the Client VM(s). Encryption keys are at least AES-128 but can be AES-256. Keys are stored on the backup system databases using the encryption key management tool, the data about the keys on the database is in a unreadable format and cannot be decrypted	

d. Alternate data center strategies for primary data centers within the continental United States.

CA	APM	The location where data is stored is generally in the country where the contract is executed.
	MAA	The MAA service is currently available from one data center only.
	CA Agile	We have a hot/warm data configuration with both data centers located within the US but ~1300 miles apart.
	ASM	ASM has a warm standby with near time data replication between the data centers.
Google	Google does not use the N+1 data center assignment due to the risk of cascading failures. Google's infrastructure makes a dynamic decision for each unique login session which data center is the closest, most highly available data center and which data centers will be used as secondary and tertiary. This assignment would shift for that session throughout the day based on availability and is done completely seamless to the end user.	
Virtru	We utilize multiple availability zones in AWS, and backup all data stored in our database to separate datacenters	
Salesforce	Customer Data for customers in Salesforce's Government Cloud is stored in two of our U.S. data center locations. The Salesforce service performs near real-time replication at each data center and annual disaster recovery tests for the service verify the projected recovery times and data replication between the production data center and the disaster recovery center. The disaster recovery site is a 100% replica of the primary production site of capacity (host, network, storage, data). Data is transmitted between the primary and disaster recovery data centers across encrypted links. Additionally, back-ups of data are performed and data is retained on backups at the geographically separated disaster recovery data center location.	
ServiceNow	Please see our response to 8.8.2a	
QTS	The QTS cloud alternate storage sites are located at the following data centers: Richmond, VA, Atlanta, GA, and Suwanee, GA. The entire QTS cloud is a unified standalone Active cloud architecture and is backed up in both Atlanta and Richmond to include: Customer data in the Service Delivery Hypervisor Cluster, and; Cloud Hypervisor Management Infrastructure and Configuration backups.	

	The QTS cloud Security documentation is backed up in alternate site located Suwanee, GA to include: Software/operating Systems, Configuration Data and Security Documentation QTS cloud Management Infrastructure and Configuration Data: Richmond, VA: The Richmond Cloud Management Layer (Cloud Hypervisor Management Cluster) and Customer data in the Service Delivery Hypervisor Cluster, and Configuration data is backed and staged locally in Richmond on the management layer then backed up across the Site-to-Site Management VPN to Atlanta, GA. This process is separate and independent of the Customers Service Delivery Layer. Atlanta, GA: The Atlanta Cloud Management Layer (Cloud Hypervisor Management Cluster) and Configuration data is backed and staged locally in Atlanta on the management layer then backed up across the Site-to-Site Management VPN to Richmond, VA. This process is separate and independent of the Customers Service Delivery Layer. This process maintains both local and remote management layer data and configuration backup for both locations. Suwanee, GA: software/operating systems, configuration data and security documentation at Rocstor Rocsecure Amphibious X7s with Secure-Encrypted Two-Factor Authentication, Utilizing AES-256 CBC Real-Time Hardware Encryption, with NIST and FIPS 140-2 Certified Cryptographic Modules, in a firerated safe located at Suwanee, GA.	
SAP	Ariba	We have a warm site for failover. Equinix (Our primary data center) is located in San Jose, California and our disaster recovery site is located at CenturyLink Data Center in Sterling, Virginia. The act of failing over from the main data center to the recovery site data center has a design goal recovery time objective (RTO) of four hours. The design goal Recovery Point Objective (RPO) is five minutes. In the event of a fail-over to the disaster recovery site location, all URLs that customers use to reach the San Jose data center will continue to work. We will notify customers via their email addresses in the event of unplanned downtime. Internally, we use a documented system recovery plan that outlines the approach and steps for recovering the applications. The document defines roles and responsibilities in the event of disaster: Local staff maintains the hardware remotely We maintain the application software Processes are in place to keep database and fileservers in sync between primary and backup data centers In the event of a catastrophe, we will declare the primary data center ""down"" and our local staff will follow a script to start the applications at the remote data center We test power outage backup scenarios and the Disaster Recovery Plan on a periodic basis.
	Fieldglass	Please see the answer to Question 8.8.2A. above. Fieldglass' backup data center is located in San Jose, CA.
	Hanna	The backup of SAP systems in HEC is executed on EMC DataDomain deduplication storage. This is done using EMC Networker for backup and administration. The backups on Site A are also replicated to remote Site B. For example, site A &B may be Santa Clara, CA and Sterling, VA, respectively.
	Hybris	In the case of catastrophic failure to your primary production data center, we offer anywhere from best efforts to enhanced DR solutions. Enhanced DR

		options translates to either RTO of 8 hours and RPO of 1 hour for a warm standby solution, or RTO of 30 minutes to RPO of 30 minutes for a hot-site. Customers have 3 choices in DR sites: • as part of our base offering, best effort DR, we would bring your site back up in an alternate datacenter which is a minimum of 500 miles away from the primary datacenter. We would actually push your project server images to the alternate datacenter, but we would still need to set up your various interfaces, 3rd party services, etc, which could day a few days. • 2nd would be to have your DR site managed by hybris Managed Services. • 3rd would be to use your own DC as a DR site, We would need to set up a technical call with our combined teams to synch up on the replication strategies. • Our DR services utilizes VMware Site Recovery Manager with storage-based replication. • For enhanced DR, we would include one annual DR test, but more can be added if required. It also includes a customer specific DR and Business Continuity plan.
	SuccessFactors	Each client has a designated primary and backup data center which is geographically separated as well as existing on different power and telecommunications grids.
VMware	Customers can purchase Rackware to provide geographical HA and COOP, but this service is not provided as a core capability of vCA or vCGS. VMware AirWatch AirWatch backs up the production environment from the primary US data center to the secondary US data center. Due to FOIA restrictions and the competitive nature of the EMM landscape, we cannot provide additional backup scheduling or image security procedures.	
FireEye	All backup and restore procedures are in compliance with SOC 2 specifications. Data and server images are backed up digitally and replicated to datacenters in geographically different locations.	
VirtueStream	State of Utah can choose any of our FedRAMP Data Centers to host their applications and the DR location. For illustrative purposes, we have assumed the primary data center will be USDC02 and DR data center would be USDC01. The State of Utah solution has been designed with all workloads running in our San Francisco (USDC02) data center. In the unlikely event of a disaster at the USDC02 facility, State of Utah's production services will be brought back online in the secondary data center located in Northern Virginia (USDC01). The target Recovery Point Objective (RPO) is 30 minutes for virtual machines with a 2 hour Recovery Time Objective (RTO). All production workloads in the primary node will have reserved compute capacity in the secondary node when deployed using Enterprise Reserve µVMs and replicated storage. All virtual machine disaster recovery services are based on storage replication. The primary and secondary data centers are interconnected by diverse private 10 Gbps Sonet rings from separate Tier 1 providers – AboveNet and Level 3. Data is replicated asynchronously and continuously between the two data centers. Virtustream also performs backups on a nightly basis and replicated offsite for further protection. The retention policies are determined by State of Utah per landscape and will be documented during the on-boarding process.	

8.9 Data Protection

8.9.1 Specify standard encryption technologies and options to protect sensitive data, depending on the particular service model that you intend to provide under this Master Agreement, while in transit or at rest.

CA	APM	All data is encrypted via TLS Mutual Auth during transit

	MAA	HTTPS/TLS encrypts the data in-transit. Sensitive data rest is encrypted using native encryption of SQL and NoSQL vendors.
	CA Agile	All data in transit is encrypted - we support TLS 1+. For data at rest we have both database and disk level encryption. DB encryption utilizes Oracle TDE w/ AES-256.
	ASM	All data transmitted between data centers is encrypted in-transit. HTTPS/TLS is used by the ASM dashboard and API.
Google	All connections from customer end point devices to Google's Front End Servers are encrypted with enforced HTTPS sessions using Forward Secrecy. Google websites and properties use robust public key technologies: 2048-bit RSA or P-256 ECDSA SSL certificates issued by a trusted authority (currently the Google Internet Authority G2). All data in transit between Google's Data Centers traverses across Google's private fiber network using a customized, proprietary encryption technology. Google hard drives leverage technologies like FDE (full disk encryption) and drive locking, to protect data at rest. These methods of encryption are fully managed by Google and Google's Key Management Servers based on 128-bit or stronger Advanced Encryption Standard (AES). Encryption Keys and Ciphers Supported by Google Protocols TLS 1.2 TLS 1.1 TLS 1.0 SSL 3.04 QUIC Cipher suites ECDHE_RSA with AES ECDHE_RSA with 3DES ECDHE_ECDSA RSA with AES RSA with 3DES Signing keys RSA 2048 ECDSA P-256 Hash functions SHA384 SHA256 SHA1 MD5	
AODocs	All data in transit is encrypted via SSL/TLS Vendor interfaces are available only via HTTPS Email is exchanged via SMTP/TLS All AODocs data are stored in Google AppEngine.	
Virtru	AES-256 in CBC mode, TLS 1.2 ECDHE	
Salesforce	Encryption Capabilities Salesforce has many customers that are subject to laws pertaining to the processing of personally identifiable information (PII) or personal data. Salesforce offers its customers a broad spectrum of functionalities and customer-controlled security features that its customers may implement in their	

	respective uses of the Salesforce services. Salesforce believes that these provide its customers the flexibility to comply with laws with stringent privacy and security requirements. Data In Motion All transmissions between the user and the Salesforce Services are TLS encrypted with a 2048-bit Public Key. The Services use International/Global Step Up TLS certificates, with AES 256-bit encryption by default. Data At Rest Salesforce includes a feature to encrypt custom text fields (ECF): The fields can be masked appropriately for specific data types (i.e., credit card number, Social Security Number, National Insurance Number, Social Insurance Number). Access to read the masked parts of the fields is limited by the ""View Encrypted Data"" permission, which is not enabled by default. Customers can manage their encryption key based on their organization's security needs and regulatory requirements. Encrypted fields are encrypted with 128-bit keys and use the AES (Advanced Encryption Standard) algorithm. Additional Salesforce Encryption Capabilities Apex Code extends the powerful and proven success of the Force.com platform by introducing the ability to write code that runs on Salesforce servers. This language makes possible the development of a new class of application and features deployed entirely on demand. Using Apex, your Agency can create user interface classes that utilize the Apex crypto class to encrypt field level data up to AES 256-bit encryption. Third Party Encryption Solutions (Additional License Option) Should additional encryption be required, third party solutions such as CipherCloud, Skyhigh, and PerspecSys are available on the Salesforce AppExchange. These solutions offer data loss prevention, user activity and monitoring, malware protection, as well as data protection with encryption and tokenization. Data can be encrypted and masked at rest, keys managed and stored in Salesforce, and compliance controls to prevent unauthorized access to data and keys.
ServiceNow	ServiceNow makes use of encryption for both data in transit and data at rest. ServiceNow provides optional capabilities with regard to the encryption of data at rest within the system, which customers can apply at their own discretion. Encryption in Transit ServiceNow customers access their instances over the Internet using forced Transport Layer Security (TLS) encryption (AES128/256) for all user access. The level of encryption is based on the browser and must be configured by the customer as ServiceNow does not modify any browser settings. All attempts to access ServiceNow over HTTP are redirected to HTTPS. Integration Encryption For integrations such as LDAP and Web Services, ServiceNow provides customers with the ability to encrypt traffic. LDAP can be configured to run over SSL, this requires customers to provide a certificate for the specific LDAP server. Certificates may also be stored within an instance to allow encrypted transmission for Web Services integrations. FTPS and SCP can be used as file transfer methods to securely transfer files to ServiceNow. Email Encryption Customers may configure their instance to generate emails to their users from the instance. ServiceNow provides the capability to receive email over TLS. Customers are able to configure their

	email system to send email to ServiceNow over TLS and ServiceNow will receive that email over TLS. Encryption at Rest ServiceNow can provide three types of encryption for data at rest that are implemented by the customer or by customer request in the case of edge encryption and dedicated hardware. •Column encryption of customer added fields and attachments: Provides data encryption using AES128/256 or 3DES symmetric key encryption. The customer provides the keys for this encryption. Data stored in these fields cannot be searched or reported on and this does not support out of the box fields. •Edge Encryption Proxy: With optional additional cost Edge Encryption, the customers create and control their encryption keys within their own network. Edge Encryption includes a proxy application that resides in a customer's network. This encrypts data before it is sent (also encrypted in transit) from the customer's environment to the ServiceNow instance. The data always remains encrypted whilst stored in the instance and the data along with the keys and the encryption configuration is never accessible by ServiceNow. Requests for encrypted data must also be made through the proxy application and is therefore decrypted only within the customer's network before being sent to their end users client browser. Please note that data encrypted with Edge encryption cannot be used by back-end scripts or processes and searching and reporting behavior is also modified through its use. •Full disk encryption: Provides via self-encrypting hard drives with AES256 bit encryption. This encryption capability is only available through the purchase of dedicated ServiceNow hardware at an additional cost. This delivers "at-rest" protection only and is focused solely on preventing data exposure through the loss or theft of hard disks holding customer data. Wherever possible, ServiceNow leverages existing FIPS 140-2 certified technologies.	
Docusign	Secure, private SSL 256 bit viewing session Anti-tampering controls Signature verification of signing events Unalterable, systematic capture of signing data Digital certificate technology Customer configurable data retention program	
SAP	Ariba	We enforce minimum AES 128-bit encryption using Transport Layer Security (TLS) for all sessions. We encrypt only PCI-DSS data in the database where appropriate and in support of PCI-DSS compliance. All backup media is encrypted using AES 256-bit cipher prior to transporting to off-site storage
	Fieldglass	Our application provides a high level of application-level security through a combination of encryption, page-level access checking, document envelopes, and activity logging. Application security is handled through a combination of programming checks, application server configuration, and database server configuration. Fieldglass uses 2048-bit SSL (HTTPS) encryption for all data transmissions over the public Internet, including data shared between the product and end users and data shared between the product and back-end systems. Data is decrypted on the internal VLAN to allow IDS monitoring. Passwords are hashed using a one-way hash based on the SHA-256 encryption algorithm. The hash value is saved within the database; not the password. The base Fieldglass application does not require data that would require breach notifications if compromised. While customers should not store sensitive personal data, custom fields may be defined by the customer that can be encrypted with AES-256 to capture any pertinent and permissible data points. These fields can also be optionally masked from view while entering and viewing the fields in the application.

	Hanna	Initial encrypted data load - physical encrypted data transfer possible Encrypted connection to HEC DC - SAP solutions support various VPN-device vendors and specifications that can be used to setup a secure and encrypted tunnel between cloud solutions from SAP on the customer network segment and the customer site. Optional Data at Rest encryption - HANA encryption at Rest activated during system build upon request. Moreover data at rest is properly protected against unauthorized access, these controls include •Physical security controls in SAP HEC Datacenters in place •Physical separation of "online" storage and backup (physically separated DC sections) •Strict User and Access Management (segregation of duties) •Authorization Management according to the need to know principle also for administrative accounts, e.g. DBAs have limited authorizations to perform DB operation only •Security Logging and Security Monitoring for critical activities / access Optional encryption in transit can be configured on customer request which requires a different subset of DC's from delivery perspective.
	Hybris	Encryption is provided through SSL connectivity at the web application layer as well as VPN secure encrypted tunnel for back-office integration connectivity. Further encryption capabilities are available through the hybris Advanced Security Module (optional).
	SuccessFactors	All data in the system is treated as highly sensitive information. The application and infrastructure offers Strong Encryption, Encryption in Transit and Encryption at Rest, including the following (some of these are options that are not included in the base services): Transport Layer Security (TLS) technology, consisting of a public key and a private key, to protect sensitive information. The public key is used to encrypt information and the private key is used to decipher it. When a Web browser points to a secured domain, a handshake authenticates the server (website) and the client (browser). An encryption method is established with a unique session key. Customers may then begin a secure session that facilitates message privacy and integrity. Hitachi SAN storage arrays provide a reliable safe, secure data storage environment. We use AES-256 bit encryption to secure data at the block level of our storage systems. Backups are performed ""disk to disk"". Data is transported over 3DES VPN and stored on encrypted disk using Data Domain replication technology
VMware	VMWare IaaS Services Data in transit will be encrypted based upon the customers selected method of transport (SSL or IPSEC VPN). Data at rest encryption is the responsibility of the customer. By example HyTrust is an endpoint encryption choice for many vCloud Air customers. VMWare AirWatch AirWatch leverages strong, non-proprietary encryption algorithms to protect applicable data at rest and in transit. Due to FOIA restrictions and the competitive nature of the EMM landscape, we cannot provide specific encryption algorithms and protocols.	
FireEye	Each of the FireEye offered solutions have their own implementations and practices concerning encryption:	

	1.Email Threat Prevention (ETP) ETP offers TLS encryption support for data in transmission. ETP only stores email found to contain malware or malicious content and does not encrypt this data. 2.Mobile Threat Prevention (MTP) All data in transit is protected using standard TLS encryption. The database itself is not encrypted. However, all systems are under strict security and access control rules, in compliant with SOC 2 regulations. 3.Threat Analytics Platform (TAP) All data in-transit between a customer environment and TAP instance in Amazon AWS is encrypted with a 256-bit Twofish key. No customer data is stored on disk, however data stores leverage Amazon AWS S3 encryption settings. 4.FireEye as a Service (FaaS CV) FireEye appliance communications, and FireEye as a Service (FaaS) non-person entity (NPE) secured inter-process communications employs industry standard HTTPS encrypted web interfaces, and multifactor SSH management access for the end-to-end protection of sensitive customer data. In addition, FaaS communicates with FireEye appliances with additional layers of protected symmetric key exchanges protecting and establishing encrypted channels for inter-device information.
VirtueStream	Encryption keys are generated at the time of backup application install on the Client VM(s). Encryption keys are at least AES-128 but can be AES-256. Keys are stored on the backup system databases using the encryption key management tool. The data about the keys on the database is in an unreadable format and cannot be decrypted.

8.9.2 Describe whether or not it is willing to sign relevant and applicable Business Associate Agreement or any other agreement that may be necessary to protect data with a Purchasing Entity.

Carahsoft would be willing to sign Business Associate Agreements or similar agreements that are set forth with a purpose of protecting customer data.

8.9.3 Offeror must describe how it will only use data for purposes defined in the Master Agreement, participating addendum, or related service level agreement. Offeror shall not use the government data or government related data for any other purpose including but not limited to data mining. Offeror or its subcontractors shall not resell nor otherwise redistribute information gained from its access to the data received as a result of this RFP.

Agreed and understood. Carahsoft and its' subcontractors will not use any government data for purposes other than those outlined within the frameworks of this contract.

8.10 Service Level Agreements

8.10.1 Offeror must describe whether your sample Service Level Agreement is negotiable. If not describe how it benefits purchasing entity's not to negotiate your Service Level Agreement.

CA	APM	The target availability SLA of 99.8% is standard and not negotiable
	MAA	The target availability SLA of 99.8% is standard and not negotiable
	CA Agile	The target availability SLA of 99.8% is standard and not negotiable
	ASM	The target availability SLA of 99.8% is standard and not negotiable
Google	Google maintains a single SLA for all customers.	
AODocs	AODocs maintains a single SLA for all customers.	
Virtru	Agreement can be negotiated for certain large customers.	

Salesforce	Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately. The persistence layer underlying Salesforce Platform is proven database technology that powers all of Salesforce's products today, serving more than 150,000 organizations and over 4 billion transactions per day with an average request response time of less than .25 seconds all with an average up time of 99.9+ percent. Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Live and historical statistics on the Salesforce system performance are publicly published at http://trust.salesforce.com/trust/status. Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (http://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers' trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance.	
ServiceNow	ServiceNow's SLA is not negotiable. ServiceNow delivers the same level of world-class support to all customers as described in the "Subscription Service Guide" included with this response. ServiceNow's homogeneous private cloud environment where all applications are on a single platform offers ServiceNow a competitive advantage in being able to concentrate its efforts to make the customer's user experience the best possible. The ServiceNow environment is a private cloud, fully owned and operated by ServiceNow. ServiceNow's experience & understanding of its private cloud and the benefits provided by a consistent infrastructure and standardized processes allow it to provide a high level of security, availability, and performance in a cost effective and reliable manner.	
Docusign	Yes SLA's can be modified per contractual agreement.	
SAP	Ariba	Our SLAs are not negotiable. As mentioned above, the SAP Ariba Cloud Service Level Agreement includes a 99.5% uptime.
	Fieldglass	Our SLA is designed to (i) meet the expectations of our customers and (ii) fit with our operational protocols and capabilities. Because of this our ability to make significant changes to the SLA is limited. However, we are always willing to work with a customer to try and determine how our SLA can address a particular business.
	Hanna	Our SLAs are not negotiable for Support. Under our SLA, System Availability is 99.5% during each month for productive systems. Customers may claim a credit of 2% of Monthly Subscription Fees for each 1% below SLA (not to exceed 100% of Monthly Subscription Fees). This credit may be applied to a future invoice relating to Cloud Service that did not meet the System Availability SLA.
	Hybris	Our SLAs are not negotiable for Support. Under our SLA, System Availability is 99.5% during each month for productive systems. Customers may claim a credit of 2% of Monthly Subscription Fees for each 1% below SLA (not to exceed 100% of Monthly Subscription Fees). This credit may be applied to a

		future invoice relating to Cloud Service that did not meet the System Availability SLA.
	SuccessFactors	Our SLAs are not negotiable for Support. Under our SLA, System Availability is 99.5% during each month for productive systems. Customers may claim a credit of 2% of Monthly Subscription Fees for each 1% below SLA (not to exceed 100% of Monthly Subscription Fees). This credit may be applied to a future invoice relating to Cloud Service that did not meet the System Availability SLA.
VMware	VMware's SLAs are specific to the product or service, and are subject to the product's Terms of Service (which are also provided). The SLA is specific to the product rather than to the customer, to define the expected availability and recourse should the product not meet the stated availability levels. VMware's existing customers include Federal, State and Local government customers as well as commercial customers, who successfully utilize our products in accordance with the current SLA and Terms of Service and their applicable, mandatory laws and regulations. Accordingly, VMware is confident that the existing SLA meets the state and local government requirements, as it is being utilized currently. VMware IaaS Services To best work with our customers and improve our terms in alignment with market requirements, VMware is willing to review the terms of its SLA during negotiations of the Participating Addendum to identify how the existing SLA meets the state's applicable and mandatory laws and regulations. If it becomes apparent to the parties that it is necessary to revise VMware's SLA to comply with the state's applicable and mandatory laws, VMware will enter into discussions about how to best address these requirements Vmware SaaS Services VMware AirWatch AirWatch Service Level Agreements are non-negotiable. AirWatch has a guaranteed uptime SLA of 99.9%. Please refer to the AirWatch Hosted Services Policy for additional information. VMware AirWatch acknowledges that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the mandatory minimum requirements and technical specifications of the RFP.	
FireEye	SLAs are negotiable.	
VirtueStream	Virtustream's Service Level Agreement is generally not negotiable. Our SLAs are one of the strictest in the market place. To change the SLA would mean either changing the design or create operational disruption and higher cost by engaging in non-standard processes and practices. For example, Virtustream's SLA for Tier 1 storage is 10 ms latency. For Virtustream to change this latency means changing the design for Tier 1 storage.	

8.10.2 Offeror, as part of its proposal, must provide a sample of its Service Level Agreement, which should define the performance and other operating parameters within which the infrastructure must operate to meet IT System and Purchasing Entity's requirements.

Below is a sample of Virtustream's Service Level Agreement:

SERVICE LEVEL FRAMEWORK
The service levels ("Service Levels") applicable to the Services specified in Sections 1 and 2 are set forth in Schedule B to this SD ("Service Levels for Cloud Platform Services"). The framework that governs all Service Levels is set forth in this Section.
Commencement of Service Levels
Commencing thirty (30) days from the Service Start Date (as set forth in the applicable Order Form), Virtustream's performance of the Services will meet each applicable Service Level. If Virtustream's performance of the Services

does not meet the applicable Service Level, then Virtustream will use commercially reasonable efforts to restore its performance to meet such Service Level.

Service Level Reports

Service Levels will be calculated and measured monthly by Virtustream on a calendar month basis and reported each month for the previous month. The reports will be provided to Customer by the tenth (10th) working day of the month following that to which such report relates, commencing on the second (2nd) month following the Service Start Date and each month thereafter. The monthly service level report will contain at least the following items: (i) Uptime statistics for the month concerned; (ii) an analysis of reported incidents over the previous month, broken down by type for discussion; (iii) action plans for items giving rise to concern; (iv) comments and observations on any issues arising from Virtustream's performance monitoring activities; (v) recommendations on service delivery strategies to maintain or enhance the service level; and (vi) review of general business requirements ("Service Level Report").

Cloud Platform Services (CPS) has its own specific service levels as described in this document. Cloud Cover Services (CCS) has service levels that pertain to the CCS offerings and are reported separately. Not all Virtustream customers have CCS but all Virtustream customers use CPS.

Service Level Review Meetings

Monthly Service Level review meetings will be conducted by Virtustream with Customer where the monthly Service Level report specified above will be discussed. If any of the Service Levels measured over the previous calendar month period is not achieved in that month, then Virtustream will include the steps taken to rectify the problem in the next monthly Service Level Report. In addition, the issue shall be an agenda topic for discussion at the next monthly service review meeting. Additionally, after restoring service or otherwise resolving any immediate problem as specified in this SD, if Virtustream fails to provide Services in accordance with the Service Levels, Virtustream shall:

a.Promptly investigate and report on the causes of such problem;

b.Provide a Root Cause Analysis of such failure as soon as practical after such failure or at Customer's request;

c.Correct such problem that is Virtustream's fault or responsibility, as soon as reasonably practicable and coordinate the correction of such problem if Virtustream does not have responsibility for the cause of such problem.

d.Advise Customer of the status of remedial efforts being undertaken with respect to such problem;

e.Demonstrate to Customer's reasonable satisfaction that the causes of such problem (that is Virtustream's fault or responsibility) have been or shall be corrected on a permanent basis; and

f.Take corrective actions to prevent any recurrence of such problem (that is Virtustream's fault or responsibility).

Root Cause Analysis

Promptly following Virtustream's failure to meet a Service Level, Virtustream will perform a root cause analysis to determine the reason for that failure. Upon Virtustream's determination of the cause of such failure, it will provide to Customer a preliminary report citing the cause of such failure. If Virtustream determines that the failure was due to Virtustream, an additional report will be provided that details the root causes of the failure, and which details any measures that should be taken to minimize the possibility that such failures will re-occur. Virtustream will correct the problem and use reasonable commercial efforts to minimize the re-occurrence of such failures.

Service Level Exceptions

Virtustream shall not be liable for any failure to meet the Service Levels, to the extent such failure was caused by one or more of the following:

a.A failure of Customer or any of its employees, agents or contractors (including any of Customer's third party service providers) to perform any of its responsibilities under this SD;

b.Any act or omission of Customer or any of its employees, agents or contractors (including Customer's third party service providers or other third parties acting on behalf of Customer);

c.Any hardware, software or other product of a third-party or Customer equipment;

d.Any failure of Customer to secure the proper access rights or maintenance and support services with respect to any component of the Services (e.g., hardware, software, network, maintenance) for which Virtustream does not bear operational responsibility;

e.Downtimes resulting from a Virtustream's scheduled maintenance windows;

f.Customer's reprioritization of the tasks to be performed by Virtustream where such reprioritization causes Virtustream to miss a Service Level;

g.Viruses; provided that the infected Virtustream-provided system had virus protection for which the virus protection software updates were up to date;

h.An election by Customer to purchase a base commitment that is not sufficient to run Customer's system (e.g., If a customer elects to size a µVM pool that is insufficient to run the designated workload);
i.Issues occurring outside of standard working hours (as defined for business level customers) — for which the Service Level Objectives (SLOs) do not apply;
j.Cloud Cover Services (CCS) offerings — for which the Service Level Objectives (SLOs) do not apply;
k.Resolution delays due to lack of client response and/or Customer provided credential based information;
l.Priority levels not agreed upon by both customer and supplier;
m.Claims of performance degradation not substantiated through Customer provided diagnostic testing results.

8.11 Data Disposal

Specify your data disposal procedures and policies and destruction confirmation process.

The disposal of data will vary based on the type of service that is being provided to the Purchasing Entity by Salesforce. As an example, please see Salesforce response for disposal of government data: Data Disposal and Destruction
In the event of termination of the Salesforce service, requests by your Agency made within 30 days after the effective date of termination or expiration of the Subscription Agreement, Salesforce will make your data available to you for export or download. Once the export has been completed, an email will be sent to you containing a link where you can download a .zip file that contains multiple .csv (spreadsheets) files, each representing your Salesforce objects. Your data on disk is flagged within the database and set to inactive status or what can be referred to as a ""soft delete."" This data is no longer available or accessible to the application but is backed up in the full database backup process. The data remains in this state for 180 days; this is done in the event that the customer decides to resume services or needs the data for a legal reason. At 180 days, the data is marked for deletion (""hard delete"") and will be deleted after 30 more days. Once this ""hard delete"" is executed the customer data is physically deleted and non-recoverable from the database. Following the purge, the data will remain on backup for an additional 90 days prior to being overwritten and unrecoverable.

Media Sanitization
Salesforce has an established process for sanitizing media consistent with industry guidelines and consistent with NIST SP 800-88 Guidelines for Media Sanitization [MP-6].

8.12 Performance Measures and Reporting

8.12.1 Describe your ability to guarantee reliability and uptime greater than 99.5%. Additional points will be awarded for 99.9% or greater availability.

CA	APM	CA SaaS production environments have an SLA at 99.8% uptime calculated arrear monthly. 1hr response for P1 issues.
	MAA	CA MAA SaaS production environments have an SLA at 99.8% uptime calculated arrear monthly. 1hr response for P1 issues.
	CA Agile	For Rally SaaS Unlimited Edition customers, our goal is to provide 99.9% up-time during each calendar quarter. If in any calendar quarter an up-time of 99.5% is not met and our customers were negatively impacted (for example, were unable to login to Rally), we will provide a service credit equal to one month of fees for use of the Rally Service.
	ASM	CA SaaS production environments have an SLA at 99.8% uptime calculated arrear monthly. 1hr response for P1 issues.

Google	Google Apps services will be operational and available to the customer at least 99.9% of the time in any calendar month. If Google does not meet the Google Apps SLA, the customer will be eligible to receive service credits.	
AODocs	Altirnao agrees to use commercially reasonable efforts to meet or exceed the Availability Service Level. The Availability Service Level means the Service is available for use by Users for not less than 99.5% of the time excluding the Exclusion Events (as defined below).	
Virtru	Virtru provides the same SLA as Gmail	
Salesforce	Salesforce has maintained high levels of availability across all Salesforce instances since inception. As the only on-demand vendor to provide daily service-quality data on a public Web site (http://trust.salesforce.com), Salesforce proves that we are the leader in availability. And by making its track record completely transparent, Salesforce proves we are worthy of our customers' trust. To ensure maximum uptime and continuous availability, Salesforce provides the best redundant data protection and most advanced facilities protection available, along with a complete data recovery plan—all without affecting performance. Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. The persistence layer underlying Salesforce Platform is proven database technology that powers all of Salesforce's products today, serving more than 150,000 organizations and over 4 billion transactions per day with an average request response time of less than .25 seconds all with an average up time of 99.9+ percent. Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately.	
ServiceNow	ServiceNow's Availablity SLA Is 99.8%, excluding Excused Downtime of up to two hours per month. This is achievable through the use of the Advanced High Availability (AHA) architecture described in 8.8.1 that provides failover capabilities for maintenance and service disruptions to minimize downtime.	
Docusign	DocuSign offers carrier class bank grade, "always on" availability. This means DocuSign has eliminated monthly maintenance (taking 0 minutes of planned downtime per year). We are a multi-year 99.99% operation. Please view the DocuSign Trust site (trust.docusign.com) for additional information.	
QTS	TIA 942 requirements for the design, construction, and management of Tier III facilities is the design basis for all QTS data centers. Using best-of-breed technologies, QTS's highly trained, certified data center professionals tailor efficient and reliable solutions to meet individual customer requirements. Primary commercial power is delivered to facilities through diverse, redundant paths to eliminate single points of failure between the nearest electrical substation (usually on-site) and each piece of customer IT equipment. QTS allows users to inspect the engineering drawings to validate that truly redundant N+1 architectures are in place and that the 99.999% uptime guarantee is supported by sound engineering and operational policies. Meaningful Service Level Agreements are backed by financial penalties spelled out in tailored Master Service Agreements with each customer.	
SAP	Ariba	Our data centers have 99.99% uptime. Our application maintains a 99.% official SLA with the last 12 months seeing 99.98% uptime.
	Fieldglass	For customers hosted in US data centers, we commit to a 99% availability standard. For customers who choose to be hosted in EU data centers, our availability standard is 96.7%. If we fail to meet the availability standard, the

		customer may be entitled to receive a credit equal to two percent (2%) of its transaction fees for the service for that month for each one percent (1%) (or portion thereof) by which we fail to achieve such level, up to one hundred percent (100%) of the fees for such month.
	Hanna	The SAP HEC offers a 99.5% uptime availability SLA for production (PRD) instances and a 95% uptime availability for quality assurance (QAS) and development (DEV) instances. This means that after taking in to account the monthly maintenance window, the TOTAL solution will be available 99.5% of the time - not that we expect it, but this equates to about 3 hours of unscheduled downtime per month. The concept of "total solution" is important because the HEC provides Holistic Solution Availability - our single SLA covers the FULL SOLUTION STACK which means it covers the Infrastructure, Operating System, local DB, the HANA in-Memory DB, and the Application layers. We do not offer individual SLAs on individual layers because if one layer fails, the entire solution is down
	Hybris	The environment is completely redundant and based on a high availability architecture. The hybris private cloud is based on VMWare virtualization and is fully load-balanced. Customer systems reside on a redundant server infrastructure ensuring that if one server (or part of the server infrastructure) fails, a backup is in place to ensure that systems remain operational. The infrastructure is load-balanced ensuring high availability of the system during peak usage periods. The load-balancing allows the systems to support large volumes of simultaneous users balancing the load of activity across multiple servers ensuring peak performance of all systems. Redundancy of Infrastructure Components: • Multihome connectivity to the Internet backbone. Multiple connections to the internet, allows optimizing the best route as well as redundancy. • At an individual component level, all devices have dual physical power connections to protect against any individual power supply failure • Redundant Firewalls • Redundant Routers, • Redundant Load balancers • Virtualized Application and Web servers • Clustered Database - active active cluster mode for enhanced redundancy • High performance SAN storage- from Netapp, with built in redundancy at the disk level (NetApp proprietary RAID technology, similar to a RAID 5) • The data centers provide diverse power (Uninterruptible Power Supply), backup generators and air conditioning systems required to ensure equipment remain online with optimal performance 24/7/365. • SLA: contractually we provide a guarantee on the performance of your application at 99.9% availability.
	SuccessFactors	We contractually guarantee a minimum of 99.5% system uptime, with the exception of regularly scheduled and emergency maintenance.

VMware	VMware's SLAs for vCloud Air. Our Availability Commitment ranges from 99.99% - 99.95 based on the Class of Service. The SLAs are subject to the terms of the applicable Terms of Service for the VMware vCloud Air Service Offerings. Dedicated Cloud 99.99%, Virtual Private Cloud 99.95%, Data Protection 99.95%, Disaster Recovery 99.95%, Virtual Private Cloud On-Demand 99.95% Availability Commitment. IaaS Object Storage: Object Storage powered by Google CLoud Platform (standard) 99.9%, Object Storage powered by Google (durable reduced availability) 99.0% and Object Storage (nearline storage) 99%. vCloud Government Service Dedicated Cloud 99.95% and Virtual Private Cloud 99.9% Availability Commitment.
FireEye	FireEye undertakes all reasonable efforts to ensure the availability for 99.9% of the time during each calendar month. In the event the solution does not meet the monthly service availability, FireEye will provide a credit as outlined in the SLA.
VirtueStream	Virtustream solution for VM workload includes the uptime of 99.99%.

8.12.2 Provide your standard uptime service and related Service Level Agreement (SLA) criteria.

CA	APM	Uptime SLA target is 99.8% CA runs test scripts using application monitoring tools on the Production system to verify that the CA SaaS service is available. Test scripts are run approximately once every ten (10) minutes, twenty-four (24) hours per day, seven days per week, throughout the contracted term of the service.
	MAA	Uptime SLA target is 99.8% CA runs test scripts using application monitoring tools on the Production system to verify that the CA SaaS service is available. Test scripts are run approximately once every ten (10) minutes, twenty-four (24) hours per day, seven days per week, throughout the contracted term of the service.
	CA Agile	See above.
	ASM	Uptime SLA target is 99.8% CA runs test scripts using application monitoring tools on the Production system to verify that the CA SaaS service is available. Test scripts are run approximately once every ten (10) minutes, twenty-four (24) hours per day, seven days per week, throughout the contracted term of the service.
Google	Google Cloud Platform SLA: Google's Cloud platform has SLAs ranging from 99.9 - 99.95% uptime.	
Salesforce	Please see response to 8.12.1 above. Salesforce does not typically offer Service Level Agreements as part of the base service offering. Our approach is to offer a service with high availability and fast resolution of problems. If a customer requires an SLA it will be negotiated separately. Salesforce uses commercially reasonable efforts to make its on-demand services available to its customers 24/7, except for planned downtime, for which Salesforce gives customers prior notice, and force majeure events. Excellent availability statistics are critical to Salesforce's customers' success and to the success of Salesforce as a company. Live and historical statistics on the Salesforce system performance are publicly published.	
ServiceNow	DEFINITIONS (a) "Available" means that the Subscription Service can be accessed by authorized users.	

	(b) "Excused Downtime" means: (i) Maintenance Time of up to two (2) hours per month; and (ii) any time the Subscription Service is not Available due to circumstances beyond ServiceNow's control, including without limitation modifications of the Subscription Service by any person other than ServiceNow or a person acting at ServiceNow's direction, a Force Majeure Event, general Internet outages, failure of Customer's infrastructure or connectivity (including without limitation, direct connectivity and virtual private network (VPN) connectivity to the Subscription Service), computer and telecommunications failures and delays, and network intrusions or denial-of-service or other criminal attacks. (c) "Maintenance Time" means the time the Subscription Service is not Available due to service maintenance. (d) "Availability SLA" means the percentage of total time during which Customer's production instances of the Subscription Service are Available during a calendar month, excluding Excused Downtime. AVAILABILITY If Customer's production instances of the Subscription Service fall below the Availability SLA of ninety-nine and eight-tenths percent (99.8%) during a calendar month, Customer's exclusive remedy for failure of the Subscription Service to meet the Availability SLAs is either: (1) to request that the affected Subscription Term be extended for the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA; or (2) to request that ServiceNow issue a service credit to Customer for the dollar value of the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA (determined at the deemed per minute rate ServiceNow charges to Customer for Customer's use of the affected Subscription Service), which Customer may request ServiceNow apply to the next invoice for subscription fees. REQUESTS Customer must request all service credits or extensions in writing to ServiceNow within thirty (30) days of the end of the month in which the Availability SLA was not met, identifying the support requests relating to the period Customer's production instances of the Subscription Service was not Available. The total amount of service credits for any month may not exceed the subscription fee for the affected Subscription Service for the month, and has no cash value. ServiceNow may delay issuing service credits until such amounts reach one thousand U.S. dollars ($1,000) or equivalent currency specified in the applicable Order Form.	
Docusign	Our industry-leading, global support model is there to back you up, no matter where you do your business. We provide you access to the expertise you want, whether through our communities, our knowledge base and on-demand training, or our team of experienced technical support professionals, who know you and your solutions.	
QTS	99.999% uptime guarantee. Meaningful Service Level Agreements are backed by financial penalties spelled out in tailored Master Service Agreements with each customer.	
SAP	Ariba	We guarantee a 99.5% system availability percentage during each month for production versions, with the exception of regularly scheduled and emergency maintenance.
	Hanna	Technical Availability for PRD systems - 99.5% Technical Availability for non PRD systems - 95% SAP shall track and report to Customer the "Technical Availability" in a monthly summary report. SAP HEC can offer a contractual SLA of 99.7 on a case by case basis.
	Hybris	SLA: contractually we provide a guarantee on the performance of your application at 99.9% availability.

	SuccessFactors	We guarantee a 99.5% system availability percentage during each month for production versions, with the exception of regularly scheduled and emergency maintenance.
VMware	AirWatch Service Level Agreements are non-negotiable. AirWatch has a guaranteed uptime SLA of 99.9%. Please refer to the AirWatch Hosted Services Policy for additional information. VMware AirWatch acknowledges that if it is awarded a contract under the RFP that it will annually certify to the Lead State that it still meets or exceeds the mandatory minimum requirements and technical specifications of the RFP.	
FireEye	FireEye cloud solutions are available 99.9% of the time in any calendar month, other than mutually agreed upon and scheduled downtime.	
VirtueStream	Virtustream IaaS Compute is comprised of computing resources hosted in secure data centers that replace the physical computing hardware traditionally housed on Customer site. These resources include physical servers which are logically divided into VMs (virtual machines), each with an allocation of CPU and memory, and linked to storage. Terms used in the detailed descriptions below: •µVM. Pronounced "micro VM," this is Virtustream's fine-grained unit of measurement designed to accurately measure the actual consumption of cloud resources. A µVM is a unit of computing resources, comprised of CPU, memory, storage IOPS, and associated local network bandwidth. The usage of each µVM resource component (CPU, memory, storage input/output, and network bandwidth) is measured at five minute intervals — one unit each for 200MHz of CPU, 768MiB of memory, 40 storage fabric input/output operations per second (IOPS), and 2Mbps of local network bandwidth. The highest of the four is averaged per hour, and the hour values averaged across the month to determine the overall µVM usage for the month. Note: The measurement is performed at the aggregate level — across Customer's entire µVM resource pool. Bandwidth usage is only within the data center. •Basic Plus uVM. These terms differentiate the two ways Virtustream offers µVMs services. "Basic Plus" µVM services are limited to a single Virtustream data center and have 99.99% availability for the Customer's committed level. "Reserve" µVM service is an equivalent quantity of Basic Plus µVMs reserved at Customer-designated secondary Virtustream data center for on-going operation during disaster events and during scheduled disaster recovery (DR) exercises. In both cases, overage resources required ("surges") up to 20% above the committed level from the contract /order form are provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level. •High Memory. Virtustream offers competitive pricing on compute services for applications that require large amounts of memory (64GiB or more). •Enterprise These terms identify the "zones" within which µVMs are made available for consumption. The "Enterprise" zone is for use by non-Internet facing workloads. Systems deployed into the Enterprise zone are not directly accessible from the Internet. Enterprise Basic Plus µVM (IC-uVM-BASP-ENT) Enterprise Basic Plus µVMs reside in a single Virtustream data center, in the Enterprise zone. Resource availability is 99.99%, and only at the designated data center. Overage resources required ("surges") up to 20% above the committed level from the contract /order form is provided at the same availability level. If Customer experiences consistent overage above this level, then Customer should reset the committed level. Service Level. 99.99% availability for the Customer's committed level. Billing. Monthly, based on resource usage. Tier 0 Block Storage - Local Only (IC-STO-TOA-LOC) Block storage with a Latency Service Level of 3ms that is maintained in a single data center with no replication capability. Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month.	

	Tier I Block Storage - Local Only (IC-STO-T1A-LOC) Block storage with a Latency Service Level of 10ms that is maintained in a single data center with no replication capability. Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month. Tier II Block Storage - Local Only (IC-STO-T2A-LOC) Block storage with a Latency Service Level of 20ms that is maintained in a single data center with no replication capability. Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month. Tier III Block Storage - Local Only (IC-STO-T3A-LOC) Block storage with a Latency Service Level Objective of 40ms that is maintained in a single data center with no replication capability. Billing. Monthly fee, based per GB of storage allocated. Allocated storage is measured every 30 minutes, averaged across the month. Tier 0 Block Storage - Replicated (IC-STO-TOA-REP) Data storage with a Latency Service Level of 3ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes. Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes. Billing. Monthly fee, based per GB of storage allocated. Tier I Block Storage - Replicated (IC-STO-T1A-REP) Data storage with a Latency Service Level of 10ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes. Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes. Billing. Monthly fee, based per GB of storage allocated. Tier II Block Storage - Replicated (IC-STO-T2A-REP) Data storage with a Latency Service Level of 20ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes. Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes. Billing. Monthly fee, based per GB of storage allocated. Tier III Block Storage - Replicated (IC-STO-T3A-REP) Data storage with a Latency Service Level Objective of 40ms that is persisted in Customer's primary Virtustream data center, and replicated to a second data center with an interval to provide a Recovery Point Objective (RPO) of 15 minutes. Service Level. Recovery Time Objective (RTO) of one (1) hour, and a Recovery Point Objective (RPO) of fifteen (15) minutes. Billing. Monthly fee, based per GB of storage allocated.

8.12.3 Specify and provide the process to be used for the participating entity to call/contact you for support, who will be providing the support, and describe the basis of availability.

CA	APM	CA Support can be engaged by telephone or online via CA Support Online at http://www.support.ca.com. CA Support is available 24x7x365. Technical support will be delivered in accordance with customer preference, and will likely include both telephone and email communications. CA Support Online is available 24 hours per

		day and allows customers to manage their cases (i.e. log, view, set severity level, update and close cases). CA Support Online also provides various other useful features, for example: a knowledge base search; product and documentation downloads; fixes, service pack and patch downloads; support utilities; automated notifications; access to communities, beta programs; subscriptions for hyper notifications, etc. While working with CA Support engineers on cases, email communications and a remote access capability can also be used to deliver support services. Secure File Transfer Protocol (FTP) and a secure FTP web client allow for the protected transfer of case file attachments to CA Support, with the web client additionally providing case file transfer protection from CA Support. Files are encrypted and stored securely while on CA systems. Optionally unsecure FTP transfers also are supported."
	MAA	CA Support can be engaged by telephone or online via CA Support Online at http://www.support.ca.com. CA Support is available 24x7x365. Technical support will be delivered in accordance with customer preference, and will likely include both telephone and email communications. CA Support Online is available 24 hours per day and allows customers to manage their cases (i.e. log, view, set severity level, update and close cases). CA Support Online also provides various other useful features, for example: a knowledge base search; product and documentation downloads; fixes, service pack and patch downloads; support utilities; automated notifications; access to communities, beta programs; subscriptions for hyper notifications, etc. While working with CA Support engineers on cases, email communications and a remote access capability can also be used to deliver support services. Secure File Transfer Protocol (FTP) and a secure FTP web client allow for the protected transfer of case file attachments to CA Support, with the web client additionally providing case file transfer protection from CA Support. Files are encrypted and stored securely while on CA systems. Optionally unsecure FTP transfers also are supported."
	CA Agile	Support is available 24/7 and a contact number will be provided upon completion of the contract.
	ASM	CA Support can be engaged by telephone or online via CA Support Online at http://www.support.ca.com. CA Support is available 24x7x365. Technical support will be delivered in accordance with customer preference, and will likely include both telephone and email communications. CA Support Online is available 24 hours per day and allows customers to manage their cases (i.e. log, view, set severity level, update and close cases). CA Support Online also provides various other useful features, for example: a knowledge base search; product and documentation downloads; fixes, service pack and patch downloads; support utilities; automated notifications; access to communities, beta programs; subscriptions for hyper notifications, etc. While working with CA Support engineers on cases, email communications and a remote access capability can also be used to deliver support services. Secure File Transfer Protocol (FTP) and a secure FTP web client allow for the protected transfer of case file attachments to CA Support, with the web client additionally providing case file transfer protection from CA Support. Files are encrypted and stored securely while on CA systems. Optionally unsecure FTP transfers also are supported."
Google	Customers are entitled to direct Google support in additional to whatever Support Services the reseller has to offer. Google has a published Technical Services Support Guide for both Google Apps and Google Cloud Platform that describe the hours of operation, how to get after hours	

	support, how to set the priority on a case, how to contact Google, and what the target response times are.
AODocs	Customers are entitled to direct AODocs support in additional to whatever Support Services the reseller has to offer.
Salesforce	Salesforce is proposing the Premier+Success Plan. Your Agency can cover all of its bases with this plan: support, training, and administration. It's what the + is all about. The Premier+ Success Plan gives you all the benefits of our Premier success plan, including a support rep assigned to your organization, priority case routing, 1-hour response time, 24x7 phone support, unlimited usage of our entire online course library, plus one very helpful addition: access to your own team of expert Salesforce administrators. This lets you focus on design and management while we support your configuration. The Premier+ Success Plan includes: ● Unlimited access to our entire online course catalog of 100+ courses ● 24x7 toll-free phone support ● Priority case queuing and routing ● Quick 1-hour response time ● An assigned support account rep ● Force.com code troubleshooting ● Customizable end-user course templates ● Premier Success Review to measure usage and trends ● Access to our pool of Salesforce Certified Administrators who can configure and maintain your Salesforce edition ● Premier Success Review to measure usage and trends ● Includes administration services: Get configuration help. Request 100+ routine configuration updates like creating users, reports, workflow, and dashboards. You take online administration training to learn the basics, then you tell us your business requirements. Our team of certified administrators updates your Salesforce system. Subject to the Government Cloud Premier+ Success Plan outlined above, access to systems and permissions which could permit access to Customer Data inside of the Salesforce Government Cloud storing U.S. government, U.S. government contractors, and FFRDC Customer Data will be restricted to Qualified U.S. Citizens. Qualified US Citizens are individuals who are United States citizens, and are physically located within the United States when accessing the Salesforce Government Cloud systems; and have completed a background check as a condition of their employment with Salesforce.Severity Levels & Response TimesIssues will be categorized and handled according to an assigned severity level, as follows: Level 1 - Critical Response time: 1 Hour* Critical production issue affecting all users, including system unavailability and data integrity issues with no workaround available. Level 2 - Urgent Response time: 2 Hours* Major functionality is impacted or significant performance degradation is experienced. Issue is persistent and affects many users and/or major functionality. No reasonable workaround available. Also includes time-sensitive requests such as requests for feature activation or a data export. Level 3 - High Response time: 4 Hours**

	System performance issue or bug affecting some but not all users. Short-term workaround is available, but not scalable. Level 4 - Medium Response time: 8 Hours** Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting a small number of users. Reasonable workaround available. Resolution required as soon as reasonably practicable. *24/7 Severity 1 and 2 coverage includes weekends and holidays **Severity 3 and 4 target response times include local business hours only and exclude weekends and holidaysOverview of Support Escalation PathAn issue is received by Tier 1 Support Rep who will document details and attempt to resolve. In the event that the problem cannot be resolved at this level, case will be escalated to a Tier 2 Support Rep for further analysis. Occasionally, a Case may be received for which technical understanding or indicated fix exceeds the responsibility of Support. These issues are quickly brought to the attention of R&D through the Tier 3/QA channel. Throughout the lifecycle of the case, customer will receive regular updates from the case owner at regular intervals based on case severity. Customers can work with their Support Account Specialist (SAS) if assigned through the purchase of Premier Support as a point of escalation should the need arise. Step-by-step escalation path: •Case is logged via Help Portal, Phone or through Live Chat •Depending on the functional area of the case a Tier 1 Support Rep from the appropriate skill group responds to the user confirming that the issue has been received and is in process. •Tier 1 analyzes the issue from the perspective of customer provided information in the case. •Tier 1 makes contact (phone or email) with the customer and gathers more information including any access needed to reproduce the problem. •With all necessary information gathered, Tier 1 will attempt to resolve the issue with the customer. •When resolution cannot be immediately achieved, Tier 1 Support Rep will escalate to a Tier 2 Support Rep in the same skill group. Tier 2 Support Rep will take all steps necessary to reproduce, understand and resolve the issue. •Technical Issues that cannot be resolved by the Tier 2 Support Rep are escalated to Tier 3. This escalation will provide a deeper layer of analysis with the possibility of escalation to QA/Development for Application issues and Escalation to Operation Services for Infrastructure issues as needed. •Functional Issues that cannot be resolved by Tier 3 are escalated to Product Management. •If it is an application Issue, necessary Development work will be performed, tested and a patch created. •Issue Fix Submitted to Operations for Infrastructure issues. •Issue Fix deployed. •Tier 2 Support Rep confirms success of Bug Fix in addressing the problem. •Tier 2 Support Rep contacts customer and confirms that the issue is Resolved. •Case is closed"
ServiceNow	Customer Support is provided by ServiceNow 24 hours a day, 7 days a week, including all holidays. Customer may contact ServiceNow using one of the following means: •Support Portal at https://hi.service-now.com/. Customer may get login access to this self-service portal by contacting its ServiceNow administrator. •Phone using one of the numbers at http://www.servicenow.com/support/contact-support.html. Customer shall contact ServiceNow's authorized reseller in accordance with its agreement with the reseller.

	See the "Customer Support Policy" contained within the "Subscription Service Guide" included with this response for more information.
Docusign	Enterprise Premier support provides 24x7 Live Phone Support.
QTS	Dedicated support staff is available 24x7x365 to generate and track incidents to resolution QTS Customer Portal provides round-the clock visibility into your environment
VMware	Global Support Services
FireEye	FireEye offers 24/7 technical support and its technical support centers around the globe in a follow-the-sun model. •Milpitas, CA, USA (UTC -7 hours) •Reston, VA, USA (UTC -4 hours) •Dublin, Ireland (UTC) •Singapore (UTC +8 hours) •Sydney, Australia (UTC +10 hours) FireEye Support is available via telephone, email, live chat, and web. Phone: U.S: +1 877-347-3393 (877 FIREEYE) Email: Support@FireEye.com Web Support: https://www.fireeye.com/support/get-support.html Support Programs: https://www.fireeye.com/support/support-programs.html
VirtueStream	Virtustream will work collaboratively with State of Utah to develop / maintain a relationship structure that leads to quick resolution, regularly scheduled status meetings, and quarterly business reviews. Virtustream will assign multiple key personnel to State of Utah including an Executive level sponsor. The primary point of contact will be Virtustream's Technical Account Manager (TAM). The TAM is responsible for daily activities/interaction and understanding/ensuring State of Utah's objectives are met at a minimum. Optimizations and other improvements to processes/standard operating procedures are delivered by the TAM in coordination with other Virtustream staff working behind the scenes. The TAM will coordinate day-to-day operation, service level management and SL reporting. The following outlines Virtustream's approach to service desk escalation and issue resolution. Escalations within Virtustream Virtustream will provide Level 0 and Level I support and first call resolution where possible, as determined by Virtustream. Where first call resolution is not possible, the Virtustream Service Desk provides incident management for Incidents and Urgent Service Requests escalated to Level II and Level III resources as defined below. In the event that Virtustream's Response to an Incident is not acceptable to the Customer, Customer can contact the Virtustream Service Desk and request escalation to the head of the Service Desk. Virtustream shall, upon receipt of any such request, immediately escalate the issue to the head of the Service Desk or technical team as appropriate. Service Request Prioritization Service Requests are assigned a priority of either 'Urgent' or 'Standard' and are queued for fulfillment with the corresponding priority. All Service Requests will be reviewed by the Virtustream Service Desk, who will determine the appropriate priority to assign with collaboration of Customer. Incident Prioritization All Incidents that are reported to the Virtustream Service Desk, or that Virtustream otherwise becomes aware of, will be initially assigned a priority by the Virtustream Service Desk as set forth below. Internal escalation for Incidents to Level II and Level III resources are based on the priority level assigned to the Incident.

Incident Prioritization			
Priority/ Severity	Definition	Response Time Service Level	
1	Major part of the system is unavailable/not operating correctly, affecting multiple users. No workarounds in place and business operations are not possible. Or Incident has a critical impact on the business (e.g., loss of the Exchange Production server impacting all users).	30 minutes	Response time will be within indicated time beginning from when the customer creates a ticket or a monitoring event is validated. Additional resources are engaged via Virtustream's on Call Process.
2	Part of the system is unavailable/not operating correctly, affecting users in a single function. No workarounds in place and business operations in this function are not possible/severely impacted. Or Incident has a serious impact on part of the business (e.g., a configuration change is impacting a small subset of users).	60 minutes	
3	Part of the system is unavailable/not operating correctly, affecting users in a single function. Workarounds in place, but business operations are impacted, although not severely. Or Incident has a temporary impact on users and is non critical or is a development issue (e.g., email is slow to deliver)	4 hours	
4	Incident that is causing inconvenience to the business, but not impacting operations. Or Incident has a minor impact on users or business, or issue is a request for further information	1 business day	

Virtustream will assign a Technical Account Manager starting on day 1 of the contract. The Cloud Platform, Cloud Cover (managed services), and Cloud Security team's will also be assigned to State of Utah upon execution of the contract. All of the individuals assigned to the State of Utah account have significant years of experience in their fields.

The TAM assigned to State of Utah will provide reports ad hoc but also on a quarterly basis. The quarterly business reviews include but are not limited to performance measurements, service requests. On a monthly basis, the TAM will provide a consumption report detailing the items consumed by each virtual machine. This delivers a very granular cost breakdown to State of Utah which will allow the data to be carved multiple ways. Also, information can be gathered by the State of Utah team any time they want from the xStream portal. State of Utah can also issue a ticket to Virtustream operations center to request information as well. The TAM will conduct scheduled meetings and be in constant contact with State of Utah. The TAM is an extension of the State of Utah team.

Virtustream defines a Root cause analysis (RCA) as the formal process, documented in writing by Virtustream and approved by Customer, to be used by Virtustream to diagnose problems at the lowest reasonable level which includes a report of the corrective action to be taken and defined timelines for corrective actions, which shall eliminate, to the extent reasonably possible, repeat failures. The following details the RASCI for RCA's:

	Role/Function	Customer	Virtustream
	Request Root Cause Analysis tickets by contacting the Virtustream TAM (Customer requests Incident report/Problem record)	R/A	S
	Document, track and manage all Problem tickets using ITSM system	S	R/A
	Provide Problem management review and Root Cause Analysis (RCA) for all in-scope P 1 Incidents (preliminary report within 48 hours; final within 15 calendar days)	S	R/A
	Provide Problem management and RCA of identified Problems (e.g., reoccurring events, alerts) - investigate and diagnose	S	R/A

8.12.4 Describe the consequences/SLA remedies if the Respondent fails to meet incident response time and incident fix time.

CA	APM	In the event that the Service Level Availability committed decreases below the Threshold for Service Availability Default, Minor or Major, Customer may be entitled to take action as outlined in the contract.
	MAA	In the event that the Service Level Availability committed decreases below the Threshold for Service Availability Default, Minor or Major, Customer may be entitled to take action as outlined in the SaaS Listing.
	CA Agile	In the event that the Service Level Availability committed decreases below the Threshold for Service Availability Default, Minor or Major, Customer may be entitled to take action as outlined in the contract.
	ASM	In the event that the Service Level Availability committed decreases below the Threshold for Service Availability Default, Minor or Major, Customer may be entitled to take action as outlined in the SaaS Listing.
AODocs	If AODocs does not meet the SLAs, the customer will be eligible to receive a service credit.	
Virtru	Email support@virtru.com	
ServiceNow	ServiceNow or its authorized reseller, as applicable, will use reasonable efforts to meet the target response times and target level of effort stated in the "Customer Support Policy" contained within the "Subscription Service Guide" included with this response for more information.	
SAP	Ariba	As part of the Cloud subscription, Ariba provides Customer Support services to help diagnose, troubleshoot and resolve functional and technical problems for all users. Ariba's award winning customer service staff can be contacted via phone (toll free), email or Web form Monday-Friday, 24/5 in multiple time zones and languages. Ariba Connect, our online support portal provides 24/7 support for service and enhancement requests. Customers may also choose to purchase ExpertCare. ExpertCare provides each customer with a named contact within Ariba that acts as an ExpertCare Manager for the customer and is knowledgeable about customer specific business process, configurations and customizations.
	Fieldglass	Our best practice is that the program office (managed by the State of Utah or your chosen MSP) provides first-level support for end users including hiring managers, approvers, suppliers, etc. Fieldglass' multi-lingual helpdesk is available by phone, email or web form 24x7x365. Our English language helpdesk is located at our corporate headquarters in Chicago. Merlin Information Systems Ltd., a UK entity, provides helpdesk service in French, German and Japanese from its Manila,

		Philippines and Debrecen, Hungary locations. We are prepared to assist with technical, functional or administrative questions about the Fieldglass application.
	Hanna	Customer key users have several options to communicate incidents into SAP Managed Cloud Delivery. Primary entry point: The best and easiest way to get an incident resolved is by creating and sending incidents directly to SAP Managed Cloud Delivery Service Teams via the SAP Support Portal. This communication channel ensures that all support teams are notified and therefore is the most preferred way to contact SAP on support/service related issues. Alternative option to the primary entry point: Customer key user can also communicate incidents by telephone via the SAP Customer Interaction Center (CIC) (e.g. in case of facing challenges in submitting an incident via the SAP Support Portal). Exceptional option: During business hours, customer key user may also communicate urgent incidents by contacting designated SAP Managed Cloud Delivery service contacts like Customer Engagement Service Manager (CESM) to create an incident on behalf of the customer. However – as already mentioned - this is not the preferred way of communication, but only should be applied in exceptional cases. Support times are contractually agreed upon with each individual customer organization. The SAP Managed Cloud Delivery (MCD) Service Desk and the Service Teams are spread across Europe, Americas and Asia.As a result of the global set-up across several time zones, SAP MCD Service Desk is able to provide worldwide 24/7 support to customers, throughout the entire year and according to the "Follow-The-Sun-Principle".
	Hybris	Key service levels are delivered through service level objectives, which provide for uptime of 99.9 for the hosted environment. Furthermore, monitoring is in place to report and alert upon uptime and response times of the environment to ensure best possible performance. The following support is specifically for the SAP Hybris Commerce, Cloud Edition. Customers can contact SAP Hybris Commerce, Cloud Edition technical support by toll-free telephone number or e-mail 24 hours per day, seven days per week. Based on the priority level, SAP Hybris's support personnel will attempt to provide Customer with remote assistance for reported issues. Contact information for technical support is as follows: Toll-Free Telephone Number: 888-944-2664 ext 6 In the event that Customer contacts SAP Hybris support, SAP Hybris shall respond to such reports as follows: Priority Level : Characteristics Response Time Resolution Time Objective

		Priority Level 1 Fatal Issue: Problem causing the Customer Website to cease from operating. This situation is generally described as a total failure. 25 Minutes (7x24) 2 hours Priority Level 2 Major Issue: Problem causing the Customer Website to experience major problems with it ability to operate. This situation exists when the Customer Website is partially failing however it is still able to function. 25 minutes (7x24) 12 hours Priority Level 3 Degradation of Performance: Problem affecting only certain non-critical functions of the Customer Website. This situation is occurring when the Customer Website is usable but has certain limited functions. 2 hours 1 business day Priority Level 4 Minor Issue: This situation includes all other non-critical problems. It is present when the Customer Website is usable however the problem results in a minor issue affecting it. 2 hours 3 business days Upon receipt of a service call classifying the priority level, SAP Hybris will deploy commercially reasonable efforts to respond and assist in the resolution of the problem. Application support for code developed by Customer or its implementation partner will be provided by Customer or Customer's implementation partner. If SAP hybris provides SAP Hybris Commerce, Cloud Edition support to a Customer as requested by Customer, and it is subsequently revealed that SAP Hybris was not responsible for the problem or the problem was not classified correctly by the customer, Customer will pay SAP Hybris on a time and materials basis for such support and assistance.
	SuccessFactors	
VMware	Our Availability Commitment for VMware AirWatch is 99.9%. The SLAs are subject to the terms of the applicable Terms of Service for VMware AirWatch. If the Availability of a class of service that you purchase is less than the associated Availability Commitment, then you may request Service Credits for that affected class of service. Availability in a given month is calculated according to the following formula: "Availability" = ((total minutes in a calendar month – total minutes Unavailable) / total minutes in a calendar month) x 100 A class of service will be considered "Unavailable," subject to the Service Level Agreement Limitations set forth below, if VMware's monitoring tools determine one of the following events has occurred ("SLA Event"). The total minutes that a class of service is Unavailable for a particular SLA Event is measured from the time that VMware validates the SLA Event has occurred, as defined below, until the time that VMware resolves the SLA Event such that the Service Offering is Available to you. If two or more SLA Event occurs simultaneously, the SLA Event with the longest duration will be used to determine the total minutes Unavailable.	

	1. Each of the following will be considered an SLA Event for the Dedicated Cloud, Virtual Private Cloud, or Virtual Private Cloud OnDemand Services: a) Any of the network interfaces of the Service Offering Network are unavailable for more than three (3) consecutive minutes. The "Service Offering Network" means the network that extends from the network interfaces of physical host servers for a class of service to the outside network interfaces providing the Service Offering's public internet connectivity. b) The data store(s) associated with your block level storage for a class of service are unavailable for more than three (3) consecutive minutes. c) The self-service console, available at https://vchs.vmware.com, cannot successfully authenticate a simulated user for more than five (5) consecutive minutes. d) Your running virtual machines for a class of service become inaccessible for more than five (5) consecutive minutes due to physical host server failures. 2. Each of the following will be considered an SLA Event for the Data Protection Service: a) The backup storage repository associated with your Data Protection service is unavailable for more than three (3) consecutive minutes. b) The start time associated with your backup scheduling window is missed for longer than thirty (30) consecutive minutes. c) The standard 24-hour recovery point objective (RPO) is missed for any virtual machines actively enrolled in the service. d) Any restore operation for a virtual machine fails to complete due to backup infrastructure failures. 3. Each of the following will be considered an SLA Event for the Disaster Recovery Service: a) Any of the network interfaces of the Service Offering Network are unavailable for more than three (3) consecutive minutes. b) The data store(s) associated with your block level storage for replication is unavailable for more than three (3) consecutive minutes. c) The self-service console, available at https://vchs.vmware.com, cannot successfully authenticate a simulated user for more than five (5) consecutive minutes. d) Your failed-over virtual machines for a class of service become inaccessible for more than five (5) consecutive minutes due to physical host server failures. e) Any built-in service functions for failover testing, planned migration, or live failover and recovery result in virtual machine replicas not powering on in less than 4 consecutive hours from the time a request is acknowledged and approved by VMware. 4. The following will be considered an SLA Event for the Object Storage service: a) A more than five (5) percent Error Rate for more than ten (10) consecutive minutes – where "Error Rate" means the number of valid requests that result in a response with HTTP Status 500 and Code "Internal Error" divided by the total number of valid requests during each five-minute period.
FireEye	FireEye shall use commercially reasonable efforts to correct any reproducible programming error in the Software attributable to FireEye, employing a level of effort commensurate with the severity of the error, provided, however, that FireEye shall have no obligation to correct all errors in the Software.

8.12.5 Describe the firm's procedures and schedules for any planned downtime.

CA	APM	Planned downtime is scheduled, and customers are notified
	MAA	Customers are notified at least two weeks in advance for planned downtime.
	CA Agile	Regularly scheduled maintenance (planned downtime for upgrades and maintenance) where the customer has been given at least eight (8) hours notice does not count as downtime. Unscheduled maintenance, in which the Rally Service is unavailable and

		advance notice was not provided to customers, will be counted against the up-time SLA.
	ASM	Customers are notified at least two weeks in advance for planned downtime.
Google	Google's maintenance routines are done in a manner that ensures there is no need to schedule any downtime.	
AODocs	AODocs's maintenance routines are done in a manner that ensures there is no need to schedule any downtime.	
Salesforce	There are two types of maintenance at Salesforce: System Maintenance and Release Maintenance. System Maintenance is for sustaining the performance, reliability, security, and stability of the infrastructure supporting our services. When maintenance is scheduled, the specific timing and availability to be expected during that time will be communicated to all customers approximately one week in advance of the maintenance window upon login to Salesforce and via a posting to http://trust.salesforce.com/trust/maintenance. In the event of planned maintenance where the services will be unavailable for more than four hours, or that requires customer action in advance, Salesforce endeavors to communicate via email several months in advance. Please Note: If emergency system maintenance is required, customers may be notified less than one (1) week in advance. Major Release Maintenance is for upgrading the services to the latest product version to deliver enhanced features and functionality. Major release dates and times are posted on http://trust.salesforce.com/trust/maintenance approximately one month before release to Sandbox instances. An email notification and blog post regarding Sandbox preview instructions is also sent approximately one month prior to upgrading Sandbox instances. Email notification of major release dates is sent one month prior to upgrading non-Sandbox instances. The Release Notes document describing the new features and functionality is posted in Help & Training one month prior to upgrading non-Sandbox instances. Final release reminders are communicated to all customers approximately one week prior via email and upon logging into Salesforce. Major release maintenance occurs three times per year. The instance will be unavailable for up to five minutes during the release window. Patch Releases and Emergency Releases are used to deliver scheduled and ad hoc application fixes. Patch releases are scheduled weekly and are usually deployed to instances on Tuesday, Wednesday or Thursday, with release to Asia-Pacific instances the following day. Emergency releases are conducted on an as-needed basis and can occur any day of the week. Whenever possible, patches and emergency releases are deployed during off-peak hours and without downtime.	
ServiceNow	ServiceNow notifies customers at least 10 days prior to scheduled maintenance for infrastructure network, hardware or software that might impact service. ServiceNow targets no more than two hours of downtime due to scheduled maintenance per month.	
Docusign	Continuous availability is a necessity for mission-critical business applications in a global world. It's also a key component of the xDTM standard. Zero maintenance downtime means that DocuSign is always available, regardless of the time-of-year, day-of-week, time zone or country. DocuSign's Carrier Grade System Architecture, a first in SaaS, eliminates maintenance downtime, and ensures the highest level of performance resiliency and data integrity. This is accomplished through a combination of advanced high availability architecture, native DocuSign engineering, and both specialized and commodity hardware and software components.	
SAP	Ariba	Scheduled downtime windows for maintenance, upgrades or new releases are provided in the Service Level Agreement. Our uptime percentage takes scheduled maintenance into account.

	Fieldglass	Fieldglass' maintenance windows are as follows: • Friday maintenance window of 11:00 p.m. – 2:00 a.m. Central (Daylight Savings Observed) • Extended maintenance windows are taken with five days advance notice and are typically as follows: - Second Friday of each of the following months: March, July, and November - Critical service packs, security issues, and other emergencies will still be taken if needed with communication as reasonable
	Hanna	SAP performs periodic scheduled maintenance activities to maintain security patching levels, application transports, fixes, network maintenance, and other scheduled proactive activities during scheduled maintenance window (agreed to by the customer). The predefined maintenance window is 4 hours per month (for example first friday of every month) SAP may perform additional maintenance services on the Customer's Computing Environment in agreement with Customer, with at least ten (10) Business Days prior notice (which notice may be by email to Customer's nominated contact or posting) of the date and anticipated length of the maintenance window, and provided that SAP adheres to Customer's reasonable requirements as to the timing and duration of any such maintenance. SAP reserves the right to apply critical application and operating system security patches in compliance with the SAP Global Security Team's reasonable recommendations. SAP will use reasonable endeavours to provide Customer with forty-eight (48) hours advance notice regarding the critical patch deployment unless a shorter notice period is required in order to address a critical security issue. Non critical security issues shall be dealt with by Scheduled Maintenance
	Hybris	Typically they are two-hour maintenance windows, with no downtime or on occasion maintenance periods require between 2 to 10 minutes of downtime. Other rare periods which may require further maintenance could have downtime between 30 min to 4 hours.
	SuccessFactors	To address issues such as security patches, hot fixes, updates, equipment upgrades, etc., we has established maintenance windows to perform scheduled maintenance. Scheduled maintenance events typically occur during only one of these windows, roughly every 6-8 weeks. A 14-hour/week window will be used for all critical / most emergency patches and all bug fixes (will include tech stack and application patch sets). We define scheduled downtime maintenance windows as: Midnight to 7 a.m. Fri-Sat local time + midnight to 7 a.m. Sat-Sun local time (dependent upon the data center where the customer data is hosted) We will provide customers with at least a 2 days' notice if a larger maintenance window is needed. Typically, for HCM / LMS products, customers receive a 3-5 day notification (via popup on login). When the system is not available during the maintenance there is a notification page displayed for the outage timing. We plan maintenance events conservatively, and use them sparingly.
VMware	VMware IaaS Services Customers are notified in advance of any expected downtime with vCloud Air services. In the event of an unexpected outages or disruption to the service, customers will be notified via their preferred contact means as soon as possible as per the terms outlined in the Service Level Agreement. VMWare AirWatch	

	We maintain standard SLAs with our customers to provide for downtime • SLAs are defined within the AirWatch Hosted Services Policy Per our Hosted Services Policy, we provide outage credits in the event of a service interruption: • ""AirWatch warrants it will provide Availability of the Hosted Services 99.9% of the calendar month (the "Service Level"). To the extent that the Hosted Services fail to conform to the Service Level, Customer may request service credits ("Outage Credits") as provided herein. A failure or lack of Availability for any period of time of at least one minute during which Customer is unable to utilize the Hosted Services due to AirWatch's failure to provide Customer with the specified services constitutes an "Outage". All Outage measurements will be rounded up or down to the nearest one minute increment, with increments equal to or greater than 30 seconds being rounded up to the next minute. Outage Credits are based on cumulative periods of Outage over a calendar month. Final determinations of the length of the cumulative periods of Outage over a calendar month shall be based on AirWatch's internal monitoring equipment and records. Outage Credits will be taken against only the Hosted Service fees for the month in which the Outage occurred.""
FireEye	FireEye undertakes reasonable efforts to ensure that the service availability maintains a minimum of 99.9% availability. However there are circumstances where the system will be down due to the following: a) "Scheduled Maintenance Period" is the period during which weekly scheduled maintenance may be performed, or a maintenance window otherwise mutually agreed upon by FireEye and Customer. Customers receive notification and announcements for any scheduled maintenance period. b)"Emergency Maintenance" means any time outside of Scheduled Maintenance that FireEye is required to apply critical patches or fixes or undertake other urgent maintenance. If Emergency Maintenance is required, FireEye will contact Customer and provide the expected time frame of the Emergency Maintenance.
VirtueStream	Virtustream planned downtimes start with the weekly change board meeting by the Platform Operations group. All requested changes whether requested by customers or by the operations staff are reviewed, if approved then scheduled. Depending on the nature of the change, routine and planned, the affected customers are notified as early as possible and adjusted based on customer needs. For example, if the scheduled downtime falls on a weekend that a customer plans to do their quarterly close, Virtustream will reschedule. An emergency/urgent change may have less notice for the customers. But in all cases, customers will be notified of the upcoming downtime multiple times, start of the downtime will be specified and the expected duration. Once the downtime is complete, another notification will go out to the affected

8.12.6 Describe the consequences/SLA remedies if disaster recovery metrics are not met.

CA	APM	In the event that the Service Level Availability committed decreases below the Threshold for Service Availability Default, Minor or Major, Customer may be entitled to take action as outlined in contract. Defined, monetary penalties are provided in the SaaS Listing document.
	MAA	Defined monetary penalties are provided in the SaaS Listing document
	CA Agile	See 8.12.4
	ASM	Defined, monetary penalties are provided in the SaaS Listing document
Google	Customers will be eligible to receive a service credit.	
AODocs	Customers will be eligible to receive a service credit.	
Salesforce	Customer data, up to the last committed transaction, is replicated to disk in near-real time at the designated disaster recovery data center, and backed up at the primary data center. Backups are performed daily at primary data center facility without stopping access to the application.	

	For business continuity purposes, Salesforce supports disaster recovery with a dedicated team and a 4 hour recovery point objective (RPO) and 12 hour recovery time objective (RTO). Additional details can be provided with the execution of an NDA between Salesforce and your Agency. In terms of remedies, the Salesforce Service Terms incorporated as part of the End User Licensing Agreement indicate the following regarding Termination allowing customers to terminate the contract at time of renewal: ""User subscriptions will automatically renew for additional periods of one (1) year at the list price in effect at the time of renewal unless You give Your Reseller notice of termination at least 30 days prior to the end of the relevant subscription term.""	
ServiceNow	See 8.12.2 for the Availability SLA.	
Docusign	See 8.12.4.	
SAP	Ariba	Please see the details provided in 8.12.4 response.
	Fieldglass	Please see the answer to Question 8.12.4, above.
	Hanna	Penalties and remediation for SLA violations are detailed in the Statement of Work.
	Hybris	Our SLA provides tenant remuneration for losses they may incur due to outages within the infrastructure.
VMware	For VMware there is a service credit reimbursement structure outlined above. We have detailed recovery procedures that include defined steps, roles and responsibilities and accountable personnel to help ensure streamlined disaster recovery. As conversations progress, AirWatch can provide specific details regarding our disaster recovery timelines and strategies.	
FireEye	FireEye has established formal Business Continuity and Disaster Recovery plan, as well as Incident Response and Recovery Plans to help maximize availability of critical customer-impacting services.	

8.12.7 Provide a sample of performance reports and specify if they are available over the Web and if they are real-time statistics or batch statistics.

CA	APM	A report of the Service's measured monthly SLA is available to Customer upon request
	MAA	Reports are generated periodically and ad hoc. Customers can use their support.ca.com credentials to access private trust site which contains SLA details for the subscribed service.
	CA Agile	Realtime and historical system status can be viewed at https://status.rallydev.com
	ASM	Reports are generated periodically and ad hoc.
Google	Google does not produce customer specific performance reports. The web based Apps Status Dashboard displays real time System Availability Details. Customers can works with their Google reseller to design a reporting system using Google Sheets based on which incident actually impacts their end users. Service availability issues are isolated to specific applications and specific geographically locations and thus would not impact all of your users or your account at all.	
AODocs	AODocs does not produce customer specific performance reports. Customers can visit the AODocs status page: status.aodocs.com. AODocs provides a set a usage reports and AODocs team can also work with the customer to build specific reports	
Virtru	We have realtime monitoring of both server side operations and client side interactions.	
Salesforce	System Performance ReportsOur track record speaks for itself—Salesforce has maintained high levels of availability across all Salesforce instances since inception. As an on-demand vendor	

	providing daily service-quality data on a public website (http://trust.salesforce.com), Salesforce proves that it is a leader in availability. And by making its track record completely transparent, salesforce.com proves it is worthy of customers' trust. A few metrics that we maintain (and publish publicly via our trust.salesforce.com website) are: -Daily Transaction Counts -Daily Transaction Speeds Salesforce is hitting almost 4 billion transactions a day. These transactions are a mix of user interacting with the system and API calls where other systems are bi-directionally interacting with Salesforce. Our Average Transaction Time hovers between 150 and low 200 milliseconds. Some additional published metrics are uptime & availability, planned maintenance windows, and any performance degradation. The Purchasing Entity can view all of this information and more by going to trust.salesforce.com. Customers can also log a case to request system uptime reports for the last 6 months and last 12 months, however, system reports are not automatically distributed.	
ServiceNow	Administrators can view a wide range of performance metrics for their instance and for the machine on which the instance is running, displayed in a graphical format. Add these graphs and their controls to a home page to monitor the performance of instances. Some of these graphs are intended for use by ServiceNow Technical Support to troubleshoot performance issues or help tune your system for maximum efficiency. Each graph enables admins to filter the data by using different measurements, such as maximum and minimum values, means, and medians. The available graphs reflect performance in eight functional areas of ServiceNow. •Database •Discovery •Disk Partitions •Linux Stats •Logging •MySQL Overview •Node Metrics •Replication •ServiceNow Servlet	
Docusign	For real-time data, please visit the DocuSign Trust site (trust.docusign.com) for additional information.	
SAP	Ariba	We provide a monthly report to customers describing the system availability percentage. Depending on the cloud service, these reports are made available either by email, through the cloud service or through an online portal.
	Fieldglass	Fieldglass executes comprehensive performance testing prior to each release to production. Performance testing is executed in accordance with the Fieldglass Performance Testing Standards document. Types of testing performed include regression, load, stress, and endurance. Results are reviewed and approved by senior members of development, QA, IT, and the Chief Architect. Our standards document can be shared upon request while under NDA. During peak periods, Fieldglass will see 12,000 concurrent users with page response times averaging 400-700ms. Across all of 2015, we have a 99.4% success rate in meeting or exceeding all monthly customer SLAs for page response times.
	Hanna	Performance reports on HEC are available to the customer via the SAP One Portal page. It provides the customer among other things: operational info about systems being managed, incident management, security management, user specific settings, planned downtime, etc.

	SuccessFactors	Customers can view hosting performance and availability information real-time at the following link: https://support.successfactors.com/Service_Status.
VMware	VMware IaaS Services VMware vCloud Air provides Web-based capacity reporting via the MyVMware portal. For detailed performance reporting, participating entities may wish to acquire VMware vRealize Operations suite, which is a non-Web based software product which provides real-time and historic performance statistics for vCloud Air. VMWare AirWatch We can provide sample performance testing documents that validate our ability to handle anticipated workload under real-world conditions as conversations progress. We have a dedicated team for scalability and performance testing. They work with both internal teams and customers to conduct testing.	
FireEye	This is not applicable as each of the FireEye offerings are classified as SaaS. The performance of the FireEye cloud environments are continuously monitored and managed by the cloud service operations (CSO) team to ensure secure operation and availability.	
VirtueStream	Service Levels will be calculated and measured monthly by Virtustream on a calendar month basis and reported each month for the previous month. The reports will be provided to Customer by the tenth (10th) working day of the month following that to which such report relates, commencing on the second (2nd) month following the Service Start Date and each month thereafter. The monthly service level report will contain at least the following items: (i) Uptime statistics for the month concerned; (ii) an analysis of reported incidents over the previous month, broken down by type for discussion; (iii) action plans for items giving rise to concern; (iv) comments and observations on any issues arising from Virtustream's performance monitoring activities; (v) recommendations on service delivery strategies to maintain or enhance the service level; and (vi) review of general business requirements ("Service Level Report"). Cloud Platform Services (CPS) has its own specific service levels as described in this document. Cloud Cover Services (CCS) has service levels that pertain to the CCS offerings and are reported separately. Not all Virtustream customers have CCS but all Virtustream customers use CPS.	

8.12.8 Ability to print historical, statistical, and usage reports locally.

CA	APM	A report of the Service's measured monthly SLA is available to Customer upon request
	MAA	Same as above.
	CA Agile	This is available upon request.
	ASM	Customers are sent monthly SLA reports.
Google	See 8.12.7	
AODocs	See 8.12.7	
Virtru	We may be able to publish reports locally for customers.	
Salesforce	Trust.salesforce.com is the Salesforce community's home for real-time information on system performance and security. On this site you'll find: • Live and historical data on system performance • Up-to-the minute information on planned maintenance • Phishing, malicious software, and social engineering threats • Best security practices for your organization • Information on how we safeguard your data	

	In addition to the Salesforce Trust site (http://trust.salesforce.com/trust/status) to monitor uptime and performance, your Agency will also have access to a System Overview, which will help you monitor performance and usage of your own Salesforce org. This overview includes: Schema - # and % of custom objects and data storage Business Logic - # and % of Rules, Apex triggers and classes, as well as % of code used License Usage API Usage - # and % of requests in the last 24 hours User Interface - # and % of custom apps, sites, flows, custom tabs and pages Portal Usage The above list is of all the possible metrics that you may have in your system overview.	
ServiceNow	Yes. Instance performance can be viewed locally. Customers can use the Customer Support Portal to obtain information about the real availability of all their instances. Real availability is the percentage of production time that an instance is up and available for use.	
Docusign	Yes. DocuSign offers a number of pre-defined reports to provide detail and summary information on DocuSign usage in the account, such as by Envelope, Recipients, Velocity of signing, and User Access among many other reports. Users can modify report criteria such as data ranges and reports can be scheduled to execute. All reports can be downloaded or Printed locally.	
QTS	Yes	
SAP	Ariba	User access is browser-based, so printing is enabled via the printers that are setup on the user's workstation. There are several "Print" buttons throughout the applications that will open an additional browser window with a printer-friendly format of the screen.
	Fieldglass	Any user with the correct permissions in the system, as specified by the State of Utah, may locally print historical, statistical, and usage reports.
	Hanna	Yes, available
VMware	VMware IaaS Services At the present time, VMware does not provide end user customers with specific reports for SLA performance. VMware tracks the overall health of the environment and will report to customers in the event of an outage. However, specific SLA performance is not delivered as a report, but as an alert. It is currently the customer's responsibility to track downtime within their environments and report to VMware when they believe SLA has been violated. VMWare AirWatch Customers can export and print solution data using interactive dashboards (CSV), reports (PDF, XLS, and CSV), the AirWatch Hub (PDF), and event log (CSV)	
FireEye	Each of the offerings in this response have reporting capabilities local to the system and users with the appropriate access rights.	

8.12.9 Offeror must describe whether or not its on-demand deployment is supported 24x365.

CA	N/A. CA only offers SaaS solutions and manages all aspects of the service. Clients do not have direct access to the environment.
Google	Purchasing entities will subscribe to an initial set of user licenses and can provision new user accounts at their convenience within that range of licenses.
Salesforce	The Salesforce service can be deployed rapidly since our customers do not have to spend time procuring, installing or maintaining the servers, storage, networking equipment, security products,

	or other infrastructure hardware and software necessary. The service is always available and the customer can deploy 24x365 at their own pace.
ServiceNow	ServiceNow is supported 24x365.
FireEye	The FireEye offerings in this response are SaaS service models. Once the application or service is set up there are no further deployment steps necessary. On-demand Self-service options referenced in section 8.1.2.1 are available 24x365.
VirtueStream	Virtustream's self-service portal allows authorized users to deploy resources on-demand 24x365.

8.12.10 Offeror must describe its scale-up and scale-down, and whether it is available 24x365.

CA	N/A. CA only offers SaaS solutions and manages all aspects of the service; monitoring and capacity planning is included as part of the service.
Google	Purchasing entities will subscribe to an initial set of user licenses and can provision new user accounts at their convenience within that range of licenses. If the purchasing entity has exceeded or is about to exceed their user count they can place an order for additional licenses at any time. Scale-down procedures will be handled on the renewal anniversary.
Salesforce	The Salesforce cloud based architecture will allow the State to deploy Salesforce solutions rapidly and scale at will for future needs. Customer's may scale up and add licenses at any point during their annual contract cycle. User counts are examined on an annual basis at time of renewal to ensure the customer had adequate license coverage.
ServiceNow	ServiceNow can automatically scale its application servers horizontally by adding or subtracting them to the load balancer pools for a particular instance. Scaling is managed by the ServiceNow Cloud Operations team.
FireEye	The FireEye offerings in this response are SaaS service models. FireEye cloud environments are continuously monitored by cloud service operations (CSO) personnel to help ensure optimal resources are allocated to the system 24x365.
VirtueStream	Virtustream's self-service portal allows authorized users to deploy or de-commission resources on-demand 24x365.

8.13 Cloud Security Alliance

Describe your level of disclosure with CSA Star Registry for each Solution offered.

a. Completion of a CSA STAR Self-Assessment, as described in Section 5.5.3.
b. Completion of Exhibits 1 and 2 to Attachment B.
c. Completion of a CSA STAR Attestation, Certification, or Assessment.
d. Completion CSA STAR Continuous Monitoring.

Carahsoft is proposing a number of Service Providers that are members of the Cloud Security Alliance. For example Salesforce is a corporate member of the Cloud Security Alliance (CSA) and contributes to their research and initiatives in a variety of ways. Salesforce has completed the CSA Consensus Assessments Initiative questionnaire (CAIQ), which maps to the CSA Cloud Controls Matrix (CCM) for the Salesforce Services, including Force.com, Analytics Cloud, Communities, Chatter, Sales Cloud and Service Cloud. A copy of the current completed CSA CAIQ can be provided to prospects or customers under NDA upon request.

8.14 Service Provisioning

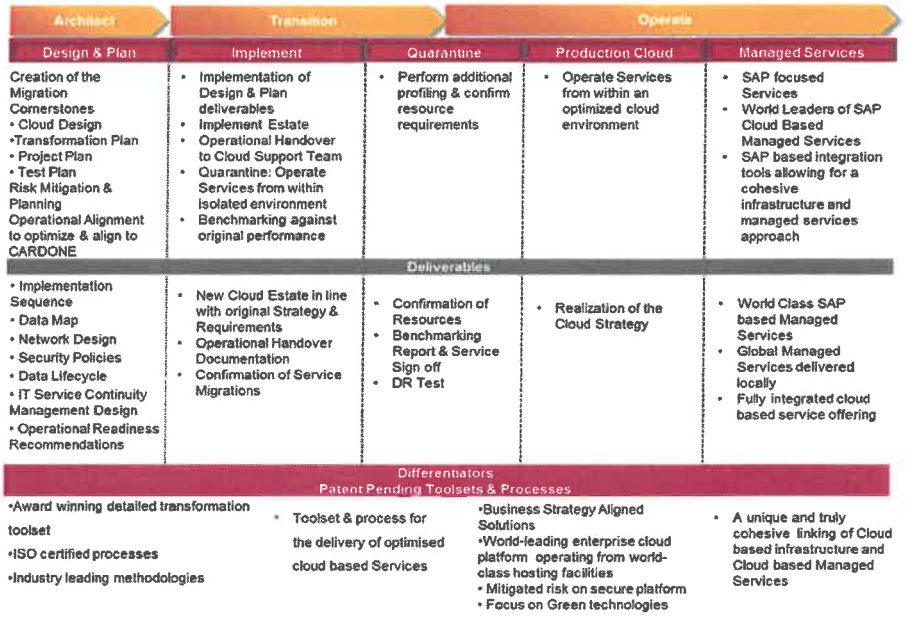
8.14. 1 Describe in detail how your firm processes emergency or rush services implementation requests by a Purchasing Entity.

CA	APM	CA SaaS Ops has a rigorous service introduction and update process that is governed by a central body to ensure adherence. Every step in the process is recorded, tracked and approved.
	MAA	Standard lead times for requests can be waived for requests that have a critical business need
	CA Agile	Standard lead times for requests can be waived for requests that have a critical business need such as a data recovery effort
	ASM	Standard lead times for requests can be waived for requests that have a critical business need such as a data recovery effort
Google	Order processing from the time a valid Purchase Order is submitted has a normal turn around time of three business days. Google's sales team can be contacted to expedite orders when needed.	
AODocs	Order processing from the time a valid Purchase Order is submitted has a normal turn around time of two business days. AODocs's sales team can be contacted to expedite orders when needed.	
Virtru	Requests are triaged by the support and if an emergency is identified, the request is escalated by the VP of Product who immediatlye assigns the issue as a top priority to a developer. Once completed a hotfix is pushed to production.	
Salesforce	Subscription-based, On-Demand Service Salesforce offers on-demand Platform as a Service (PaaS) and Software as a Service (SaaS). The Salesforce PaaS and SaaS offerings are subscription based and in a per user/month or user/year format billed annually with some of our products offered as total logins per month or by defined number of members billed annually. Multi-tenancy gives applications elasticity. Force.com applications can automatically scale from one to tens of thousands of users. Processing more than three billion transactions each day, Force.com is used for large-scale deployments. Any application that runs on Force.com is automatically architected to seamlessly scale from 1 user to 100,000 users without the customer having to do anything differently. All applications (includes mobile, offline and read-only options) and data running on Force.com are deployed to and replicated across multiple data centers in different geographies. Every application, no matter how large or small, gets the full benefits of the backup, failover, disaster recovery, and other infrastructure services required for an organization's mission-critical applications.	
ServiceNow	ServiceNow professional services organization responds to customer needs based on each request. Once a purchase order is received from the Purchasing Entity, ServiceNow contacts the Customer to discuss schedules. Resources are assigned based on the project need. If the customer has a priority issue with the system, they would open a ticket and the ticket SLA process would proceed until the issue is resolved. Every ServiceNow customer is supported based on their priority and need.	
SAP	Hanna	Rush or emergency infra provisioning can be request in exceptional situations and would be addressed on best effort priorty basis.
VMware	VMware IaaS Services Initial Order - Expedite the purchasing process thro - In the event that an emergency or rush service implementation request is received, VMware's NASPO program manager will coordinate an expedited response depending on the request. - Expedited Procurement - The Program Manager will directly interface with each company in the supply chain to ensure that the order is processed immediately upon receipt by each party. - Expedited In Increased capacity	

	VMWare AirWatch Participating Agencies will work with thier dedicated Account Executive to procure addition services for thier AirWatch implementations. Customers can implement and update configurations through the AirWatch administrative console. Additionally, customers can submit ASK tickets for any solution issues that will be tracked through completion.
FireEye	FireEye will make every reasonable effort to accommodate rush provisioning requests. The purchasing entity should contact their sales account team who will interface directly with the corresponding implementation team to coordinate an expedited implementation.

8.14.2 Describe in detail the standard lead-time for provisioning your Solutions.

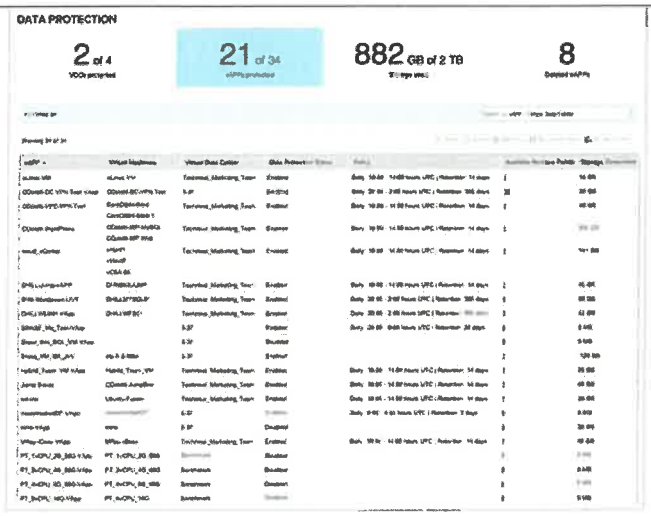
CA	APM	48 hour turnaround is typically required
	MAA	Services do not generally require client action for provisioning. General service catalog requests have a standard 48 hour lead time
	CA Agile	Services do not generally require client action for provisioning. General service catalog requests, such as a data refresh, have a standard 48 hour lead time
	ASM	Services do not generally require client action for provisioning. General service requests have a standard 48 hour lead time
Google	Standard lead time is three business days.	
AODocs	Standard lead time is two business days.	
Virtru	The Lead-time for provisioning is no more than 15 minutes	
ServiceNow	ServiceNow provisions new instances or newly purchased users or applications to the instance within 48 hours after receipt of order. If users or applications are required more quickly, the customer controls access to all ServiceNOw capabilities at any time and the true-up occurs thereafter.	
Docusign	DocuSign is intuitive and easy-to-use. Getting started with our cloud solution, standard console, can be implemented in a day. Adding integrations or API's will add to the complexity of the implementation, but our Professional Services are there to guide you every step of the way.	
VMware	VMware vCloud Air Services VMware vCloud Air OnDemand services can be purchased and provisioned in minutes via the vCloud Air self service portal. VMware vCloud Air services other than OnDemand are purchased via purchase order. Purchase orders are typically processed on the day of order. Once services have been purchased the user can immediately begin provisioning services from the self service portal. These services are available within minutes of launch. VMware vCloud Government Services VMware vCloud Government Services are purchased via purchase order. Purchase orders are typically processed on the day of order. New environments require an RSA token that is overnighted for 2 factor authentication. Once the user has their RSA token they can begin to provision IaaS Services. VMWare AirWatch AirWatch is committed to implementing the solution in a timely manner and we work closely with customers to meet internal deadlines. Delivery and deployment models will vary depending the hosting model selected by the customer: • SaaS deployments can be implemented within several days and some within a few hours • Large enterprise deployments with numerous integration endpoints may require additional time Once an order is placed, we immediately begin working with the customer to finalize terms and conditions in a mutually agreeable manner and begin the implementation process. We schedule regular check-ins for project status updates and to discuss any questions or concerns.	

FireEye	FireEye anticipates that the standard lead-time is expected to take no more than five (5) business days. However, FireEye is willing to accommodate an urgent request from NASPO in order to provide adequate service to the participating states.
VirtueStream	Virtustream's standard lead-time for provisioning can vary based of the type of deployment and requirement. Resources can be deployed on-demand basis by State of Utah. For the initial services, there is a standard which is maintained as best practice. At project kick-off, Virtustream and State of Utah will develop a detailed Implementation Plan, on a system-by-system, week-by-week basis, to ensure that both sides of the relationship have clear expectations on what is to be accomplished, by whom, and in what timeframe. Upon completion of the Implementation Plan, Virtustream and State of Utah will establish a Project Governance Plan and the Project Governance Plan will manage Implementation Plan and ensure alignment at all tiers of the organization, define expectations for status update frequency and formats, and establish an escalation path for issue identification and resolution. Virtustream offers a dedicated onboarding project team that is charged with migrating clients into the xStream® cloud. This chargeable service includes resources from our platform and SAP teams and development of an onboarding project plan with milestones and deliverables. Virtustream uses a mature methodology to move clients onto our cloud platform, a process which is continuously refined and improved. A link is established to the client site using a Virtual Private Network (VPN) or Multiprotocol Label Switching (MPLS) circuit, for customer access and testing of migrated systems. Prerequisites are put into place (domain controllers, backup systems, infrastructure, networking, etc.) prior to systems being onboarded, in a defined sequence. Virtustream SAP basis team members test the systems before turning them over to Ascend for validation. Once on the xStream® platform, Virtustream monitors, backups and maintains the systems. As a component of the Virtustream platform, all core units are replicated to an alternate data center to provide disaster-recovery capability. **Figure 3. Sample Work Plan** 

8.15 Back Up and Disaster Plan

8.15.1 Ability to apply legal retention periods and disposition by agency per purchasing entity policy and/or legal requirements.

CA	APM	Not currently available.
	MAA	Not Available.
	CA Agile	The customer is responsible for the lifecycle of their data. We will retain all data until it has been deleted from our systems. We can remove data from our systems upon written request from the customer at termination of the contract.
	ASM	Not available.
Salesforce	Salesforce customers are responsible for complying with their company's data retention requirements in their use of the Salesforce Services. If a Salesforce customer must preserve data and the retention procedures above are insufficient, they may schedule a weekly export of data or copy to a sandbox account. Exports of Customer Data are available in comma separated value (.csv) format by request via Salesforce's Customer Support department. In addition, many exports can be manually pulled by the designated org administrators.	
ServiceNow	Once notified ServiceNow has the ability to leverage our internal clone operation process. This provides a locked state copy of the instance, while the customer can continue working on the production instance. Any data additions, changes or deletes will be on the production but not on the frozen instance copy. Additionally, ServiceNow can freeze backups to prevent them from being over written.	
Docusign	DocuSign customers determine their retention policies.	
QTS	Yes QTS will work with customers to meet legal requirements.	
SAP	Ariba	For the network's standard record retention is 180 days, but customers can request longer terms.
	Fieldglass	Fieldglass has many methods in which we can freeze customer data, today. We have the capabilities to restore, utilizing a point in time recovery method to a secondary system for legal review effectively delivering a system that has been frozen in time for all clients.
	Hanna	HEC standard backup retention is 1 month for productive systems, and 14 days for non-productive systems. However retention period can be changed per request and may have cost impact.
	SuccessFactors	A customer can configure as many ""purge rules"" as required to comply with data privacy rules. Since these rules vary by country, the solution provides the flexibility to define different retention periods for groups defined by country, department, division, location, job code and hire date. Customers can grant permissions to the appropriate users to create a request to purge data and to approve the request to purge data. These ""purge rules"" can be scheduled to reoccur. User records are kept in the system, for reporting purposes, but their data is anonymized. Our customers use the solution in compliance with local regulations today in almost 180 countries.
VMware	VMware IaaS Services Participating entities that leverage VMware Data Protection are able to specify the retention period of their backups to comply with policies and legal requirements. Data Protection leverages snapshots to take an image level backup of virtual machines. When a backup is initiated, a snapshot is taken of that virtual machine. Once the snapshot is taken it is then stored on the Data Protection storage for the duration of the retention period assigned in the policy. The policy column in the screenshot below illustrates the variety of data retention policies that have been set within a sample customer's vCloud Air Data Protection instance. In this example retention policies range from 3 to 365 days.	

	 VMWare AirWatch Customers can export and archive solution data using interactive dashboards (CSV), reports (PDF, XLS, and CSV), the AirWatch Hub (PDF), and event log (CSV). Customers in a Dedicated Cloud deployment can leverage a robust data mart.
FireEye	Customers have access to data stored in the varying cloud solutions and are accessible at any time during the length of the subscription contract. Retention periods vary per service offered. See section 8.7.2 for further information.
VirtueStream	Specific retention requirements can be accommodated on a custom basis. More detailed information would need to be provided in order to scope.

8.15.2 Describe any known inherent disaster recovery risks and provide potential mitigation strategies.

CA	APM	DR is provided only in a single geography at this point. Professional Services would need to be engaged to provide multi-geo DR
	MAA	N/A
	CA Agile	None - our DR plan is tested at a minimum semi-annually.
	ASM	None
Virtru	Please see the Virtru Disaster Recovery Plan provided in the Supplemental Information section of this response.	
Salesforce	The Salesforce service performs near real-time replication at each data center and annual disaster recovery tests for the service verify the projected recovery times and data replication between the production data center and the disaster recovery center. The disaster recovery site is a 100% replica of the primary production site of capacity (host, network, storage, data). Data is transmitted between the primary and disaster recovery data centers across encrypted links. Additionally, back-ups of data are performed and data is retained on backups at the geographically separated disaster recovery data center location [CP-4, CP-6, CP-7, CP-9, MP-5].	
ServiceNow	ServiceNow is divided into two distinct environments for Business Continuity (BC) and Disaster Recovery (DR). ServiceNow's corporate environment and its data center environments are physically and logically isolated from each other. A disaster in ServiceNow's corporate environment could occur with little or no impact on the ability for the data centers within the private cloud to operate. In both cases, the BC and the DR are supported by a series of SOPs that allow ServiceNow to quickly and effectively take action when it is required.	

<table>
<tr><td></td><td colspan="2">ServiceNow's customer DR is documented in its Information System Contingency Plan (ISCP), which covers its data center environments, and includes all customer environments as well as the instances that ServiceNow uses to run its business.

ServiceNow formally tests this process on an annual basis and can produce compliance reports for customers requiring them. ServiceNow also uses the process of transferring instances to reduce the impact of maintenance on its service and will move instances out of one data center to the other on a daily basis. As a result, ServiceNow is very well practiced at the process of "failing over" customer instances.

ServiceNow's BC process covers its functional offices and is a separate standard operating procedure from its customer environments. The BC Plan (BCP) has been developed in concert with the entire business including Business Impact Assessments (BIA) to understand the impact of the loss of any given systems or locations.</td></tr>
<tr><td>Docusign</td><td colspan="2">DocuSign is dedicated to providing the industry's most secure eSignature solution through the DocuSign Security Assurance Program.</td></tr>
<tr><td>QTS</td><td colspan="2">Not having a current copy of your information.
Mitigation - QTS's DR High Availability Service provides continuous data replication of your physical and virtual server environments, ensuring you always have access to a current copy of your data, applications and operating systems.</td></tr>
<tr><td rowspan="4">SAP</td><td>Ariba</td><td>Ariba has a strong disaster recovery procedure, tested every 6 months though has never required to fail over to the backup data center. The RTO is 4 hours and RPO is 5 minutes. Please see the SaaS Technical Infrastructure Whitepaper for addiitonal details.</td></tr>
<tr><td>Fieldglass</td><td>None.</td></tr>
<tr><td>Hanna</td><td>SAP Hana Enterprise Cloud helps customers improve their Business Continuity requirements with High Availability (HA) , Disaster Recovery & Backup options.
High Availability (HA) - HA is achieved by failover to standby node
Disaster Recovery (DR) - Systems are configured in the secondary datacenter.
DR is an optional service that can be included as per customer's requirements</td></tr>
<tr><td>SuccessFactors</td><td>We maintain an N+1 approach for all equipment in the hosted cloud environment, so that there is never a single point of failure. All customer database backups are encrypted and streamed in a secure manner from the customer's "primary" data center to their "alternate" data center, allowing for a timely restoration of service in the event of disaster.
Based on the terms of the agreement, we will designate one of the data centers as the customer's "primary" data center, with an additional data center designated as the "alternate" for data redundancy and disaster recovery purposes.</td></tr>
<tr><td>VMware</td><td colspan="2">VMware IaaS Services
The following table provides common inherent disaster recovery risks and potential mitigation strategies.
<table>
<tr><th>RISK</th><th>Unmitigated Probability</th><th>Mitigation</th><th>Mitigated Probability</th></tr>
<tr><td>Participating agency's lack of a disaster recovery plan leads to</td><td>High Risk</td><td>Participating Entities are encouraged to develop a disaster recovery plan to mitigate against service</td><td>No Risk</td></tr>
</table>
</td></tr>
</table>

	service outage or data loss in the event of a disaster.		outage or data loss. In parallel, entities are encouraged to leverage vCloud Air data protection, vCloud Air Disaster Recovery, and other high availability services while a formal plan is written	
	Participating entity chooses inappropriate data center location leading to service degradation or outage.	High Risk	Participating entities are encouraged to choose datacenter(s) that is geographically proximate to their end users to maximize performance. In addition, location of disaster recovery data center should be geographically separated from primary data center.	Low Risk
	Participating entity fails to budget for and acquire appropriate DR technology leading to inability to recover from disasters.	High Risk	Participating entities are encouraged to include DR capabilities in their costs estimates for cloud deployments to ensure budget is available to acquire those services.	No Risk
	Participating entity fails to ensure cloud service SLAs (e.g. RPO & RTO objectives) meet their mission requirements leading to inadequate service recovery times and data loss.	High Risk	Participating entities are encouraged to review SLAs for each cloud service that they are interested in acquiring to ensure that they meet mission requirements. Care should also be taken to ensure service SLAs do not significantly exceed mission requirements to avoid unnecessary cost.	No Risk

VMWare AirWatch

	Providing a secure and stable product that mitigates vulnerabilities, reduces risk and quickly responds to the evolving threat landscape is considered a top priority. Following the guidelines established in NIST SP 800-30, regular risk and vulnerability assessments are performed against the production environment to identify, assess and remediate emerging threats. When potential vulnerabilities are discovered, we follow a documented procedure to prioritize and deploy necessary patches. •Vulnerabilities and threat-sources are identified by conducting interviews with various members of the Cloud Operations community and mapping data to the AirWatch business landscape. •We can provide additional information as conversations progress.
FireEye	Varies by service and customer deployment. Will be defined during engagement setup.
VirtueStream	Virtustream has built redundancy into all layers of the physical infrastructure in order to deliver SLAs up to 99.999% and mitigate any known risks. To further mitigate against the unknown, Core microVM's are designed for mission-critical workloads and include reserved compute capacity in a secondary datacenter and automatic storage replication to facilitate the ability to restore operations in the event of an outage at the primary data center.

8.15.3 Describe the infrastructure that supports multiple data centers within the United States, each of which supports redundancy, failover capability, and the ability to run large scale applications independently in case one data center is lost.

CA	APM	AWS datacenters provide redundancy and failover within a single AWS EC2 zone (i.e., a single geographic location). Professional Services would need to be engaged to provide multi-geo DR
	MAA	MAA service is currently available from one data center only.
	CA Agile	We run a hot/warm data center configuration and have the ability to quickly failover if required. Our data centers are ~1300 miles apart to ensure redundancy. We perform full system planned switch over testing at a minimum semi-annually.
	ASM	ASM core services run in one primary data center, and can fail over to the DR site if there is a catastrophic failure.
AODocs	As described elsewhere in this response, AODocs is built on Google Cloud Platform (AppEngine) and Altirnao does not manage this infrastructure.	
Virtru	We operate our infrastructure in multiple Availability Zones, and any given data center failure would not result in data loss.	
Salesforce	Customer Data for customers in Salesforce's Government Cloud is stored in two of our U.S. data center locations. Our service is collocated in dedicated spaces at toptier data centers. Salesforce's hardware is located inside of secure server rooms designated to Salesforce and separated by concrete walls from other data center tenants. Individual racks inside of the data center are secured with a lock. Specific racks are allocated for hardware supporting the Salesforce Government Cloud. Access to the racks supporting the Salesforce Government Cloud hardware is restricted to Qualified U.S. Citizens as described in the section above.	
ServiceNow	ServiceNow's data centers and cloud-based infrastructure have been designed to be highly available. All servers and network devices have redundant components and multiple network paths to avoid single points of failure. At the heart of this architecture, each customer application instance is supported by a multi-homed network configuration with multiple connections to the Internet. Production application servers are load balanced within each data center. Production database servers are replicated in near-real time to a peer data center within the same geographic region.	

	ServiceNow leverages this Advanced High Availability (AHA) architecture for customer production instances in several ways: •In the event of the failure of one or more infrastructure components, service is restored by transferring the operation of customer instances associated with the failed components to the peer data center. •Before executing required maintenance, ServiceNow can proactively transfer operation of customer instances impacted by the maintenance to the peer data center. The maintenance can then proceed without impacting service availability. This approach means that the transfer between active and standby data centers is being regularly executed as part of standard operating procedures – ensuring that when it is needed to address a failure, the transfer will be successful and service disruption minimized. See the "ServiceNow Security, Operations, and Compliance White Paper" included with this response for more information.
Docusign	Each component of our trusted platform - Hardware & Infrastructure, Systems & Operations, Applications & Access, and Transmission & Storage - undergoes tremendous security scrutiny. HARDWARE & INFRASTRUCTURE Three geo-dispersed, SSAE 16 audited datacenters Near real-time secure data replication and encrypted archival 365x24x7 on-site security Annual Business Continuity Planning (BCP) & Disaster Recovery (DR) testing Third-party penetration testing SYSTEMS & OPERATIONS Physically and logically separate networks Two-factor, encrypted VPN access Professional, commercial grade firewalls and border routers Distributed Denial of Service (DDoS) mitigation Active monitoring and alerting APPLICATIONS & ACCESS Formal code reviews and vulnerability mitigation by third parties Application level Advanced Encryption Standard (AES) 256 bit encryption Key Management & Encryption Program Enterprise-class malware protection Digital audit trail Multiple authentication mechanisms TRANSMISSION & STORAGE Secure, private SSL 256 bit viewing session Anti-tampering controls Signature verification of signing events Unalterable, systematic capture of signing data Digital certificate technology Customer configurable data retention program

QTS	QTS cloud utilizes alternate telecommunications services from both TW Telecom and NTT America that reduces the likelihood of experiencing a single point of failure. QTS's failover facilities in RIC1 and ATL1 are a carrier-class and carrier-neutral datacenter with multiple Internet Service Providers. QTS-FC can establish connectivity with another service provider with 24 hours in the event of an unrecoverable catastrophic connectivity failure of QTS-FC's primary/secondary provider.	
SAP	Ariba	Ariba has implemented two sites within each region. In North America the sites are currently located in San Jose, California and Sterling, VA. In Europe the sites are located in St. Leon-Rot, Germany and Amsterdam, Netherlands. The act of failing over from one site to another has a design goal for its Recovery Time Objective (RTO) of no more than four hours. The design goal for the Recovery Point Objective (RPO) is five minutes. Disaster recovery options are included for all Ariba Cloud Services. In the event of a fail-over to the disaster recovery site, no customer changes are required as all URLs that customers use to reach the applications will continue to work. Ariba will notify customers via their email addresses in the event of unplanned downtime. Internally, Ariba uses a documented system recovery plan that outlines the approach and steps for recovering the applications. This document defines roles and responsibilities in the event of disaster: Local Ariba staff maintains the hardware remotely. Ariba maintains the application software. Processes are in place to keep database and fileservers in sync between primary and backup data centers. The failover process of all parts of the infrastructure is automated. In the event of a catastrophe, Ariba will declare the primary data center "down" and locally the script will be run to switchover and start the applications at the remote data center. Ariba tests power outage backup scenarios and the Disaster Recovery Plan on a periodic basis to ensure it is up-to-date, successful, and effective.
	Fieldglass	We host and manage the Fieldglass system within secure Internet data centers provided by CenturyLink in Elk Grove, IL, and our disaster recovery center provided by Equinix in San Jose, CA. Both are managed by Server Central which is a Tier 4 hosting provider and a Tier 1 data provider (see the note below). All systems are ""mission-critical loads"" supported by IDC Redundant Power Management System (UPS, generators etc.). Note: Data centers can be classified by tiers, with Tier 1 being the most basic and inexpensive, and Tier 4 being the most robust and costly. According to definitions from the Uptime Institute and the latest draft of TIA/EIA-942 (Telecommunications Infrastructure Standard for Data Centers), a Tier 1 data center is not required to have redundant power and cooling infrastructures. It needs only a lock for security and can tolerate up to 28.8 hours of downtime per year. In contrast, a Tier 4 data center must have redundant systems for power and cooling, with multiple distribution paths that are active and fault tolerant. Furthermore, access should be controlled with biometric readers and single-person entryways, gaseous fire suppression is required, the cabling infrastructure should have a redundant backbone, and the facility can permit no more than 0.4 hours of downtime per year. Tier 1 or 2 is usually sufficient for enterprise data centers that primarily serve users within a corporation. Financial data centers are typically Tier 3 or 4 because they are critical to our economic stability and, therefore, must meet

		higher standards set by our government. Public data centers that provide disaster recovery/backup services are also built to higher standards.
	Hanna	Infrastructure setup: * Standby SAP HEC systems at DR failover site will be shutdown / not useable during regular operations. * WAN connectivity & special requirements (e.g. acceleration services) fall into the responsibil-ity of the customer. * Customer must have independent network connections to both DR sites. * All DR-relevant systems are going to be installed according to the Adaptive Computing (AC) principle (virtual hostnames + virtual IP addresses HSR will be used to replicate data from Primary to DR site for HANA solutions, similarly Sybase Replication Server (SRS) will be used to replicate data from Primary to DR site for ASE based solutions. For more information, please refer to attached Business Continuity document
	SuccessFactors	Our infrastructure architecture is designed with high availability in mind, and engineered for resiliency. All major components are redundant, including power, HVAC, fire suppression, and the physical components of our network. Production data centers have strict access controls, and are continuously staffed and monitored to help prevent acts of sabotage or vandalism. All production data centers are ANSI/EIA/TIA-942Tier III/IV facilities, and are ISO 27001 certified. Production data centers are also geographically dispersed to help prevent a single event from affecting more than one data center. In the event a production data center has an outage we failover to an alternate data center in the same geographic region to minimize impact to customers. Our Cloud Operations teams are also geographically dispersed, working in offices in the US, Europe, South America, and India. Should an office be impacted by an environmental event or pandemic, other offices can continue operations. Aspects of the plan are described in the SOC reports, Disaster Recovery Plan ("DRP") and Business Continuity Plan ("BCP") solutions are dependent on several factors. The customer may be responsible for parts of the recovery/continuity activities
VMware	VMware IaaS Services VMware offers several technologies to provide redundancy, failover capability and the ability to run large scale applications independently in case one data center is lost. vCloud Air is built upon infrastructure that is architected for High Availability leveraging proven vSphere High Availability (HA), vSphere vMotion, and VMware Distributed Resource Scheduler (DRS). These technologies allow participating entities to migrate live workloads and/or automatically restart VMs in the event of host maintenance or unexpected issues. These technologies also maintain a consistently high level of performance for all tenants. VMWare vSphere vMotion enables migration of live VMs to transfer your workloads during maintenance, without downtime. Unlike other cloud providers, VMWare ensures that tenants are not impacted by standard maintenance. VMware performs vMotion migrations for maintenance behind the scenes for its tenants in vCloud Air during maintenance windows without disrupting tenant applications. vMotion is also used to seamlessly migrate VMs from an on-premises environment to vCloud Air and back. Today, vCloud Air is one of only a few major cloud vendors that uses live migration to do maintenance. This capability will enable NASPO participating entities to perform live migrations to move thier applications to and from the cloud for maintenance and other purposes. This	

	technology inherently prevents the lock-in experienced when migrating to cloud services offered by others. VMware Dynamic Resource Scheduler continuously monitors CPU and memory utilization across a cluster of vSphere hosts, allocating resources among VMs and rebalancing performance during high-volume peak times. This is performed 24x7 within the VMware vCloud Air environment. VMware vSphere High Availability delivers the availability required by most applications running in VMs, independent of the operating system and application running in it. Whether participating entities leverage Microsoft Windows or Linux; off-the-shelf or custom developed application; single VMs or many, HA provides uniform, failover protection against hardware and operating system outages within vCloud Air. HA can: • Monitor VMware vSphere hosts and VMs to detect hardware and guest operating system failures. • Restart VMs on other vSphere hosts in the cluster without manual intervention when a server outage is detected. • Reduce application downtime by automatically restarting VMs upon detection of an operating system failure. Other cloud providers require you to build availability in to your application. In the best case scenario, this is as simple as including a load balancer in front of multiple VMs in the same tier to achieve basic high availability. However, often the technologies of other cloud service providers requires a complete redesign of the hosted application, and often network devices such as load balancers are offered at an additional cost, unlike vCloud Air. vCloud Air was built to run hosted applications as-is, providing availability down to a single VM instance, and balancing resources across multiple tenant needs with DRS. Unlike other clouds, with vCloud Air and vCGS, participating entities are not required to rebuild thier application to get the flexibility and agility that cloud can provide. Of course, vCloud Air customers usually do not just stop at moving applications to vCloud Air. Once in the cloud they start to explore features like our Advanced Networking Services and using APIs, automation, and CI/CD tools to deliver services faster. And, where it makes sense, customers do look at application redesigns as well, but with vCloud Air it is not because they must redesign to ensure the application is always available. VMWare AirWatch AirWatch features active-passive configurations for high availability and redundancy with all components made to failover with minimal downtime. Load balancing capabilities are deployed across multiple data centers to ensure immediate server pick up, ensuring zero end user downtime. AirWatch also incorporates replication technology featuring SQL log shipping or network SAN byte replication to prevent data loss.
FireEye	Varies by service and customer deployment. Will be defined during engagement setup.
VirtueStream	Virtustream's U.S. based data centers are located in Washington, DC, Las Vegas, and San Francisco. All data centers meet the highest industry standard in terms of operational protocol and have redundancy built into all layers of the physical infrastructure. Core microVM's, which are used for mission-critical workloads, provide reserved compute capacity and automatic storage replication so that these systems can be failed over to a secondary data center and have access to the compute capacity required in the event of a catastrophic outage at the primary data center.

8.16 Solution Administration

8.16.1 Ability of the Purchasing Entity to fully manage identity and user accounts.

CA	APM	Customer has full control over all user accounts

	MAA	CA MAA provides user management self-service to customers to manage their own accounts and create accounts for other users.
	CA Agile	The customer is responsible for managing the lifecycle of all user accounts.
	ASM	The Purchasing Entity can manage their account and create sub-accounts within ASM.
Google	Comply	
AODocs	Comply	
Virtru	Virtru does not have an identity system. We federate authentication to Oauth and Email loop verification.	
Salesforce	Identity Management Logon is form-based. When users log into the Salesforce application, they submit a username and password, which are sent to Salesforce via an TLS-encrypted session. Security features are developed by Salesforce and built into the application. Third-party packages are not used for development or implementation of security internal to the application. In addition, single sign-on and two-factor authentication may be used to authenticate users. Some organizations prefer to use an existing single sign-on capability to simplify and standardize their user authentication. You have two options to implement single sign-on—federated authentication using Security Assertion Markup Language (SAML) or delegated authentication. Federated authentication using Security Assertion Markup Language (SAML) allows you to send authentication and authorization data between affiliated but unrelated Web services. This enables you to sign-on to Salesforce from a client application. Federated authentication using SAML is enabled by default for your organization. Delegated authentication single sign-on enables you to integrate Salesforce with an authentication method that you choose. This enables you to integrate authentication with your LDAP (Lightweight Directory Access Protocol) server, or perform single sign-on by authenticating using a token instead of a password. You manage delegated authentication at the profile level, allowing some users to use delegated authentication, while other users continue to use their Salesforce-managed password. Delegated authentication is set by profile, not organization wide. You must request that this feature be enabled by Salesforce. Salesforce can be configured to utilize Active Directory directly via Delegated Authentication, or indirectly via Federated Identity using either SAML 1.1, or SAML 2.0. Additionally your users can be loaded from information drawn from your Active Directory servers and modifications made in Active Directory can be propagated into Salesforce. Customers can use their own SAML Identity Provider, or license one directly from Salesforce with our Identity Connect product. User Accounts All users and application-level security are defined and maintained by the organization administrator, and not by Salesforce. The organization administrator is appointed by the customer. An organization's sharing model sets the default access that users have to each other's data. There are four sharing models: Private, Public Read Only, Public Read/Write, and Public Read/Write/Transfer. There are also several sharing model elements: Profiles, Roles, Hierarchy, Record Types, Page Layouts, and Field Level security.	
ServiceNow	Customers manage their own instances, including assigning users, defining user roles and profiles, and administrating the system. ServiceNow does not have access to the Customer's instances. The ServiceNow wiki has all ServiceNow documentation available.	

Docusign	Yes, DocuSign allows the purchasing entity to mange identities and user accounts. DocuSign for Enterprise is customizable to meet the administrative needs of the largest organizations. Full administration rights give you total control over document custody and retention policies, how signers sign or adopt signatures, user authentication and more. The branding tools ensure recipients can easily identify documents from your organization.
QTS	24x7x365 Operations Staff - Let QTS provide the expertise and experienced staff to monitor and manage your data center facility. Never again worry about staff turnover or whether your technologists are current with data center best practices.
SAP	Hanna: Yes
VMware	VMware IaaS Services VMware management infrastructure requires 2-factor authentication and multiple layers of access control. vCloud Air customers have the ability to provide access to their designated users. User account management is maintained by the customer. control. vCloud Air customers have the ability to provide access to their designated users. User account management is maintained by the customer. VMWare AirWatch The Purchasing entity has the ability to fully manage identity and user accounts for administrators and end users through the web console. Customers can optionally integrate with AD/LDAP to inherit your existing structure and policies.
FireEye	User identity and account settings are controlled within the administration sections of the FireEye cloud solutions.
VirtueStream	Virtustream can provide solution for managed solution for Active Directory or LDAP. As standard, we provide support for managing the VM itself and all OS support. However, our typical use case is, customer manages the users and related activities, as Virtustream might not be aware of internal HR elements of User Management.

8.16.2 Ability to provide anti-virus protection, for data stores.

CA	APM	AWS provides protection/virus scanning for data at rest
	MAA	Logical security is provided by ClamAV Antivirus.
	CA Agile	We have ClamAV installed on all Linux hosts and TrendMicro for Windows hosts.
	ASM	Logical security is provided by ClamAV Antivirus.
Google	Comply	
AODocs	N/A	
Virtru	AlienVault IDS is used to perform virus and vulnerability scans.	
Salesforce	Salesforce runs antivirus software on the production systems that store, transmit or process customer information. The Anti-virus scans host filesystems (not customer data). The antivirus software checks for virus definition updates daily. Other controls are also used to address malware such as hardening the Operating System of our servers, firewall configuration to ensure only required ports are open and all others denied, and use of intrusion detection systems. Access to these systems is restricted to authorized personnel and all these systems, as well as the host platforms, are monitored in real time through a security monitoring system. The application only accepts http and https traffic, but Salesforce does not restrict the file types users can upload. Salesforce does not modify or clean any customer data; the system stores the information provided in an encoded format within the database. It is recommended that customers run updated antivirus and antimalware solutions to help mitigate these threats. The production system receives inbound mail as part of the workflow functionality, but this does not pose any threat to our network, application, or users. No code in the email can be executed or transferred,	

	eliminating the malicious software risk. Email sent from the Salesforce system is not currently scanned for viruses.
ServiceNow	If Customers want to schedule an antivirus software scan on certain computers after a pre-defined number of days, Customer would define a model-based plan with a duration-based maintenance schedule. This would do the scan automatically to those models defined in the Planned Maintenance area.
Docusign	Yes, DocuSign maintains enterprise-class malware protection.
QTS	Yes - 24x7x365, dependable and detailed support
SAP	Hanna Yes
VMware	VMware IaaS Services Anti-virus software is installed on all development, domain and production hardware devices owned and operated by VMware, which hold company data, passwords, or keys. These devices maintain the most recent version of the anti-virus software signature file. VMWare AirWatch AirWatch has installed a best-in-class, continuously-updated anti-virus suite on servers in the SaaS environment
FireEye	FireEye employs a multi-layered, continuously monitored and engaged set of active defenses to provide anti-virus protection for customer data stores that both meet and exceed traditional approaches. FireEye, and our customers, not only are prepared to reactively withstand attacks from known virus vectors, but since FireEye and our MVX technology is literally, continuously, and securely detonating viruses and other advanced malware on the way to our customer's data stores, FireEye proactively defends from zero day and other emergent attacks as they happen.
VirtueStream	Virtustream offers Anti-Virus protection based on per virtual machine, per month charge.

8.16.3 Ability to migrate all Purchasing Entity data, metadata, and usage data to a successor Cloud Hosting solution provider.

Carahsoft will work with each Participating Entity to develop a cost effective plan to assist in the migration and implementation of their data into the new service that has been selected.

8.16.4 Ability to administer the solution in a distributed manner to different participating entities.

Carahsoft will view each Participating Entity as a separate customer and privileges can be assigned for control access even within the individual services.

8.16.5 Ability to apply a participating entity's defined administration polices in managing a solution.

Each Participating Entity will have the ability to work with Carahsoft and the Service Provider to identify defined administration policies to mangage the solution.

8.17 Hosting and Provisioning

8.17.1 Documented cloud hosting provisioning processes, and your defined/standard cloud provisioning stack.

CA	APM	CA SaaS Ops has a well defined Service Introduction and update process, including review boards, staged rollouts and followups to ensure service integrity. Our cloud provisioning stack is tied to AWS EC2 services, and includes S3 and RDS for storage; RHEL instances for the applications; route 53 DNS services; cloudfront for monitoring; and ELB for load balancing

	MAA	Automation tools are used to install and configure MAA software on CA infrastructure. SOP documents are used by CA internally.
	CA Agile	All new systems should be provisions according to our baseline standards and we use configuration management tools to ensure all systems are created with the same standards.
	ASM	Automation tools are used to install and configure ASM software on CA infrastructure. SOP documents are used by CA internally.
Google	Google has administrative document and Google Deployment Guides accessible on the web.	
AODocs	This is not applicable to Google.	
Virtru	Ubuntu AMIs provisioned using terraform and configured by Ansible	
Salesforce	Cloud Hosting and Provisioning Salesforce's deployment model is a "public" cloud infrastructure, as defined by NIST 800-145. In the Salesforce Government Cloud, an agency dynamically provisions computing resources over the Internet on our multi-tenant infrastructure. This is a cost effective deployment model for agencies as it gives them the flexibility to procure only the computing resources they need and delivers all services with consistent availability, resiliency, security, and manageability. Salesforce provides market leading PaaS and SaaS solutions and is a multitenant cloud-based subscription service. Multi-tenant cloud solutions provide a single, shared infrastructure, one code base, one platform that is all centrally managed, with platform-based API to support all integration traffic, and multiple release upgrades included as part of the subscription service. Multi-tenancy and the Cloud Computing model remove unneeded tasks from the process of delivering, managing, and integrating software. Salesforce customers will not need to maintain any hardware or software. Without multiple versions to support, integrations don't break during updates; they are simply updated automatically. As a result, both the initial integration and its continued maintenance are simplified. More resources can be focused on creating a better product, with a faster cycle of innovation, instead of having to manage the complexity of many different versions to support a vast installed base. Salesforce's position as an online service enables us to roll out all levels of improvement, from patch releases to major upgrades, that are largely transparent to the end users. When a bug is fixed and tested, it is rolled out to the application as part of regular maintenance; the nature of the service prevents special patches and code branches for individual customers, so all fixes can potentially benefit all customers. The Salesforce Services is delivered using a world-class data center infrastructure. Each customer's org is hosted from a primary and secondary production data center, with near real-time replication occurring between the two sites. Salesforce is a pure multi-tenant web application. No software or infrastructure is required by the customer other than a computer, browser and internet connection or a mobile device. User Administration and ProvisioningUser provisioning and management is performed by the customer through the Salesforce Administrative Setup environment. Users, their profiles, permissions and passwords may be managed, edited, activated and deactivated as needed by those with appropriate permissions. An administrator with appropriate privileges can manage session timeout, password policies, IP range login restrictions, delegated authentication/SSO, and requirements as part of this process. On first time login or password reset request, users are required to change their passwords to gain access.	
ServiceNow	ServiceNow includes all documentation on the wiki at wiki.servicenow.com.	
Docusign	DocuSign hosts customer accounts in its own data centers managed by DocuSign. Upon a new contract executed with a customer, DocuSign provisions a customer account based on the	

	contract terms. A designated point of contact becomes the default primary administrator who then adds additional users and other admin tasks. DocuSign's cloud stack is defined in architecture documents available under separate confidential disclosure.	
QTS		
SAP	Ariba	Our solutions are offered and delivered in a true subscription-based model and shared service (multi-tenant) offering. There is no software to install, no hardware to buy, no maintenance or support costs and no need to hire consultants or tech specialists to run the system. We deploy and manage the infrastructure. Customers only need a web browser for access. Subscriptions include system maintenance, automatic upgrades, enhancements and application of service packs, Level 1– 3 help desk support, professional services and best practices built directly into the application.
	Fieldglass	Fieldglass maintains its own platforms and follows a mature change control process for introducing new systems to the hosted environments.
	Hanna	The Managed Service includes the following: • Infrastructure operations management: monitoring, patching, software updates & maintenance up to the OS Layer • OS management: monitoring, patching, updates, and maintenance of the specific OS • Network and system administration • HANA database platform operations includes: space management revision management , security management , hardware configuration management, backup & recovery, change management coordination • Health check services, proactive monitoring, capacity management • SAP Technical Application Basis Operations (incl. SAP Basis) • Monitoring • Troubleshooting – Incident Management Level 2 and 3 • Patch Management • Housekeeping • Backup/Recovery
	SuccessFactors	We offer a cloud based solution. Our application is standardized on the J2EE technology stack with the majority of our software written in industry-standard software programming languages, such as Java. We also make extensive use of Web 2.0 technologies, such as AJAX and Flash, for improved usability and performance and to deliver a rich and highly interactive experience. Our hardware consists primarily of industry standard web servers, application servers, database servers and storage and networking equipment. Customers share the network security infrastructure, web servers, application servers and database instance, and each customer has their own set of database tables that are logically partitioned in the database containing its own unique database schema. Each company instance can be completely exported out of the database without affecting any other customer. The application utilizes the JAVA and J2EE industry standards. Integration is supported through .CSV, XML and web services standards. The application is portable to any platform and is deployed on Apache (Solaris) Web Servers, JBOSS Application Servers, and Veritas High Availability Cluster Servers, and utilizes Cisco Networking.
VMware	VMware IaaS Services An interface that allows users to select from a catalog of pre built OS images and allows them to provision on the fly.	

	VMWare AirWatch AirWatch uses industry recognized tools and follow best practices to deploy, configure, and maintain server images. We do not apply customer-supplied templates and do not share templates with customers. Our Information Security team identifies applicable security standards and the AirWatch Server Team creates a secure baseline image for deployment throughout the SaaS environment. Due to FOIA restrictions, additional information regarding capacity planning and image creation/safeguarding cannot be disclosed at this time.
FireEye	This is not applicable as each of FireEye's offerings are classified as SaaS.

8.17.2 Provide tool sets at minimum for:

1. Deploying new servers (determining configuration for both stand alone or part of an existing server farm, etc.)

CA	APM	New servers are predefined by the CA SaaS Ops toolchain, and automated using AWS tooling to be able to bring up/down servers on demand
	MAA	Same as above.
	CA Agile	We utilize configuration management tools to ensure consistent configuration across our servers.
	ASM	Same as above.
Google	1. This is not applicable to Google. Capacity planning and server deployment is fully managed by Google. 2. This is not applicable. With the Google IaaS solutions all server images are provided by Google. 3. With respect to the SaaS offfering, Google Apps, if customers have not selected the Google Apps Unlimited option which offers unlimited storage, they have options to upgrade. With respect to the PaaS/IaaS offering, Google Cloud Platform, storage space is allocated dynamically based on actual usage demand. 4. SaaS, Google Apps includes numerous administrative tools to monitor end user and administrator activites."	
AODocs	This is not applicable.	
Virtru	AMIs provisioned using terraform and configured by Ansible to include all configuration parameters	
Salesforce	This is not applicable. These services while applicable to IaaS are not applicable to PaaS/SaaS where all of the infrastructure is managed by Salesforce as the Cloud Service Provider. These services are included and managed as part of the Salesforce subscription service and not directly exposed to the customer. The multitenant architecture and secure logical controls address separation of customer data. There are no dedicated servers used for individual customers. The Salesforce Services infrastructure is divided into a modular architecture based on "Instance". Each Instance is capable of supporting several thousand customers in a secure and efficient manner. Services are grouped within each Instance; with app, search, and database elements contained. There are appropriate controls in place to ensure that any given customer's org (application) is not compromised. The service has been designed to accomplish this and is robustly tested on an ongoing basis by both Salesforce and its customers. An instance consists of a database instance run on clustered database servers and physical storage subsystems. Each server has been allocated a different volume group so it can fail over to its backup server within the instance independently of the others. As scalability needs dictate,	

	additional database instances can be brought online (the application already provides for this). For additional server capacity, one or more databases could be moved onto its own database server.	
ServiceNow	ServiceNow has read and understands this requirement. ServiceNow supports only a SaaS environment so there is no on-premise offering.	
SAP	Ariba	Operating systems when installed through default means and with default settings are typically not secure and often include applications and services not required. Ariba has standardized operating systems' installations based on best practices. Ariba servers are configured with just the applications and services required to run the server as designed. Services not required are disabled and binary files not required for operation are removed, which reduces the total number of vulnerabilities a system may have. Ariba standardized installation process also ensures that all servers of the same type are configured exactly the same, utilizing a process that initiates an upgrade to system binaries across all systems. Based on the system type, the configuration will remain the same. If one server type needs to receive a patch for a vulnerable binary file, that patch is pushed to all systems of that particular server type. If that binary exists on all systems, it is patched across all systems. Patches are then included in the build process as well so that future systems built are in compliance with security standards. Ariba uses this configuration process to 'harden' the operating system prior to implementing additional controls as detailed below.
	Fieldglass	Fieldglass uses group policy to ensure the configuration of all servers match our security requirements.
	Hanna	HEC is a private cloud offering where servers configurations are discussed and approved by customer prior to deployment.
	SuccessFactors	We apply hardening in line with ISO 27k standards and audit key areas in the SOC 2 Type 2 report. Audit reports are available to customers and prospects upon completion of an NDA.
VMware	VMware IaaS Services vCloud Hybrid Service provides an interface that allows users to select from a catalog of pre-built OS images and allows them to provision on the fly. vRealize Automation is the next level for provisioning, delivering, and managing IT services on VMware vSphere infrastructure as well as VMware vCloud Air all with a unified management experience. It provides governance and blueprints to deliver services from on premise into vCloud Air. Customers can integrate vCloud Air with vRealize Automation. In this setup, users access vCloud Air primarily through the vRealize Automation service catalog which handles authentication to the service itself. vRealize Automation supports VMWare AirWatch AirWatch uses industry recognized tools and follow best practices to deploy, configure, and maintain server images. We do not apply customer-supplied templates and do not share templates with customers. Due to FOIA restrictions, additional information regarding capacity planning and image creation/safeguarding cannot be disclosed at this time.	
FireEye	This is not applicable as each of FireEye's offerings are classified as SaaS.	
VirtueStream	Virtustream offers on-demand self-service portal where State of Utah can deploy new servers as stand-alone or part of a server farm.	

2. Creating and storing server images for future multiple deployments

CA	APM	Servers are brought up on demand

	MAA	Same as above.
	CA Agile	We utilize configuration management tools to ensure consistent configuration across our servers.
	ASM	Same as above.
Virtru	Provisioning system automatically persists all past AMIs for ability to roll-back	
Salesforce	This is not applicable. These services while applicable to IaaS are not applicable to PaaS/SaaS where all of the infrastructure is managed by Salesforce as the Cloud Service Provider. These services are included and managed as part of the Salesforce subscription service and not directly exposed to the customer.	
ServiceNow	ServiceNow has read and understands this requirement. ServiceNow supports only a SaaS environment so there is no on-premise offering.	
SAP	Ariba	Ariba has standard 'realms' which are default versions of the various configurations the Ariba on-demand products can be setup for each customer with one test and one production instance. Ariba maintains all hardware, software, realms and entitlements taking the burden off our customers and suppliers whilst providing a platform to configure to each company's needs and business processes
	Fieldglass	Fieldglass uses virtual servers within our hosted environments uses the hardening configurations to maintain the right level of security.
	Hanna	HEC is a private cloud offering where servers configurations are discussed and approved by customer prior to deployment.
VMware	VMware IaaS Services We also allow for template and gold master images to be stored on-premise and deployed to the cloud as well as storage of templates and master images in vCloud Director catalogs in in vCloud Air VMWare AirWatch Our Information Security team identifies applicable security standards and the AirWatch Server Team creates a secure baseline image for deployment throughout the SaaS environment. Due to FOIA restrictions, additional information regarding capacity planning and image creation/safeguarding cannot be disclosed at this time.	
FireEye	This is not applicable as each of FireEye's offerings are classified as SaaS.	
VirtueStream	Virtustream offers server images, templates, or other methods (OVF and blueprints) for multiple deployments as part of standard solution.	

3. Securing additional storage space

CA	APM	AWS EC2 storage is elastic, and can be expanded on demand
	MAA	Virtual storage can be added when needed.
	CA Agile	We have redundant systems for all critical infrastructure and have the ability to add additional storage if deemed necessary.
	ASM	Additional storage is added manually.
AODocs	AODocs storage is based on Google Apps Drive storage and with respect to the SaaS offfering, Google Apps, if customers have not selected the Google Apps Unlimited option which offers unlimited storage, they have options to upgrade.	
Virtru	New hardware added at Cloudant	
Salesforce	Salesforce provides extensive storage capabilities. Storage is divided into two categories: file storage and data storage. File storage includes files in attachments, the Documents tab, the Files tab, the File field, Salesforce CRM Content, Chatter (including user photos), and Site.com assets. Data storage includes the following entities/records stored within the Salesforce application: Accounts, Article types, Article type translations, Campaigns, Campaign Members, Cases, Case	

	Teams, Contacts, Contracts, Custom objects, Email messages, Events, Forecast items, Google docs, Ideas, Leads, Notes, Opportunities, Opportunity Splits, Orders, Quotes, Quote Template Rich Text Data, Solutions, Tags: Tag applications, Tags: Unique tags, and Tasks. For file storage, Unlimited Edition is allocated a per-user limit multiplied by the number of users in the organization plus an additional per-organization allocation. For example, an Unlimited Edition organization with 600 users receives 1,211 GB of file storage, or 2 GB per user multiplied by 600 users plus an additional 11 GB. For data storage, Unlimited Edition is allocated either 1 GB or a per-user limit, whichever is greater. For example, an Unlimited Edition organization with 10 users receives 1 GB because 10 users multiplied by 20 MB per user is 200 MB, which is less than the 1 GB minimum. Additional storage can be purchased, or files can be exported and archived outside of Salesforce, thus freeing up file storage space.	
ServiceNow	ServiceNow has read and understands this requirement. ServiceNow supports only a SaaS environment so there is no on-premise offering.	
QTS	Services that scale to meet your web and IT infrastructure needs - QTS offers space options from single cabinets to multi-rack cages to private suites. Coupled with configurable primary and redundant power options to run your infrastructure, QTS Colocation services can be scaled to support your near term growth requirements and future expansion.	
SAP	Ariba	We carefully monitor all network interfaces. Internally we are well below capacity on our most congested interconnects. To the internet we use Border Gateway Protocol to peer with redundant Internet Service Provider's and manage the bandwidth accordingly.
	Fieldglass	As a software-as-a-service (SaaS), Fieldglass automatically and transparently handles the scaling and redundancy for customers based on SLAs governing performance and availability. Fieldglass monitors application servers, database servers, bandwidth, and infrastructure for average and maximum utilization with Orion. Current utilization averages approximately 20 percent across all components with a goal of scaling the component vertically or horizontally (depending on the specific component) upon reaching a 60 percent threshold). All systems are scalable either horizontally or vertically to handle capacity requirements. This includes but is not limited to web servers, database servers, and storage.
	Hanna	HEC is a private cloud offering where servers configurations are discussed and approved by customer prior to deployment.
VMware	VMware IaaS Services Additional storage can be purchased and provisioned in 48 hours. VMWare AirWatch Our Information Security team identifies applicable security standards and the AirWatch Server Team creates a secure baseline image for deployment throughout the SaaS environment. Due to FOIA restrictions, additional information regarding capacity planning and image creation/safeguarding cannot be disclosed at this time.	
FireEye	This is not applicable as each of FireEye's offerings are classified as SaaS.	

4. Monitoring tools for use by each jurisdiction's authorized personnel – and this should ideally cover components of a public (respondent hosted) or hybrid cloud (including Participating entity resources).

CA	APM	all SaaS based instances are monitored by CA SaaS Ops. With Hybrid deployments, customers can manage the on premise components of the deployment using their own tooling or CA products
	MAA	MAA is monitored internally as well as externally using multiple tools recognized within industry.
	CA Agile	Access to monitoring tools is provisions according to the principle of least priviledge and is only granted based upon business need.
	ASM	ASM uses Nimsoft Monitor, third-party open source monitoring tools, and ASM itself to monitor the health of ASM internal services and servers.
AODocs	AODocs includes numerous administrative tools to monitor end user and administrator activites.	
Virtru	Dtrace, CloudWatch, CloudTrail, Logstache, ElasticSearch, Kibana, DataDog	
Salesforce	Trust.salesforce.com is the Salesforce community's home for real-time information on system performance and security. On this site you'll find: • Live and historical data on system performance • Up-to-the minute information on planned maintenance • Phishing, malicious software, and social engineering threats • Best security practices for your organization • Information on how we safeguard your data System Overview In addition to our Trust site (http://trust.salesforce.com/trust/status), you will also have access to a System Overview, which will help Salesforce customers monitor performance and usage of their own Salesforce org. This overview includes: Schema - # and % of custom objects and data storage Business Logic - # and % of Rules, Apex triggers and classes, as well as % of code used Licenses API Usage - # and % of requests in the last 24 hours User Interface - # and % of custom apps, sites, flows, custom tabs and pages Portal The above list is of all the possible metrics that Salesforce customers may have in their system overview.	
ServiceNow	ServiceNow has read and understands this requirement. ServiceNow supports only a SaaS environment so there is no on-premise offering.	
QTS	Alert Logic's Threat Manager Intrusion Detection System (IDS) and Vulnerability Scanning functionality are designed to monitor, detect, report and alert on adverse security issues on behalf of our customers. Within this process there are a number of both automated and manual processes which are supported by our SIEM software ('The Expert System') as well as our Network Security Analysts in our Security Operations Center (SOC). Threat Manager is the Alert Logic IDS and VA scan product. It includes the physical or virtual appliances and software tools used to analyze the customer's infrastructure and monitor that infrastructure for attacks. ActiveWatch is the managed aspect of Threat Manager, providing 24 x 7 monitoring and incident response operations from the Alert Logic SOC. Threat Manager's Expert System identifies valid security events and suppresses false positives through a patented multifactor correlation process. Every security event monitored by its global network of threat sensors is analyzed in real time. When the Expert System determines that a set of events comprise a valid security threat, an incident is created and escalated according to severity via email or through an Alert Logic Network Security Analyst. This approach dramatically	

	reduces false positives and keeps analysts and customers focused on real, actionable incidents. In addition, Alert Logic's security research team continuously monitors threat data and tunes the Expert System to respond to the most current threats.	
SAP	Ariba	Within our solution, specific logging takes place that is viewable by the customer administrator or their designee. Audit logs produced through use of the solution are considered customer data and are maintained within the customer's instance of the database. These logs are retained so long as the customer has an active contract with us. As a user control consideration, customers are responsible for monitoring the proper entry of data to the solution and reviewing reports generated by the system.
	Fieldglass	Fieldglass has a comprehensive set of performance monitoring tools in place. Some tools are built in the application and some are external. The Fieldglass application captures every page hit and the time it takes to respond. It captures the server response time and the client rendering time separately. The average page times are available to be seen by privileged users through the application. The user can drill down to the hour or minute or a single request for analysis. The information can be displayed by time range for all users, by company, or even for an individual user. Orion Network Monitoring watches more than 1,000 different points of interest on the production infrastructure. These monitors include, but are not limited to, the following: CPU, Memory, I/O, Capacity and Synthetic Transactions. These monitors along with our custom application performance monitors are used to produce and comply with customer SLA requirements. Fieldglass also uses Splunk Enterprise Security for event/audit log collection and correlation. Events and logs are retained online for 90 days and offline for two years. Alerts are generated and reviewed as they occur.
	Hanna	SAP HEC uses Solution Manager for monitoring the infrastructure end to end.
	Hybris	SAP Hybris offers continuous 24/7 systems monitoring in-place, which automatically notifies you, SAP Hybris support and optionally your designated implementation partner in the event of any monitored system problem. Tools used for monitoring include HP Sitescope and Nagios. This service ensures quick response times to emergency problems. Standard monitors are in place for basic site availability. Customer can utilize additional 3rd party monitoring services should it wish to add additional monitoring. Upon request, monthly or quarterly reviews are offered to review performance over the period. When a system problem occurs, in addition to monitor alerts sent to the customer, SAP Hybris support may send emails to a designated customer notification email address to provide status, updates or further detailed information. In addition, a support ticket would be created which would include such information.
	SuccessFactors	The application logs the following for every transaction: Event/transaction Time, Transaction ID, Event/transaction Type, Event/transaction Status (Result of the event; if failure, includes reason), Object Attributes (Describes the object affected by the event), Originator User ID (ID of the user who initiated the event or action), Subject ID, Process User ID, Account Number, Transaction Specific Elements. The application audits changes to the major components. Examples of this are goal auditing and document auditing. The audit trail includes who made the change, the date of the change and the ability to see the data as it existed at

		that point in time. The data in the audit log can be viewed with appropriate permissions. We also provide an optional Audit Framework for additional audit logging capabilities. All audit logs within the application are accessible only by customers. Therefore, the review of application audit logs as well as retention periods for the application audit logs are the customer's responsibility, and can be determined as per requirements
VMware	VMware IaaS Services The vCloud Hybrid Service infrastructure, including the top layer management stack, the customer management stack and the computing/storage/network hardware are monitored for availability, capacity and performance. Customers are responsible for monitoring their own VMs (OS, apps). Customers can use on premise monitoring tools to manage and monitor their applications and OSes over VPN and direct connect. VMWare AirWatch The AirWatch Cloud Operations team monitors the SaaS environment. AirWatch follows the Fault, Configuration, Accounting, Performance, and Security (FCAPS) model to monitor the SaaS environment. •We have configured the system to notify support personnel of any issues with key performance items •Because the solution is built on industry-standard ASP.NET architecture, it integrates into existing management and monitoring tools. Administrators can configure log data storage to destinations such as Windows Event Viewer, SNMP traps, syslog, SMTP email alerts, etc. The solution also integrates directly with Microsoft SCCM. The communication layer includes a complete infrastructure for API integration to third parties as well as a rich set of existing APIs, web services, single sign on and authentication protocols. Integrate with security information and event management (SIEM) solutions for enhanced logging of events occurring in the console. Administrators can view events, filter by event type, category and module, and export events. Event logging settings can be configured based on severity levels, with the ability to send specific levels to external system via syslog integration.	
FireEye	This is not applicable as each of FireEye's offerings are classified as SaaS.	

8.18 Trial and Testing Periods (Pre- and Post- Purchase)

8.18.1 Describe your testing and training periods that your offer for your service offerings.

Training and testing periods will vary based on the Service provider as well as the complexity of the request that is made by the Purchasing Entity. Some of the services can be functional within a few days and some will take a few months for full implementation.

8.18.2 Describe how you intend to provide a test and/or proof of concept environment for evaluation that verifies your ability to meet mandatory requirements.

Upon Request, Carahsoft will provide access to any of the Cloud Technologies proposed. The precise Access to the technology may be in a limited or "DEMO" fashion. Access will be to an extent that the State may complete any necessary tests or verifications that may be required. Instructions on precisely how each technology will be accessed will be provided upon request. All of the proposed technologies are currently live/ active and support many customers. A specific instance of the requested technology would be stood up within the cloud framework to support this request. As this will be occurring within a production, the creation of the instance is a quick and straight forward process not requiring any sort of extraordinary effort.

8.18.3 Offeror must describe what training and support it provides at no additional cost.

Carahsoft provides the customer with free training for specific deals on a case by case basis. This can include free installation, training, and maintenance for high value customers who purchase Carahsoft's solution through the NASPO contract vehicle. In addition, Carahsoft will provide webinars with basic training on a quarterly basis, made available to any Purchasing Entity who wishes to participate.

8.19 Integration and Customization

8.19.1 Describe how the Solutions you provide can be integrated to other complementary applications, and if you offer standard-based interface to enable additional integrations.

The integration into other applications will vary base on the Service Provider, however it is standard practice to allow for open AIs for integration development. For example Connecting Salesforce to an existing enterprise application is a common and frequently performed task. Integration options range from native Web Services support (APIs, outbound workflow, etc.) to import/export utilities to middleware integration via packaged connectors to toolkits for Java, .NET, and other open platforms. Our solution provides the ability to call out to virtually all common APIs, to enable synchronization, push / pull, and mash-ups with external apps/systems. Salesforce itself is based on web-service based APIs that in turn simplify access to Salesforce data from external systems. API-based integration is heavily leveraged by our customers.

8.19.2 Describe the ways to customize and personalize the Solutions you provide to meet the needs of specific Purchasing Entities.

The Service Providers customization options are very extensive and highly configurable. For example The Salesforce Platform offers a core set of technologies that not only power the Salesforce SaaS products, but also allows your Agency to build custom apps, connect data from any system, and manage it from anywhere. The Salesforce Platform allows customers to build apps fast with just a few clicks, designed for desktop and mobile devices, all from a single canvas. The Salesforce Platform has been given top ratings by Gartner, Forrester, & Info-Tech Research. To help IT deliver apps faster, the Salesforce Platform offers a simple yet powerful set of declarative, point-and-click tools that anyone can use to achieve business goals at lightning speed. Without writing code, developers and business users alike can quickly and easily create custom apps on the Salesforce Platform with complex business logic and beautiful user interfaces designed specific to every screen. Salesforce Lightning Builder tools allows your Agency to work in alignment with agile development methodologies as IT meet business demands faster. The Platform uses open APIs based on industry standards such as REST and SOAP to make it easy for your Agency to build apps that integrate with legacy systems. For more complex applications, developers can leverage the Apex programming language. Apex is an object-oriented, on-demand language. It is like Java, with similar syntax and notation, and is strongly-typed, compiled on demand, and fully integrated into the Platform. All of the application services come right out of the box, from a powerful workflow engine to API services, integration services, authentication, event log framework, analytics, and collaboration.

8.20 Marketing Plan

Describe your how you intend to market your Solutions to NASPO ValuePoint and Participating Entities.

Carahsoft offers deep experience in public sector marketing. Our dedicated team plans, promotes and executes more than 2,000 public-sector marketing campaigns and events each year, including contract-specific promotional activities. These include but are not limited to:

- News announcements

- Social media promotion (Twitter, Linked In, Facebook, Carahsoft Community)
- Website content/reciprocal links (Carahsoft website page; content for contract sponsor page)
- Marketing materials (FAQs, contract overviews, solution spec sheets, powerpoint slides)
- Training documents
- Co-branded tradeshow graphics, giveaways, display materials
- Tradeshow participation (national, state and local government and education shows)
- Digital and print ads
- Webinars
- Email campaigns
- Proactive marketing opportunity tar available through:
  - National Coalition for Public Procurement (NCPP) – publicprocurementcoalition.org
  - Institute for Public Procurement (NIGP) – nigp.org
  - National Association of Counties (NACo) – naco.org
  - The United States Conference of Mayors – usmayors.org
  - National League of Cities – nlc.org
  - National Governors Association – nga.org
  - Relevant State Associations

8.21 Related Value-Added Services to Cloud Solutions

Describe the valued-added services that you can provide as part of an awarded contract, e.g. consulting services pre- and post- implementation. Offerors may detail professional services in the RFP limited to assisting offering activities with initial setup, training and access to the services.

In addition to Carahsoft's quoting and configuration expertise, we also have a wide range of Service Provider implementation partners that we leverage to work with Purchasing Entities in order to ensure successful adoption and deployment within a Purchasing Entity. We will help to identity needs for initial setup, training and access to the services so that it is all available at the best prices from one source to the Purchasing Entity.

8.22 Supporting Infrastructure

8.22.1 Describe what infrastructure is required by the Purchasing Entity to support your Solutions or deployment models.

The Service Providers that are being proposed operate on their own secure infrastructure. The Purchasing Entities will only need an internet connection to access the services.

8.22.2 If required, who will be responsible for installation of new infrastructure and who will incur those costs?

The Service Providers maintain all costs for updating and building new infrastructures.

8.23 Alignment of Cloud Computing Reference Architecture

Clarify how your architecture compares to the NIST Cloud Computing Reference Architecture, in particular, to describe how they align with the three domains e.g. Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS).

CA	APM	The SaaS portal runs in Amazon Web Services.
	MAA	CA MAA is a SaaS service.
	CA Agile	Only SaaS is being offered via a public cloud

	ASM	As a monitoring service, ASM is considered to be SaaS.
Virtru	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2 . The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited userspecific application configuration settings.	
Salesforce	Salesforce's deployment model is a "public" cloud infrastructure, as defined by NIST 800-145. In the Salesforce Government Cloud, an agency dynamically provisions computing resources over the Internet on our multi-tenant infrastructure. This is a cost effective deployment model for agencies as it gives them the flexibility to procure only the computing resources they need and delivers all services with consistent availability, resiliency, security, and manageability. Salesforce was the first Cloud Service Provider to attain FedRAMP Authority to Operate for both Software as a Service (SaaS) and Platform as a Service (PaaS), consistent with the FedRAMP moderate baseline controls. Salesforce does not provide IaaS as a direct service offering to our customers, it is an underlying part of our PaaS and SaaS offerings. Salesforce Government Cloud In May 23, 2014 Salesforce achieved a FedRAMP Agency Authority to Operate at the moderate impact level (as described in FIPS 199 and 200) issued by Health and Human Services (HHS) for the Salesforce Government Cloud. Additionally, on May 15, 2015, HHS, as the FedRAMP authorizing agency, approved the Salesforce Government Cloud authorization package that was updated based on annual attestation requirements and updates to the FedRAMP baseline which is FISMA compliant and based on the current release of NIST SP 800-53 Rev. 4. Testing for the ATO was performed by a third party assessment organization (3PAO). The Salesforce Government Cloud information system and authorization boundary, is comprised of the Force.com Platform, Salesforce Services (Sales Cloud, Service Cloud, Chatter), and the backend infrastructure (servers, network devices, databases, storage arrays) that support the operations of these products, referred to as the General Support System (GSS). To obtain compliance with FedRAMP, Salesforce conducted security assessment and authorization activities in accordance with FedRAMP guidance, NIST SP 800-37, and HHS guidance. As part of this process Salesforce documented a System Security Plan (SSP) for the Salesforce Government Cloud service offering. The SSP is developed in accordance with NIST SP 800-18, Guide for Developing Federal Information System Security Plans. The SSP identifies control implementations for the GSS and in-scope customer facing products (Force.com Platform, Salesforce Services) according to the FedRAMP moderate baseline and HHS security control parameters. A security assessment of the information system was conducted by a third party assessment organization (3PAO) in accordance with NIST 800-53A and FedRAMP requirements. The security assessment testing determined the adequacy of the management, operational, and technical security controls used to protect the confidentiality, integrity, and availability of the Salesforce service and the customer data it stores, transmits and processes. To maintain compliance with FedRAMP, Salesforce conducts continuous monitoring. Continuous monitoring includes ongoing technical vulnerability detection and remediation, remediation of open compliance related findings, and at least annual independent assessment of a selection of security controls by 3PAO. As part of our FedRAMP annual assessment, Salesforce is now aligned with NIST SP 800-53, Rev. 4 controls.	
ServiceNow	ServiceNow's architecture aligns with Software as a Service (SaaS).	

Docusign	DocuSign's DTM® solution is ISO 27001:2013 certified and many of the ISO 27001:2013 controls are mapped to the NIST 800-53 requirements; we can provide additional information upon request.	
SAP	Ariba	Our solutions are offered and delivered in a true subscription-based model and shared service (multi-tenant) offering. There is no software to install, no hardware to buy, no maintenance or support costs and no need to hire consultants or tech specialists to run the system. We deploy and manage the infrastructure. Customers only need a web browser for access. Subscriptions include system maintenance, automatic upgrades, enhancements and application of service packs, Level 1– 3 help desk support, professional services and best practices built directly into the application.
	Fieldglass	Fieldglass is offered in a SaaS model. We follow the public cloud model identified by NIST. All customers access the same Fieldglass application version in a multi-tenancy database. The system is hosted in a secure hosting facility. Fieldglass manages everything from the cage in including all servers, devices, wiring, software, and configuration. Fieldglass uses the Cloud Security Alliance framework to measure itself against the recommended controls, in addition to ISO 27001 and SOC 2 controls in the Trust Services Principles of Security, Availability, Processing Integrity, Confidentiality, and Privacy.
	Hanna	HEC is a private cloud offering from SAP that provides fully 'managed' Infrastructure as a Service (IaaS) following NIST Cloud Computing Reference Architetcure.
	Hybris	The SAP Hybris Commerce, Cloud Edition is a Private Cloud Managed Service that offers a best practice multichannel commerce platform built on hybris accelerator technology, running in SAP Hybris own datacenters with a pay as you grow subscription model.
	SuccessFactors	Our IT architecture is aligned with ISO 27002. We are Safe Harbor certified and in alignment with BS10012 and ISO 20000 for Service Delivery. We demonstrate an on-going commitment to protecting the confidentiality, integrity and availability ("CIA") of data from internal and external threats, making us a reliable and secure system provider. Our secure multi-tenant Software as a Service (SaaS) platform is designed for availability, security, scalability, and performance. Industry best practices and standards are adopted and incorporated. Our Network also complies with the Authority to Operate as a Moderate Risk Federal Information System by the Office of Personnel Management and Department of Homeland Security; NIST SP800-53 Security Controls; EU Privacy Directive 95/46/EC for EU and non-EU customer data; Payment Card Industry (PCI) Data Security Standard (DSS) v 2.0; Safe Harbor. We provide privacy compliant data center facilities not only in the United States but also as a Member State of the European Union (EU) or a state of the European Economic Area (EEA). Currently, such data centers are certified for ISO27001, ISO9001 and PCI-DSS compliance. Our security services provide complete and thorough monitoring of all traffic on the network on a 24x7x365 basis, and include security technology, alert services and incident management support. We are audited twice annually to SSAE16 (US) or ISAE 3402 (international) accounting standards.

<table>
<tr><td>VMware</td><td>See section 8.1.1 for additional details.

Due to FOIA restrictions, we cannot share specific infrastructure details or architecture diagrams at this time. We can provide sample architecture diagrams under NDA to participating entities during task order negotiations as required.

VMWare AirWatch
AirWatch partners with co-located and cloud-hosted Tier III data centers to support of SaaS offering.
Due to FOIA restrictions, we cannot share specific infrastructure details or architecture diagrams at this time. We can provide sample deployments as under NDA to participating entities during task order negotiations as required.</td></tr>
<tr><td>FireEye</td><td>Each of the FireEye cloud solutions are classified as Software as a Service (SaaS) and leverage a private cloud deployment model. With respect to the NIST Cloud Computing Reference Architecture, the following actors are integral to the overall design of the solutions:

<table><tr><th>Actor</th><th>Definition</th></tr><tr><td>Cloud Consumer</td><td>Customer organizations who have purchased FireEye cloud solutions</td></tr><tr><td>Cloud Provider</td><td>FireEye</td></tr><tr><td>Cloud Carrier</td><td>Internet service providers and organizations who have been contracted to host FireEye cloud solutions.</td></tr></table>
A Cloud Broker is not leveraged in the FireEye cloud offerings. FireEye has contracted independent service auditors for evaluating controls relevant to security and confidentiality, however this occurs on an as-needed basis.</td></tr>
<tr><td>VirtueStream</td><td>Virtustream solution is fully NIST compliant for Essential Characteristics, as the Infrastructure as a Service (IaaS) Service Model, with all deployment options – Private Cloud, Community Cloud, Public and Hybrid Cloud. To that extent:
1.Virtustream IaaS provides a self-service portal called xStream, where users can access, view, edit, provision, and modify compute, storage, network and application services based on granular Role Based Access Control, which can be integrated with Active Directory or LDAP.
2.Virtustream IaaS provides Broad Network Access, where it can provide landing zone for any private network (Point-to-Point, Virtual Private Label Switching, Multi-Protocol Label Switching, or Direct Connect), public network (Internet, Trusted Internet Connectivity as landing zone, IPSEC VPN and SSL VPN) and also extranet connectivity (shared network, i.e, Cloud Connect, Cloud Exchange, NetBond, etc.) which is growing rapidly as option for connecting cloud resources.
3.Key to Virtustream solution is its proprietary and patented solution of uVM technology, which is effectively a granular solution for resource pooling, providing application performance, pay for consumption only and segregate resources for security and compliance, but aggregate for cost efficiency. In addition, Virtustream is currently one of very few Cloud Service Provider with capabilities for Geo-Fencing and Geo-Tagging of the virtual machines to a specific data center, and getting down to cluster and host machine level.
4.Virtustream's self-service portal, ticketing system and also the Technical Account Manager, who is the single point of contact for State of Utah allows for provisioning and deprovisioning of resources and services. In addition, Virtustream is uniquely positioned to provide application level provisioning as part of its standard automation and orchestration tool.
5.The fundamental of Virtustream solution is based on uVM Technology, which is very unique in terms of billing. Virtustream solution takes average consumption of compute resources, and State of Utah would only pay for actual resources based on a monthly average. This is in comparison</td></tr>
</table>

	with traditional cloud solution, where the billing is based on allocation of resources in T-Shirt size (Micro, S, M, L, XL, XXL), and if the server is up, consumer of the cloud pays, but when it is down, they don't. In case of the Virtustream solution, customer only pays based on the average of vCPU, RAM, IOPS and Network I/O; the key is average, not aggregate and based on consumption not allocation. In addition, all storage, security, application management services are offered as a monthly fee, based on the VMs; also, Virtustream can provide consultative and project support based on time and materials. 6.The deployment of Virtustream cloud can be on-premise or private based on purchase of its Cloud Management Platform, Community Cloud based on its IaaS, Public Cloud based on its IaaS and Hybrid cloud based on its ability to provide software and IaaS combined.

CONFIDENTIAL, PROTECTED, OR PROPRIETARY INFORMATION

All confidential, protected or proprietary Information must be included in this section of proposal response. Do not incorporate protected information throughout the Proposal. Rather, provide a reference in the proposal response directing Lead State to the specific area of this protected Information section.

If there is no protected information, write "None" in this section.

Failure to comply with this Section and Section 3.13 of the RFP releases the Lead State, NASPO ValuePoint, and Participating Entities from any obligation or liability arising from the inadvertent release of Offeror information.

Carahsoft Technology Corporation ("Carahsoft") respectfully requests that section 6.3 Financials of Carahsoft's response be treated as a trade secret under the Utah Uniform Trade Secrets Act, Utah Code § 13-24-2 and submits this justification in accordance with Utah Code 63-G-2-305 demonstrating that its audited financials should be treated as a trade secret under Utah's Uniform Trade Secrets Act. Additionally, Carahsoft is claiming the same confidentiality of the Consensus Assessments Initiative Questionnaire provided in relation to DocuSign and FireEye offerings, as well as the Cloud Controls Matrix for DocuSign.

Carahsoft has marked this attachment as "confidential" in accordance with the RFP instructions by including all confidential data into the Confidential, Protected, or Proprietary Information in our response.

Carahsoft is claiming confidentiality for these specific Consensus Assessments Initiative Questionnaires and Cloud Controls Matrix because releasing these documents would cause irreparable damage and would create the potential for cyber security breach. While portions of this information are in the public domain, the information contained within is not represented or assimilated this way in any other format.

Carahsoft's Audited Financial Data satisfies the three-part test of the Utah Uniform Trade Secrets Act as set forth below and should therefore be treated as confidential and by the Utah Division of Purchasing and should not subject to public disclosure as provided in Utah Code § 63G-2-305.

1. *Carahsoft's Audited Financial Data is a "compilation" within the meaning of Utah Code § 13-24-2(4).* Carahsoft's Audited Financial Data is a compilation of all of the Company's financial data and results for 2014. While some aspects of this information may be available, the compilation of this information is unique and the result of sustained and distinct effort by the Company's financial staff and its accountants.

2. *As required by Utah Code § 13-24-2(4)(a) Carahsoft derives independent economic value, actual or potential, from its Audited Financial Data not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.* Carahsoft is a leading distributor of technology products and services to public sector customers such as the State of Utah, and throughout the United States and Canada. Sales in this market are intensely and deliberately competitive, with each sale subject to a structured bidding process in which low price is frequently the deciding factor on which contract award is based. Competition in this market is fierce, with competitors regularly competing with one another for federal, state, county and city business.

Carahsoft's competitors closely monitor this market, and regularly attempt to gain financial and other information about Carahsoft and other competing vendors. Allowing Carahsoft's competitors access to this compilation of financial data by releasing it in response to a public records request will damage Carahsoft's competitive position because it will provide competitors insight into Carahsoft's financial structure, including compensation, overhead costs, rental rates, profit margins and the like. Indeed, allowing insight into compensation may violate individual employees' expectations of privacy. Once competitors have this access and insight, they can use it to undercut Carahsoft in the marketplace, damaging Carahsoft's business with its customers and its suppliers, and inflicting economic hardship upon the Company.

For these reasons, Carahsoft does not itself disclose its Audited Financial Data except when required by law to do so. For example, Carahsoft discloses its financial information in filing its periodic tax returns—disclosure of which is prohibited by applicable state and federal law. In this regard, we note that Carahsoft is a privately owned company. Therefore, Carahsoft does not publicly report its financial results to the United States Securities and Exchange Commission.

3. Carahsoft uses reasonable efforts to maintain the secrecy of its Audited Financial Data.

The third part of the Utah Uniform Trade Secret Act's test for trade secret treatment is whether the information "...is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." Utah Code § 13-24-2(4)(b).

Carahsoft satisfies this test because it takes reasonable steps to maintain the secrecy of its financial information. As noted above, Carahsoft is a privately held company and therefore does not report its financial results publically to either its shareholders or the Securities and Exchange Commission. This is in contrast to public companies such as IBM or AT&T who report financial results quarterly as a matter of public record.

Even within Carahsoft's business operations itself, Carahsoft's management strictly limits disclosure of this information to a few carefully selected employees, and then only on a "need to know" basis in connection with their work assignments. Indeed, each Carahsoft employee signs a Confidentiality Agreement agreeing not to disclose this information.

Conclusion

Based on the forgoing, Carahsoft believes it has demonstrated that its Audited Financial Data, Consensus Assessments Initiative Questionnaires, and Cloud Controls Matrix are trade secret as defined in Utah Code § 23-24-2 . It is a compilation the content of which affords Carahsoft a competitive advantage. Carahsoft's competition cannot readily discern it by proper means. Moreover, Carahsoft itself treats this information as a trade secret even within its own business operations.

Should there be a public records request for this information, Carahsoft respectfully requests that the State afford Carahsoft's requested confidential information and documents trade secret protection in accordance with Utah law and deny the request. In the event that the State determines to release the requested confidential data, Carahsoft requests that you notify us promptly so that we may provide further justification for trade secret protection of this confidential data.

CLAIM OF BUSINESS CONFIDENTIALITY

Pursuant to Utah Code Annotated, Subsections 63G-2-305(1) and (2), and in accordance with Section 63G-2-309, Carahsoft Technology Corporation (company name) asserts a claim of business confidentiality to protect the following information submitted as part of this solicitation. Pricing/Cost Proposals may not be classified as confidential or protected and will be considered public information. **An entire proposal cannot be identified as "PROTECTED", "CONFIDENTIAL" or "PROPRIETARY".**

☒ Non-public financial statements
☐ Specific employee name and contact information
☐ Specific customer information, client lists, or subscription lists
☒ Other (specify): Consensus Assessments Initiative Questionnaires and Cloud Controls Matrix

This claim is asserted because this information requires protection as it includes:

☒ trade secrets as defined in Utah Code Annotated Section 13-24-2 ("Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (a) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy).

☒ commercial information or non-individual financial information obtained from a person if: (a) disclosure of the information could reasonably be expected to result in unfair competitive injury to the person submitting the information or would impair the ability of the governmental entity to obtain necessary information in the future; [and] (b) the person submitting the information has a greater interest in prohibiting access than the public in obtaining access.

This statement of reasons supporting the claim of business confidentiality applies to the following information in this proposal:

Page	Paragraph	Reason
187-204, Technical Response Template	All	See Confidential, Trade Secret, & Proprietary Information Explanation Page 176-177 of Carahsoft's Technical Response
Exhibit 1-DocuSign Excel	N/A	See Confidential, Trade Secret, & Proprietary Information Explanation Page 176-177 of Carahsoft's Technical Response
Exhibit 1-FireEye Excel	N/A	See Confidential, Trade Secret, & Proprietary Information Explanation Page 176-177 of Carahsoft's Technical Response
Exhibit 2-DocuSign Excel	N/A	See Confidential, Trade Secret, & Proprietary Information Explanation Page 176-177 of Carahsoft's Technical Response

Please use additional sheets if needed.

You will be notified if a record claimed to be protected herein under Utah Code Annotated § 63G-2-305(1) or (2) is classified public or if the governmental entity determines that the record

should be released after weighing interests under Utah Code Annotated § 63G-2-201(5)(b) or Utah Code Annotated § 63G-2-401(6). See Utah Code Annotated § 63G-2-309.

Signed: Robert R. Moore, Vice President
On behalf of (company): Carahsoft Technology Corporation
Date: March 10, 2016

(Revision 6/4/2015)

EXCEPTIONS AND/OR ADDITIONS TO THE STANDARD TERMS AND CONDITIONS

Proposed exceptions and/or additions to the Master Agreement Terms and Conditions, including the exhibits, must be submitted in this section. Offeror must provide all proposed exceptions and/or additions, including an Offeror's terms and conditions, license agreements, or service level agreements in Microsoft Word format for redline editing.

Offeror must also provide the name, contact information, and access to the person(s) that will be directly involved in terms and conditions negotiations. If there are no exceptions or additions to the Master Agreement Terms and Conditions, write "None" in this section.

The point of contact who will be directly involved in terms and conditions negotiations is Jack Dixon – Contract Specialist. He can be reached at – 703.230.7545 / Jack.Dixon@Carahsoft.com.

32. Transition Assistance:

a. The Contractor shall reasonably cooperate with other parties in connection with all Services to be delivered under this Master Agreement, including without limitation any successor service provider to whom a Purchasing Entity's Data is transferred in connection with the termination or expiration of this Master Agreement. The Contractor shall assist a Purchasing Entity in exporting and extracting a Purchasing Entity's Data, in a format usable without the use of the Services and as agreed by a Purchasing Entity, at no additional cost to the Purchasing Entity. Any transition services requested by a Purchasing Entity involving additional knowledge transfer and support may be subject to a separate transition Statement of Work.

b. A Purchasing Entity and the Contractor shall, when reasonable, create a Transition Plan Document identifying the transition services to be provided and including a Statement of Work if applicable.

c. The Contractor must maintain the confidentiality and security of a Purchasing Entity's Data during the transition services and thereafter as required by the Purchasing Entity.

Carahsoft takes exception to section 32 – Transition Assistance and request it includes the following.

9.4 RETURN OF CUSTOMER DATA. Carahsoft shall provide Customer Data in its standard database export format, excluding the any Core Technology, to Customer upon Customer's written request and at no additional cost to Customer, provided that Carahsoft receives such request from Customer within forty-five (45) days following the expiration or termination of a provided service. If Carahsoft has not received a request within the foregoing time frame, Carahsoft shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, have the right to delete all Customer Data in its systems or otherwise in its possession or under its control and delete Customer's instances of any provided service.

Carahsoft takes exception to Section 13 – Indemnification. Carahsoft requests that Indemnification from the state to the customer under a certain set of circumstances.

IN SUMMARY

Carahsoft Technology Corporation appreciates the opportunity to offer this solution for the State of Utah's initiative.

The Carahsoft Team has proposed a superior and cost-effective solution that fully complies with the State of Utah's requirements set forth in Solicitation # CH16012. We understand the importance of your project goals, and we are confident you will benefit from this solution and our expertise.

Carahsoft looks forward to the opportunity to speak with you regarding the details of this proposal, as well as the opportunity to work with the State of Utah on this project.

SUPPLEMENTAL INFORMATION

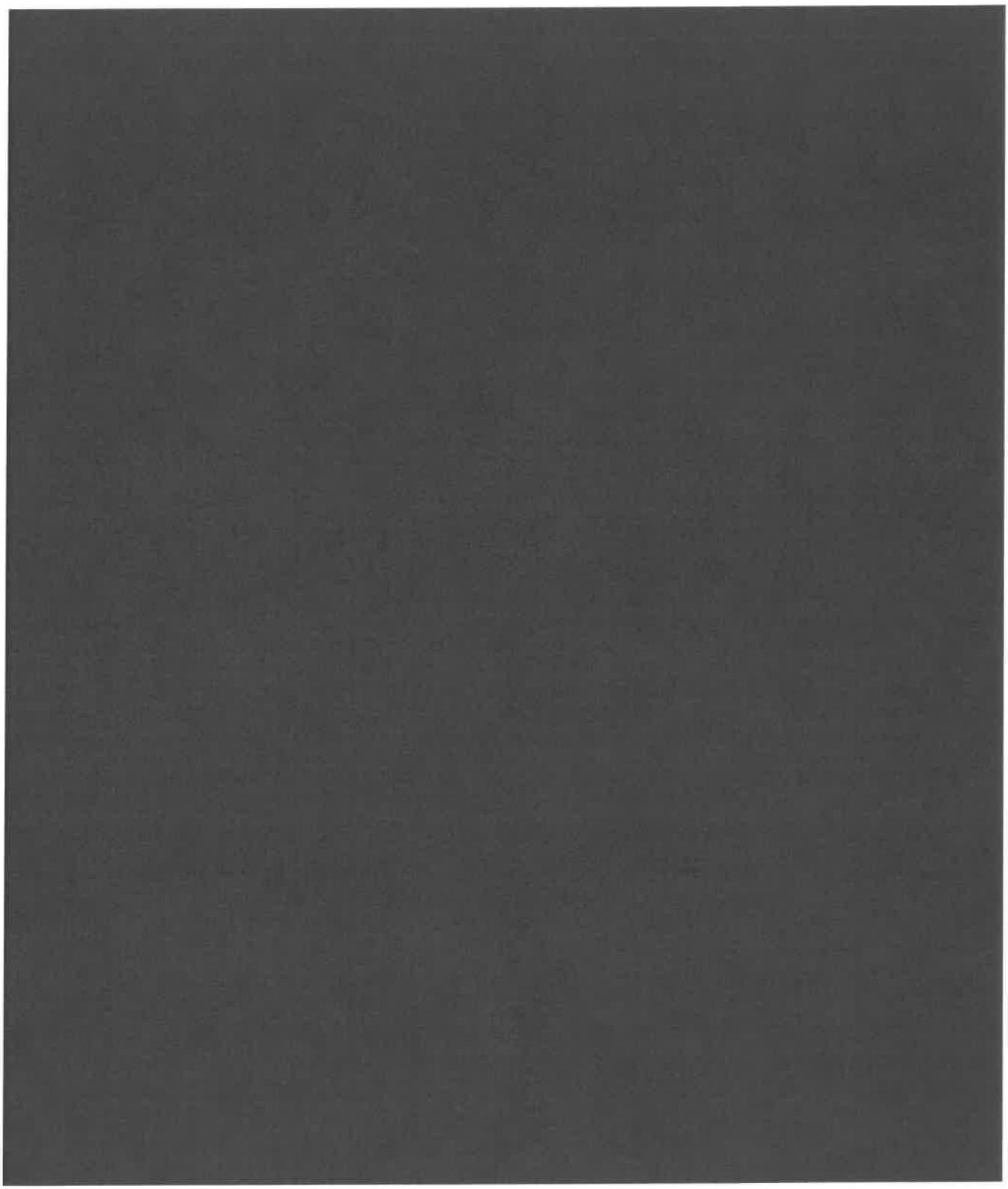
Please find below Carahsoft's supplemental information.

Carahsoft Technology Corporation

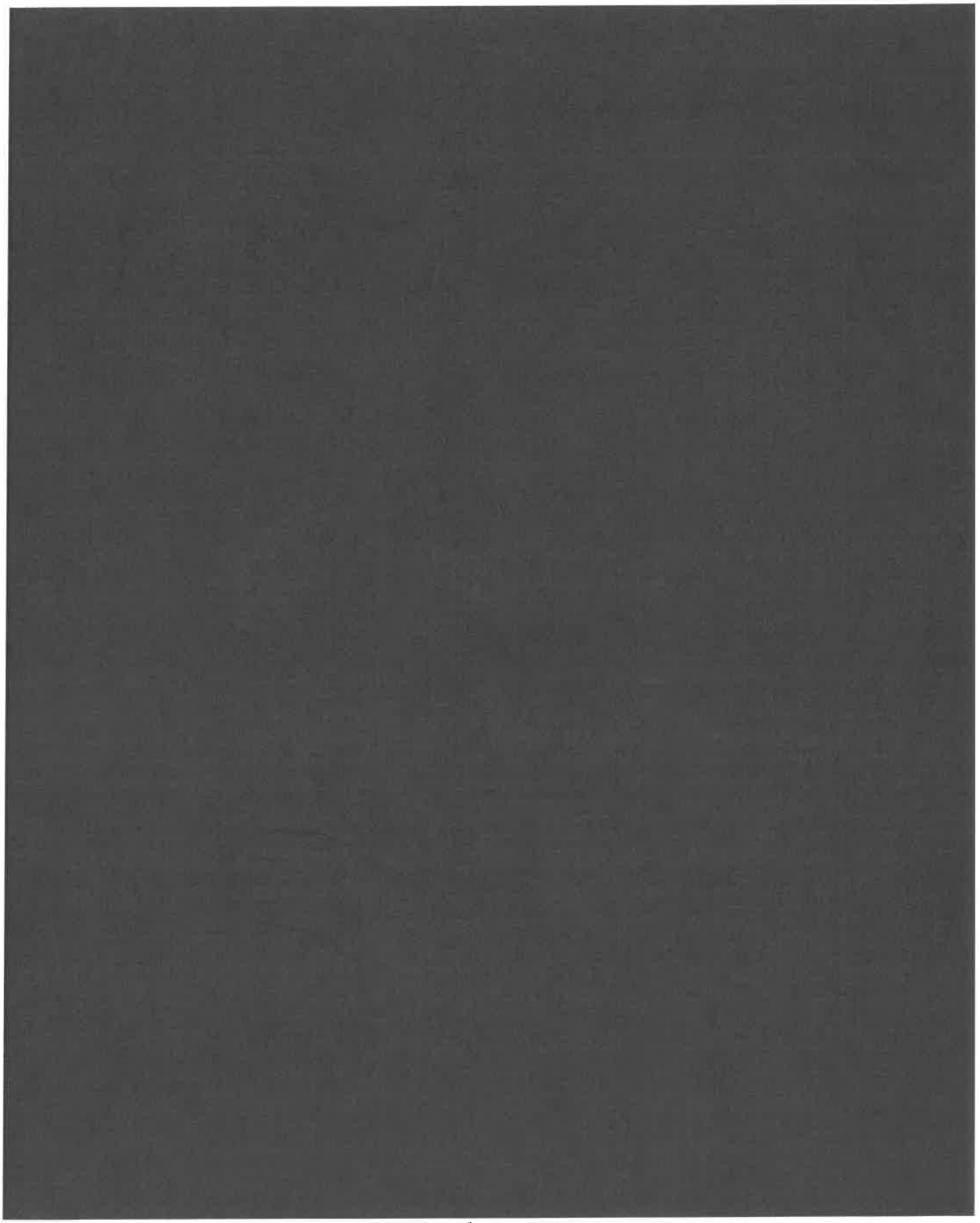
Financial Statements with Independent Auditors' Report

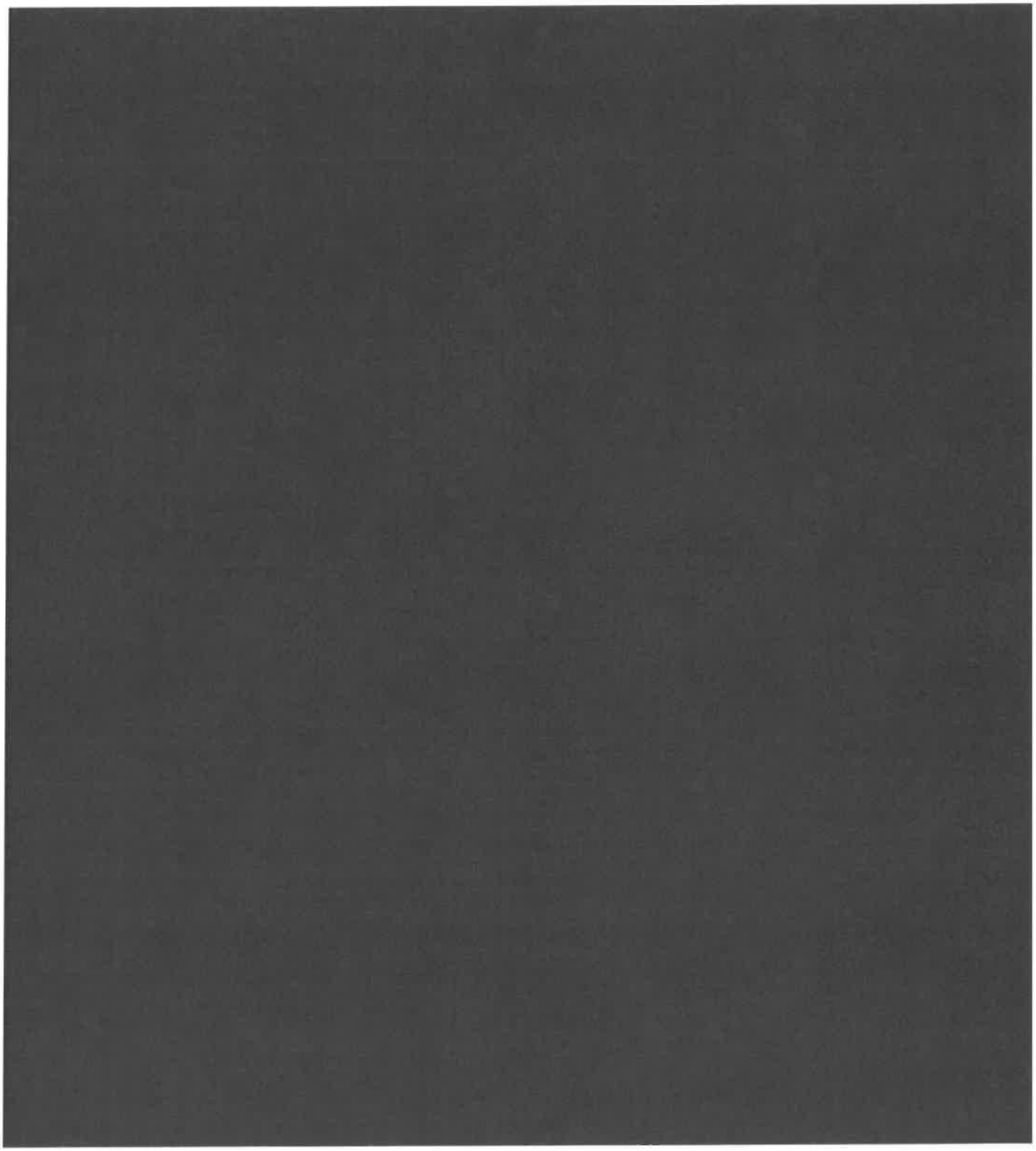
December 31, 2013

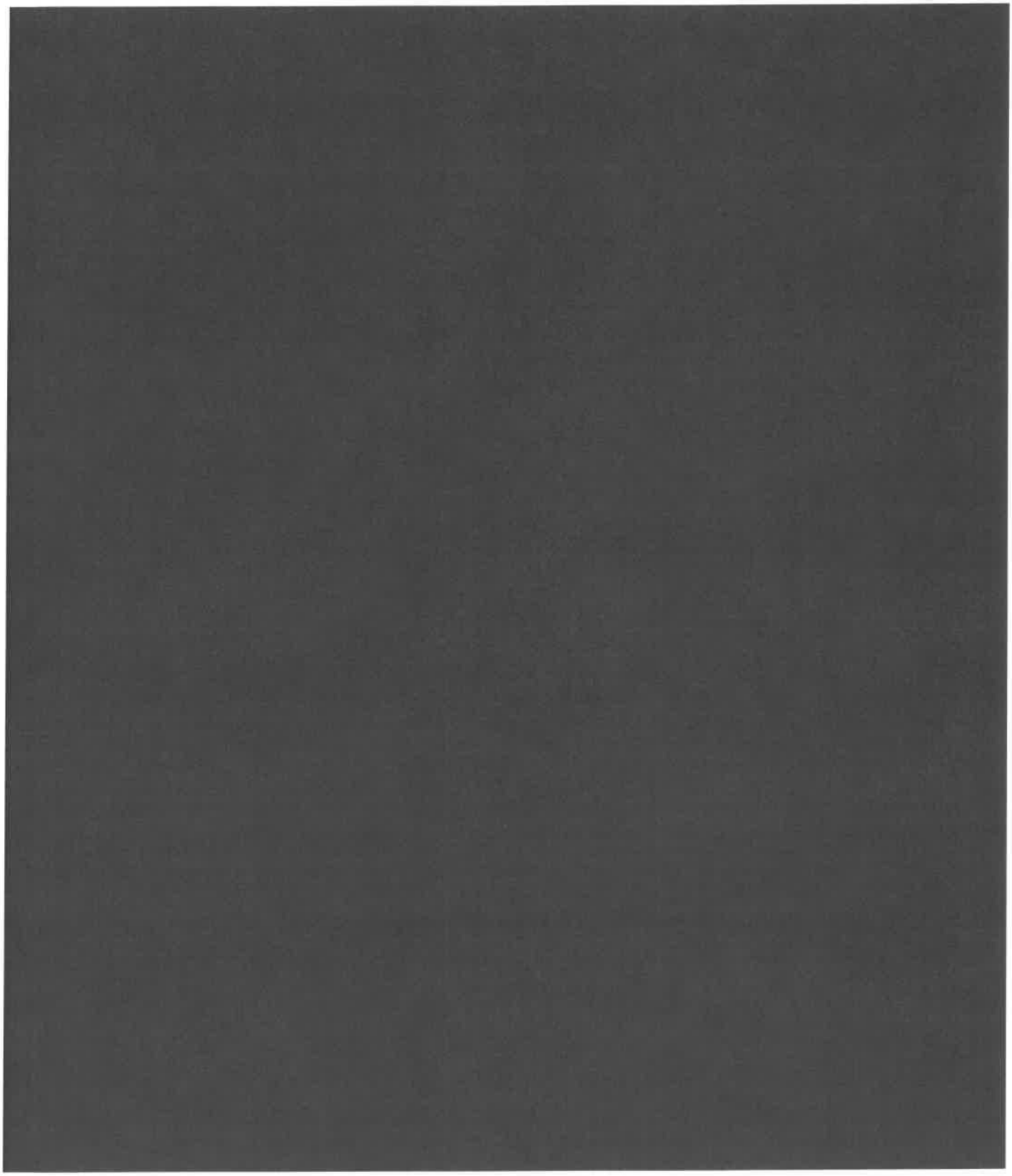
CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

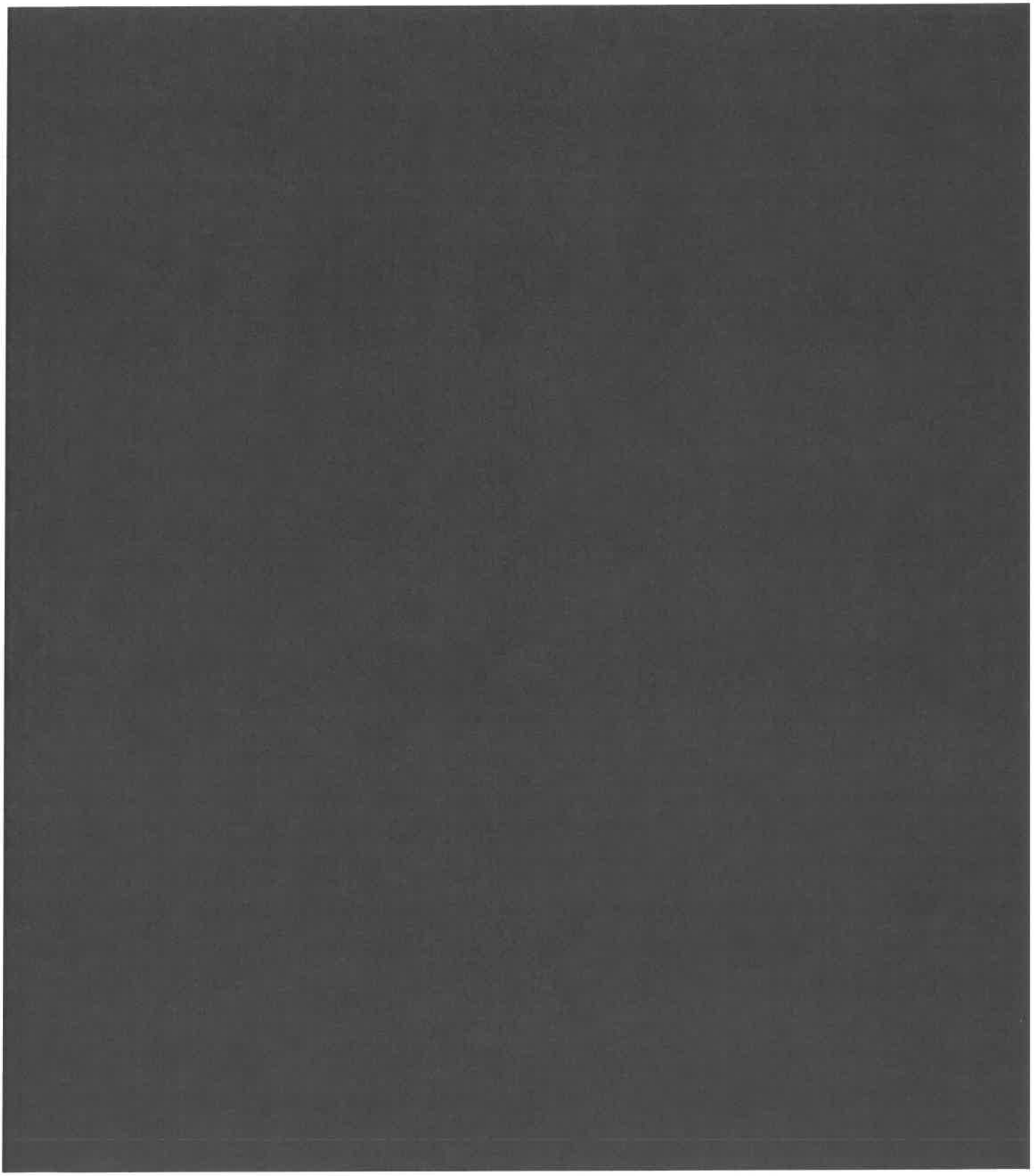






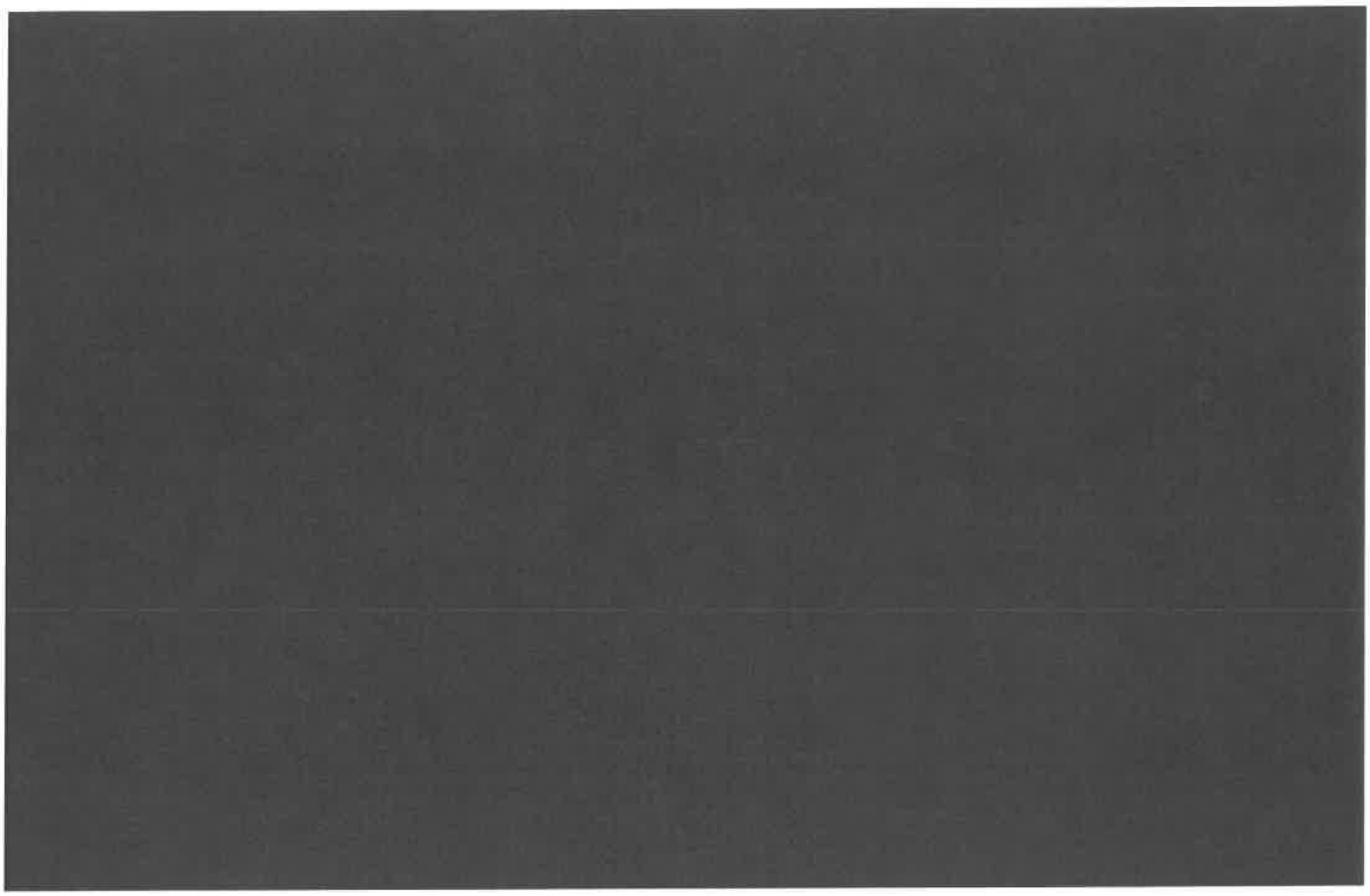
CONFIDENTIAL PROPRIETARY INFORMATION

All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



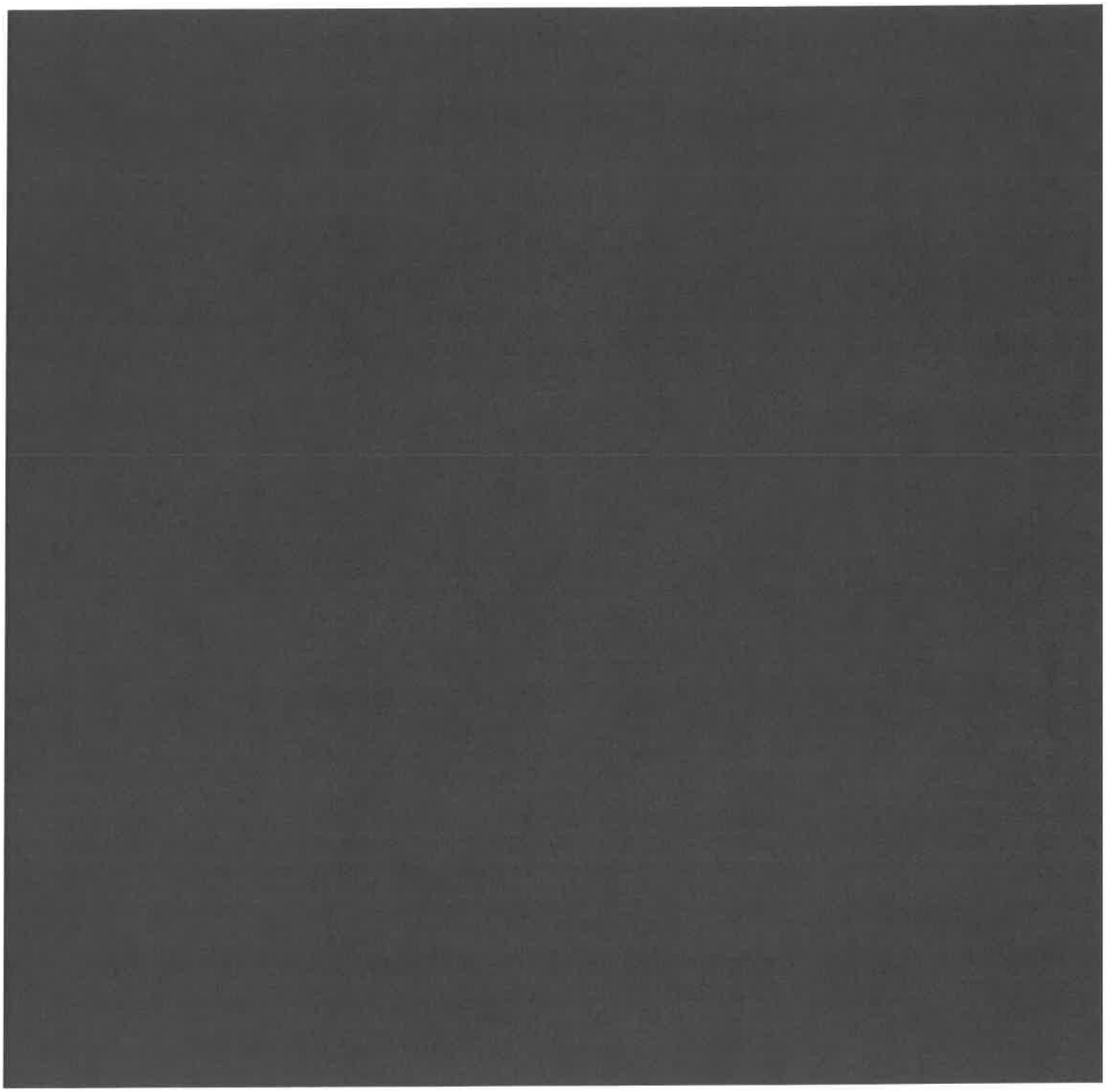
CONFIDENTIAL PROPRIETARY INFORMATION

All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



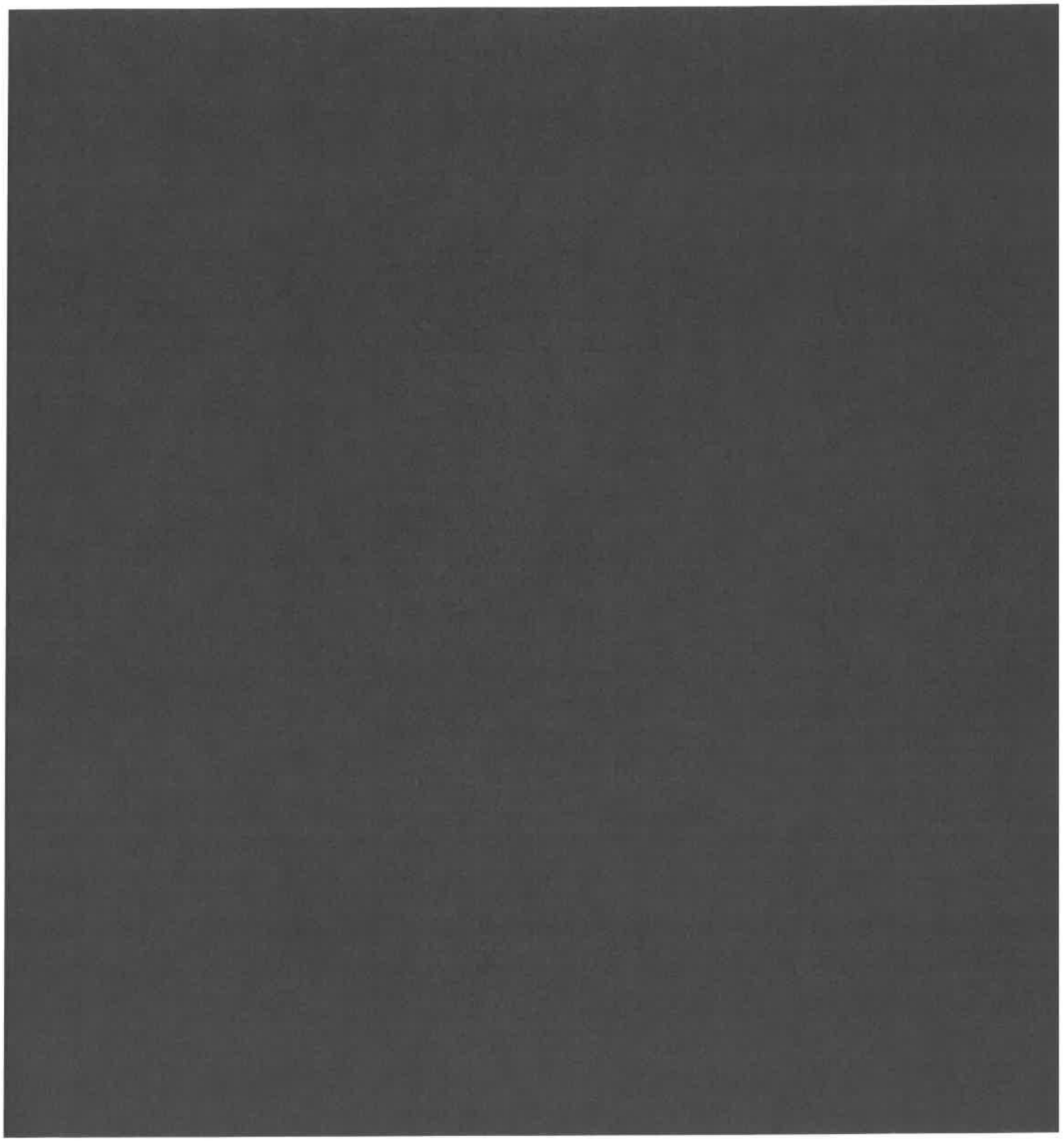
CONFIDENTIAL PROPRIETARY INFORMATION

All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

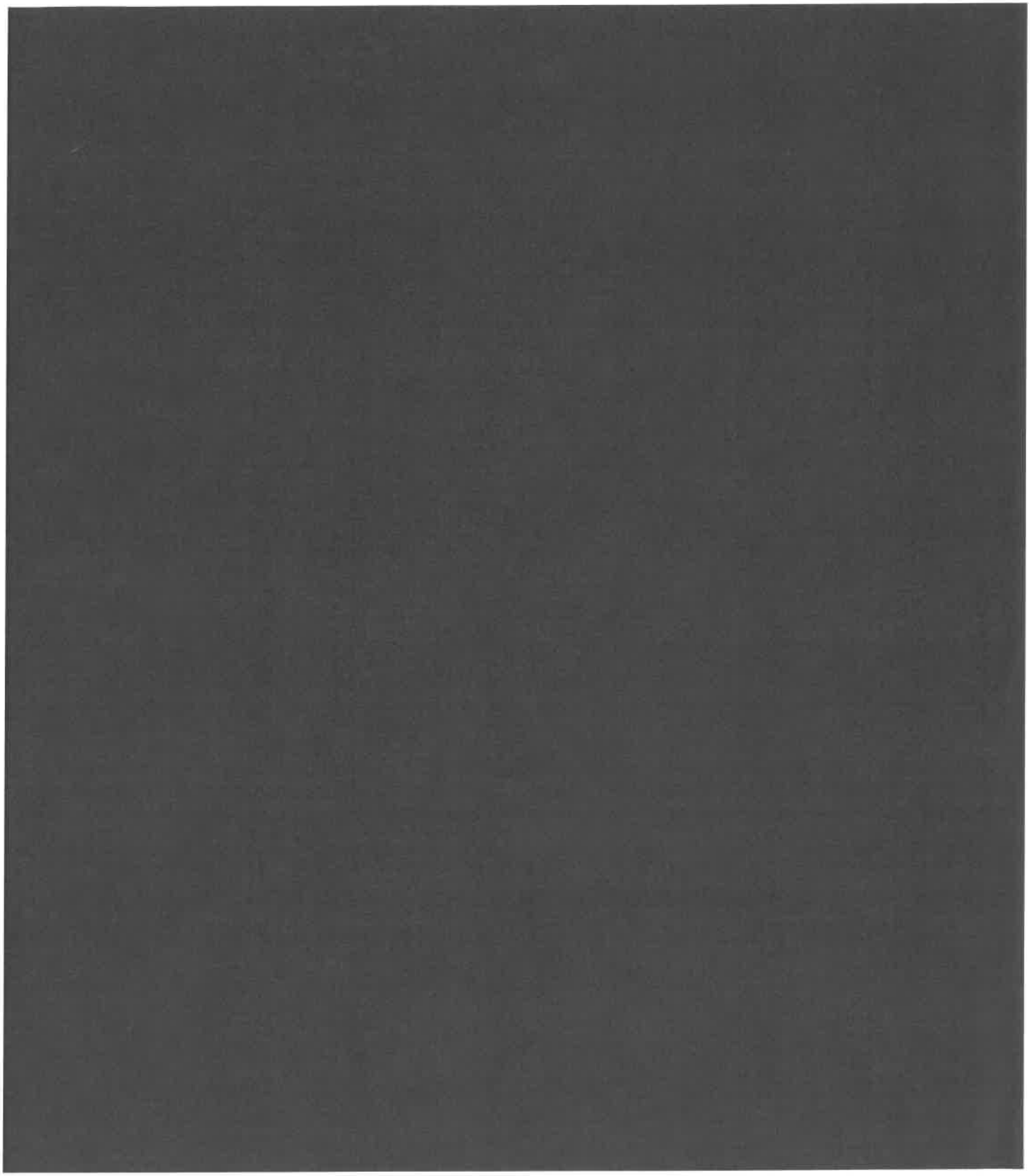


CONFIDENTIAL PROPRIETARY INFORMATION

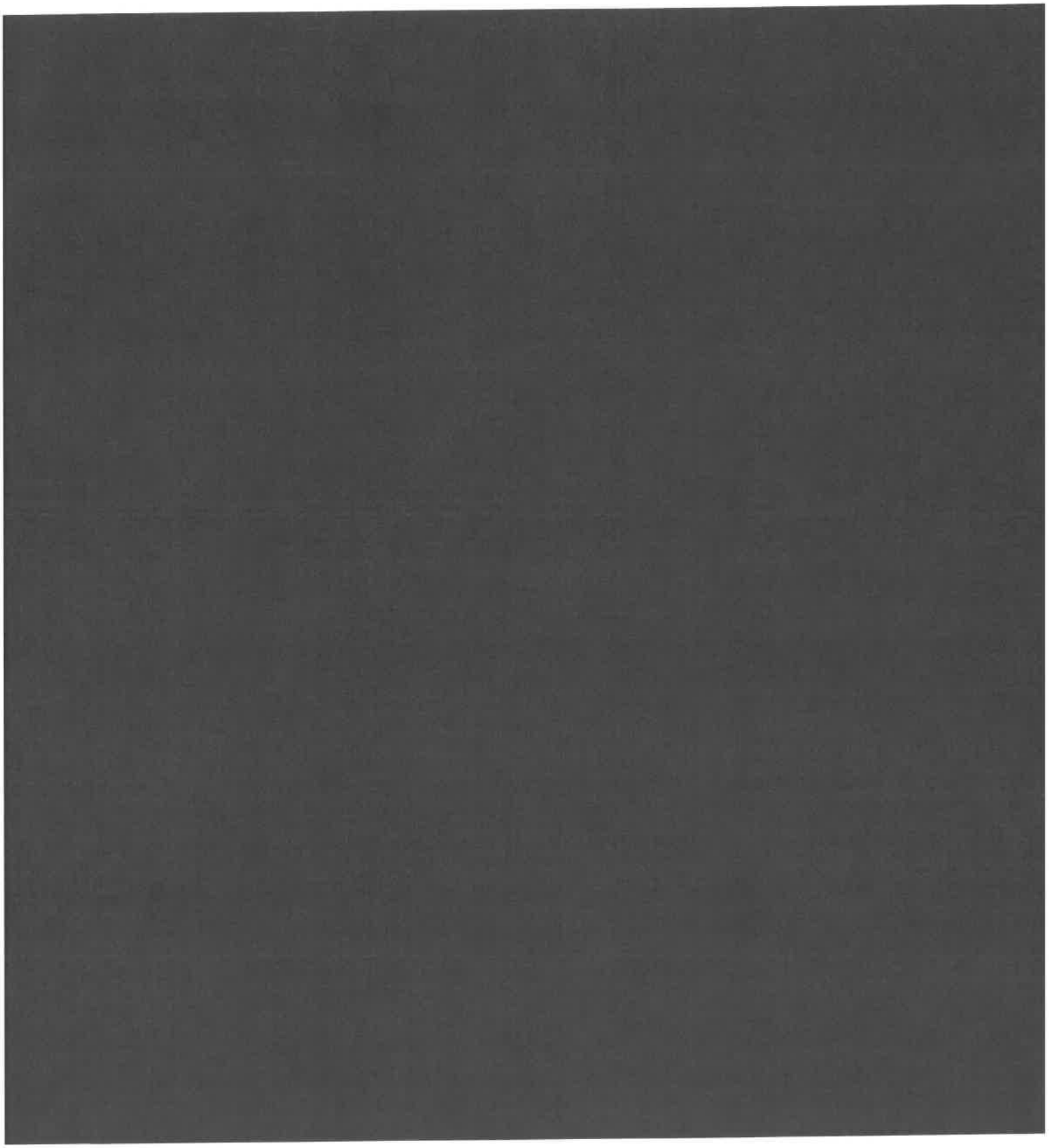
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



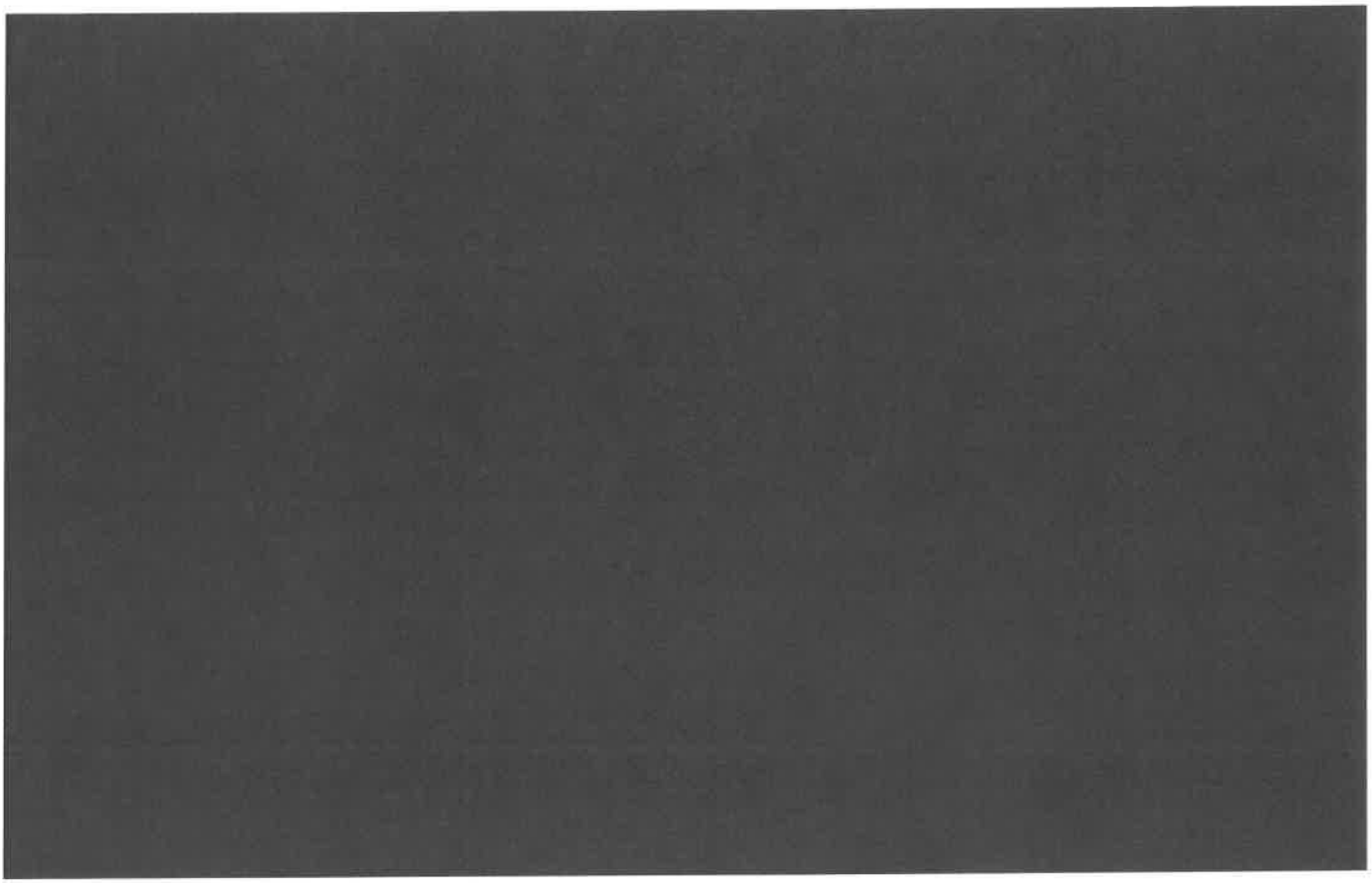
CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



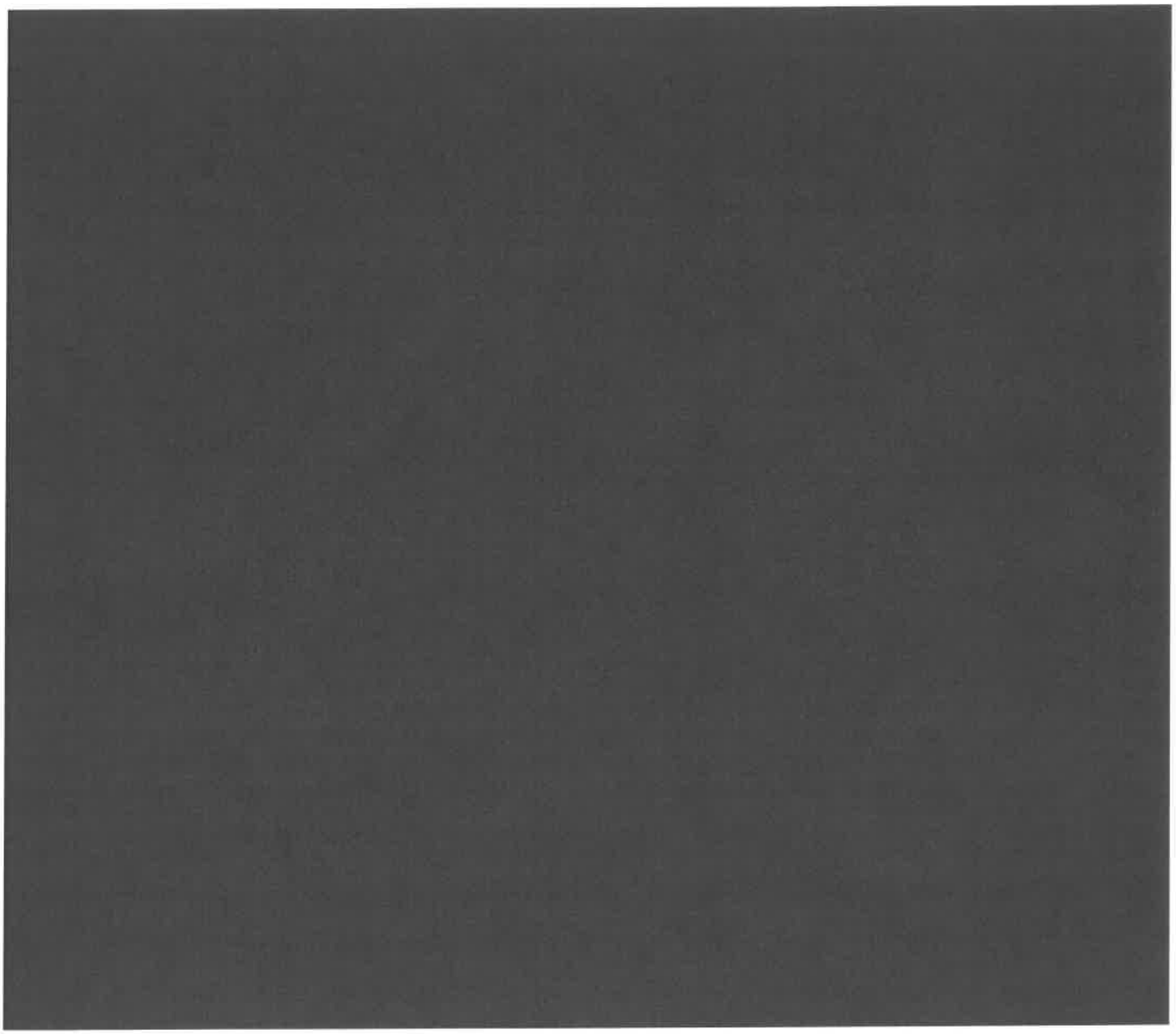
CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

Carahsoft Technology Corporation

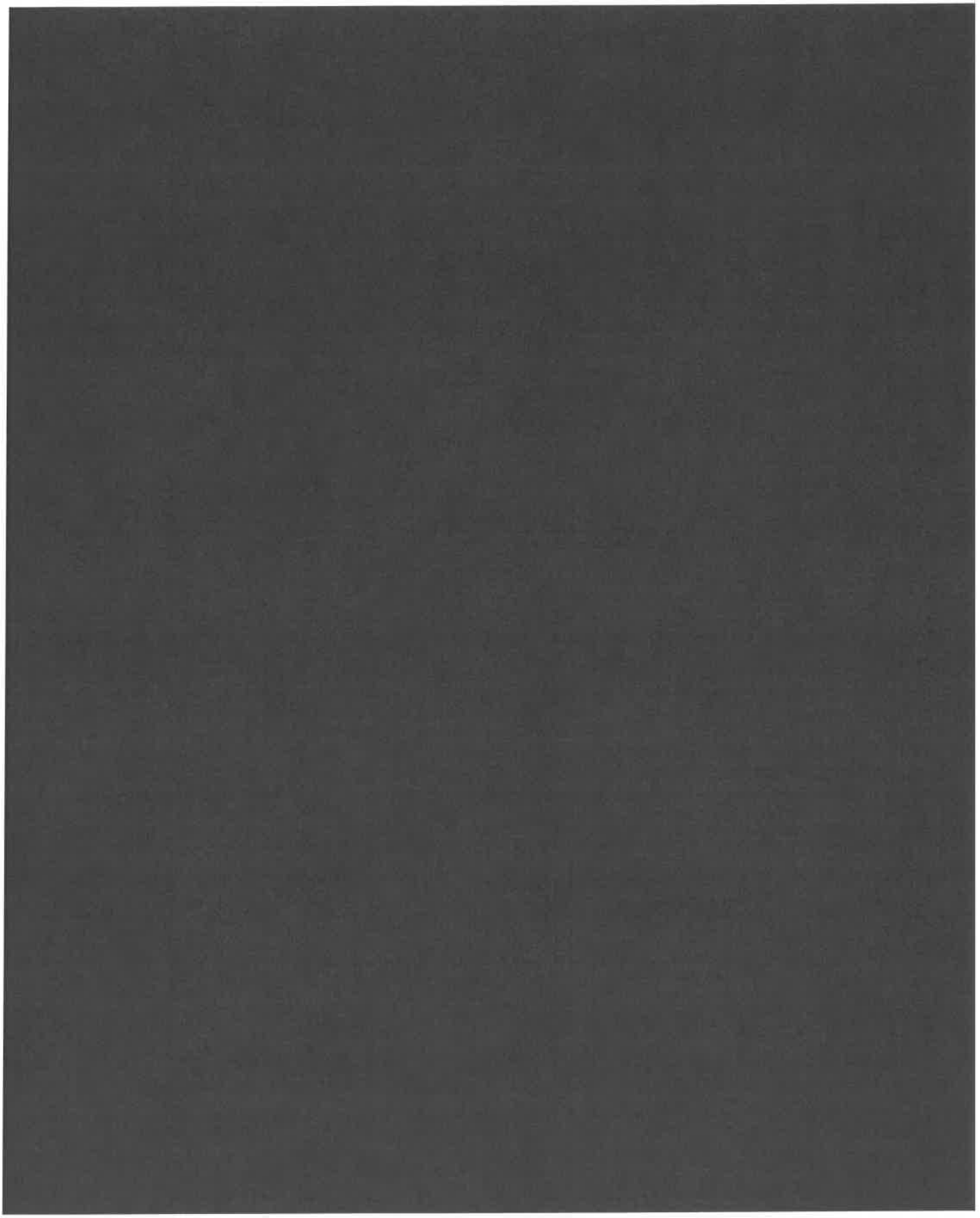
Financial Statements with Independent Auditor's Report

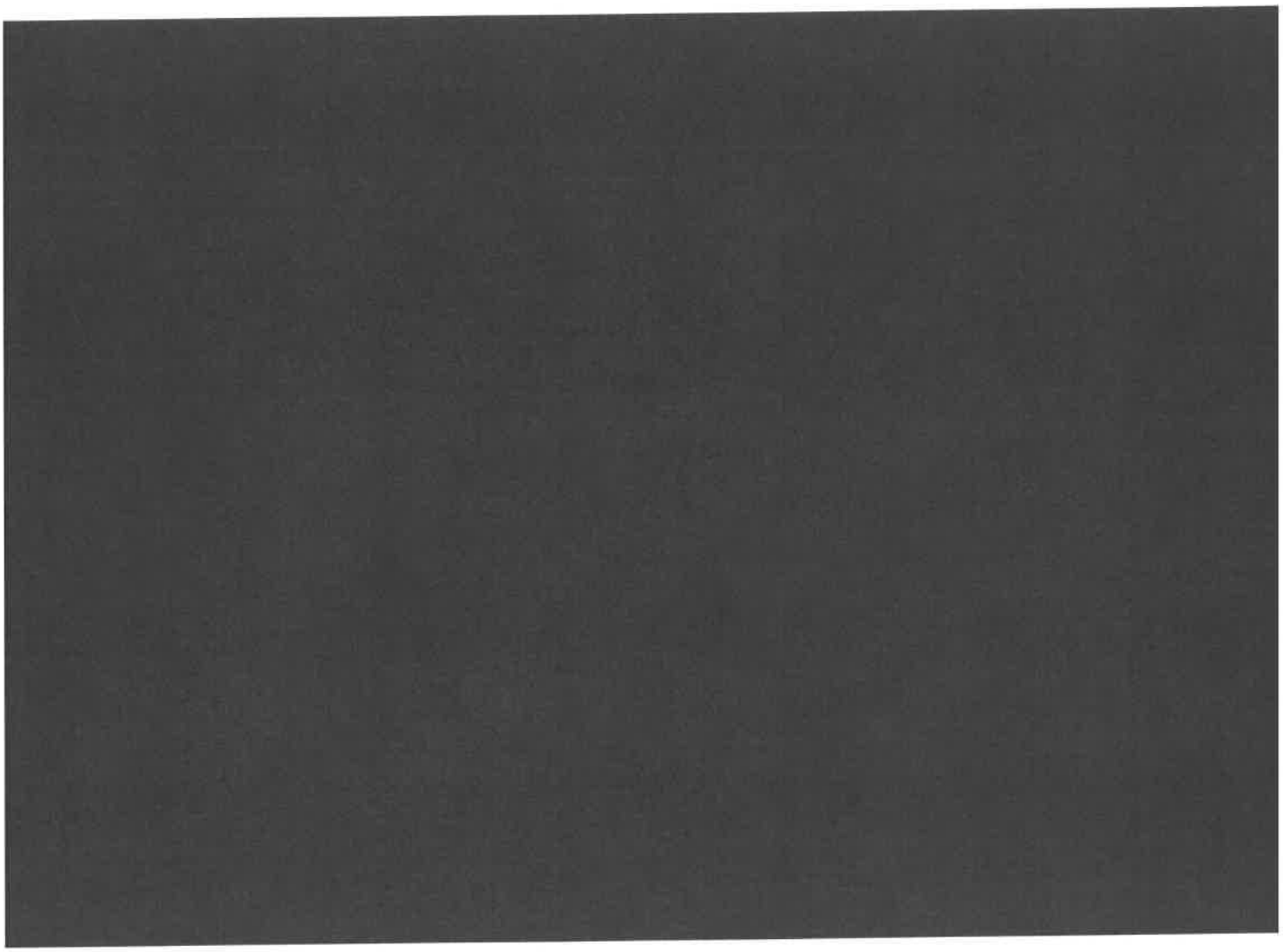
December 31, 2014

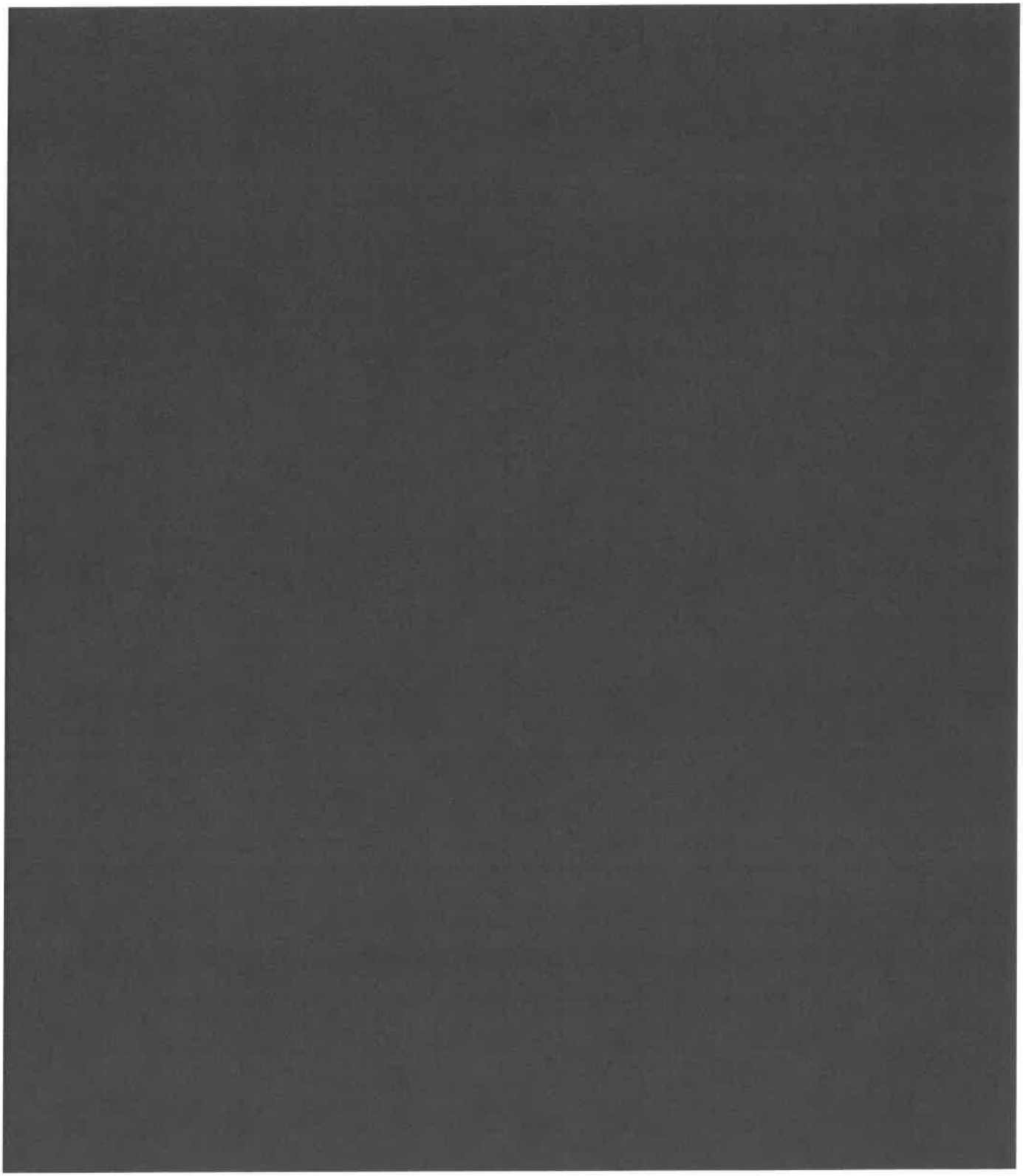
CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

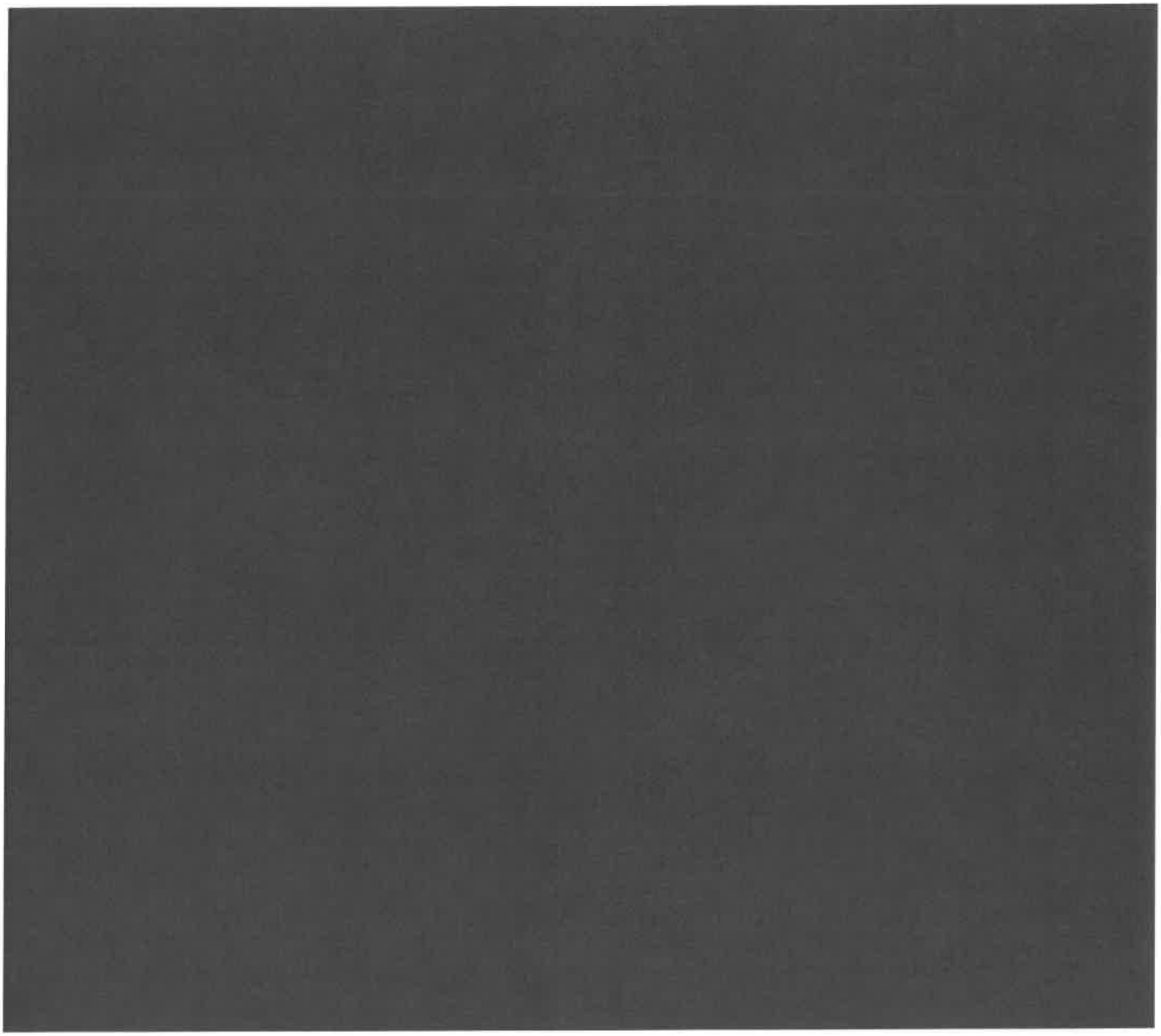






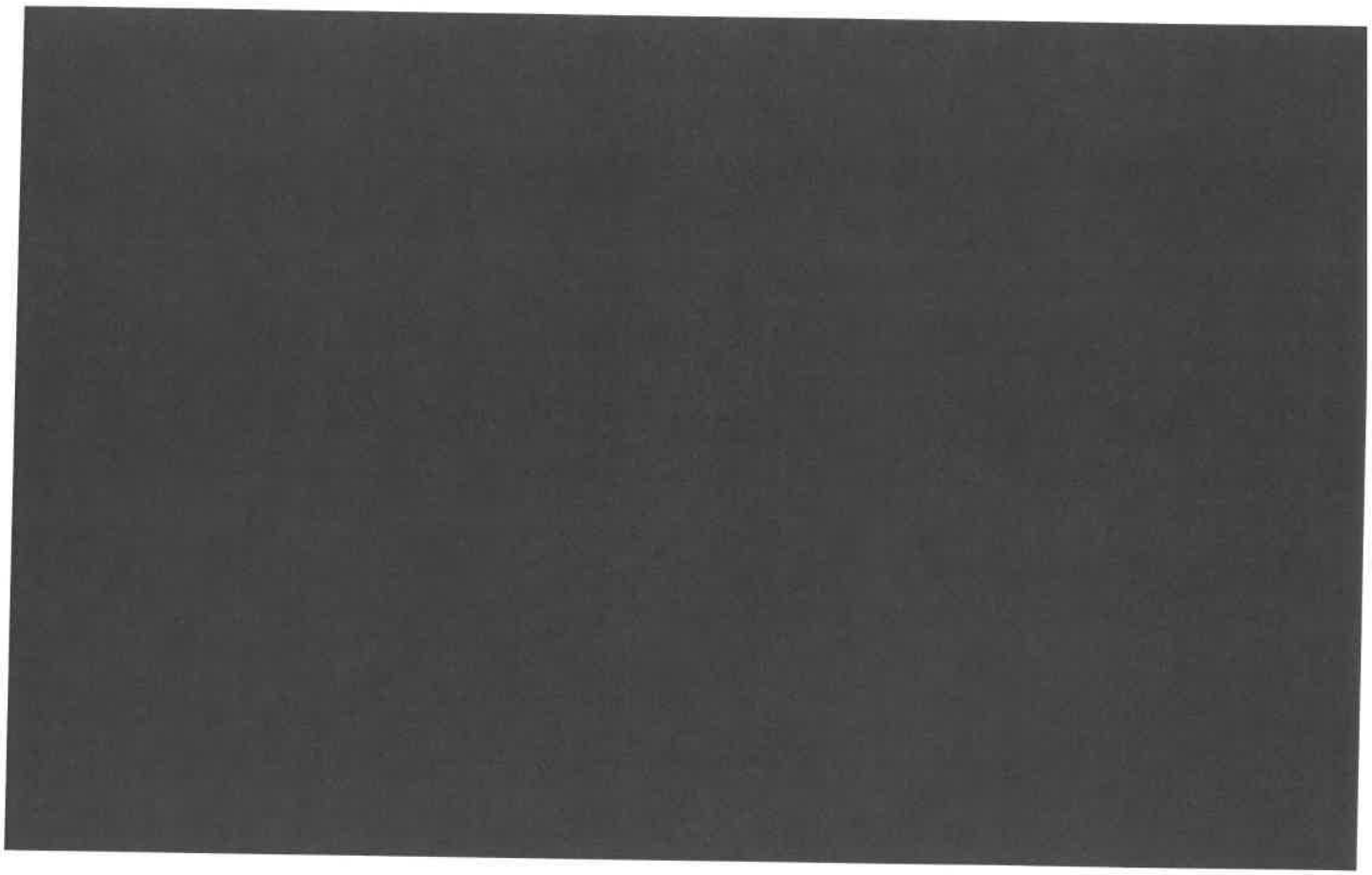
CONFIDENTIAL PROPRIETARY INFORMATION

All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



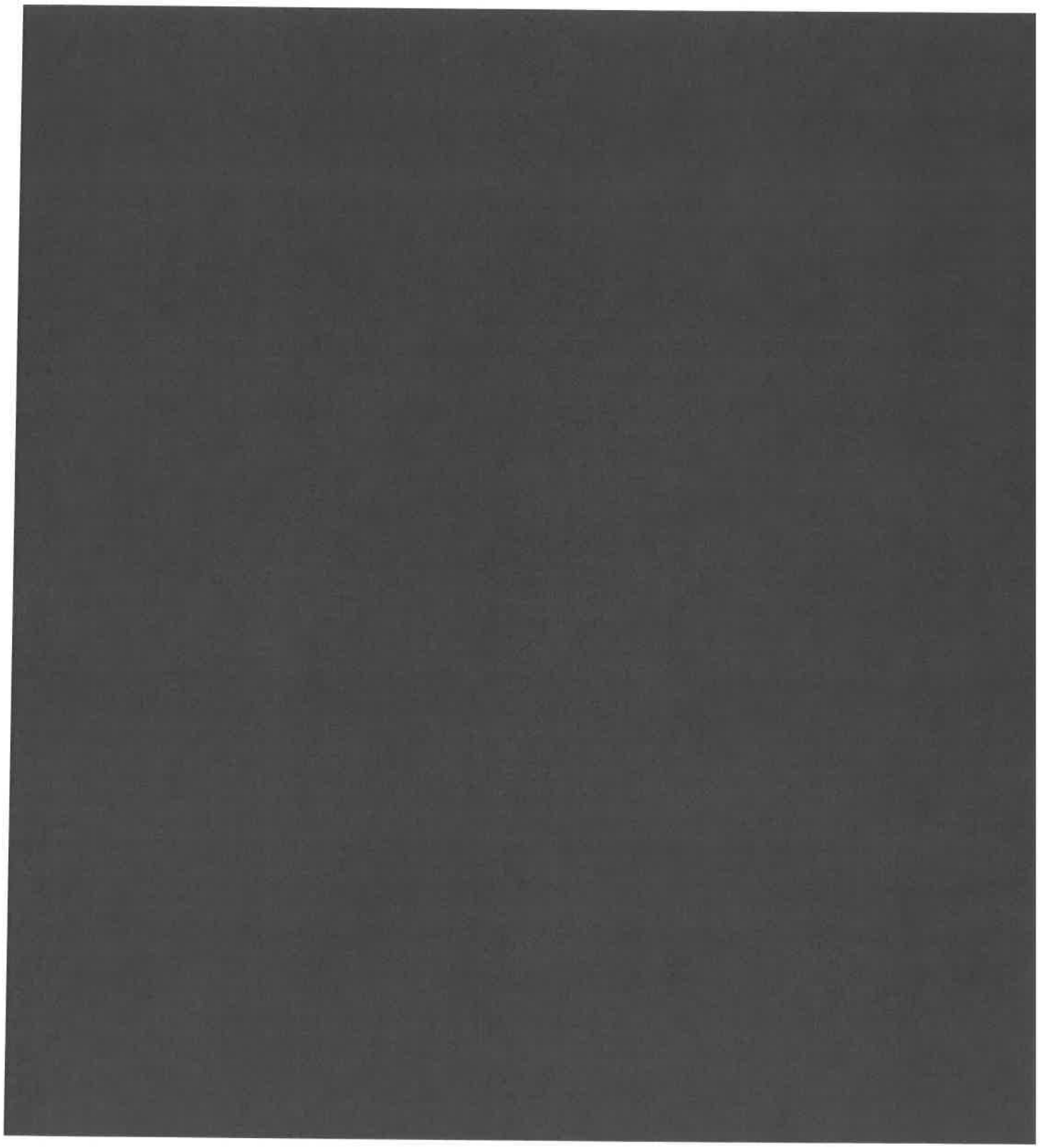
CONFIDENTIAL PROPRIETARY INFORMATION

All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



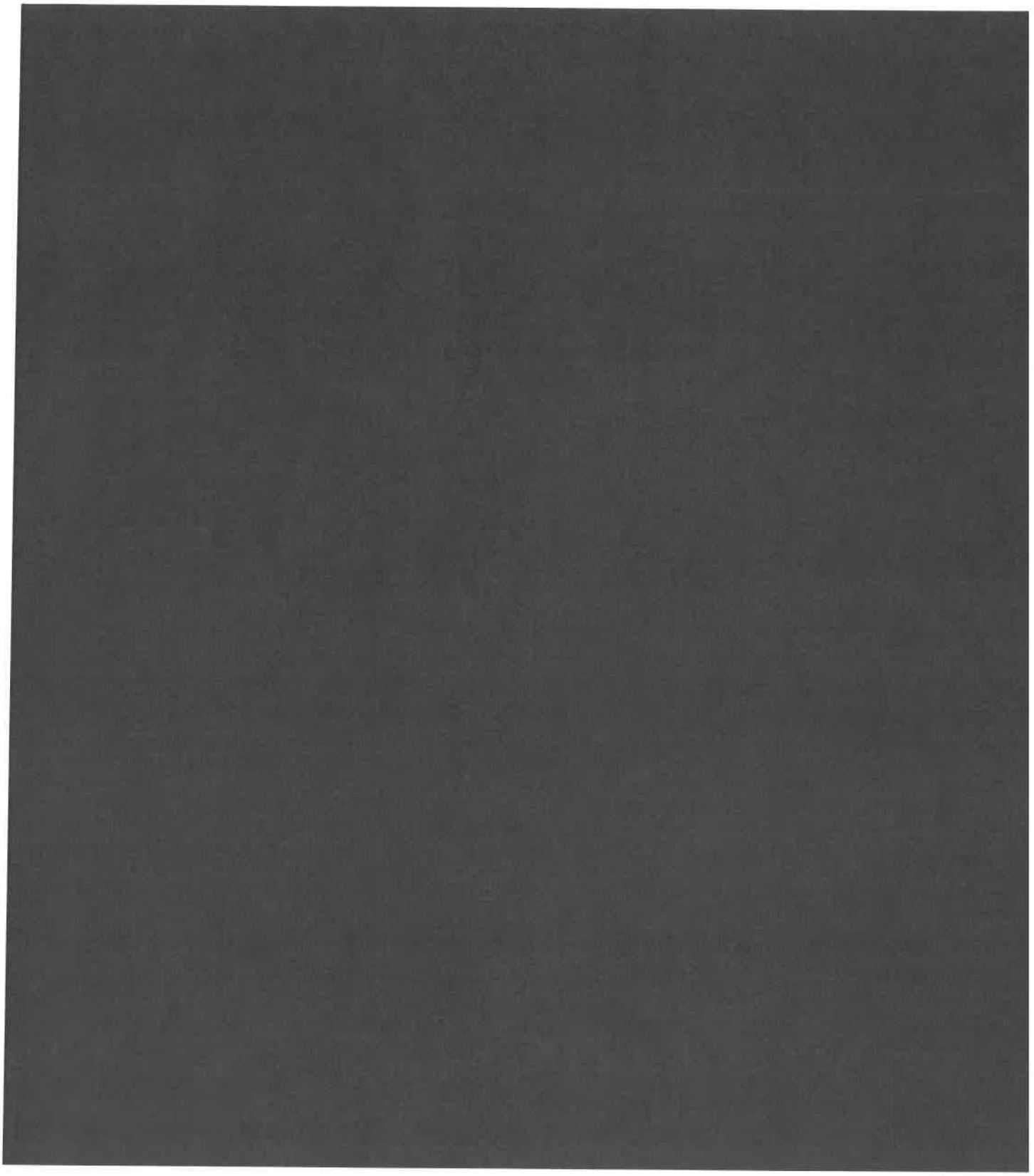
CONFIDENTIAL PROPRIETARY INFORMATION

All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.

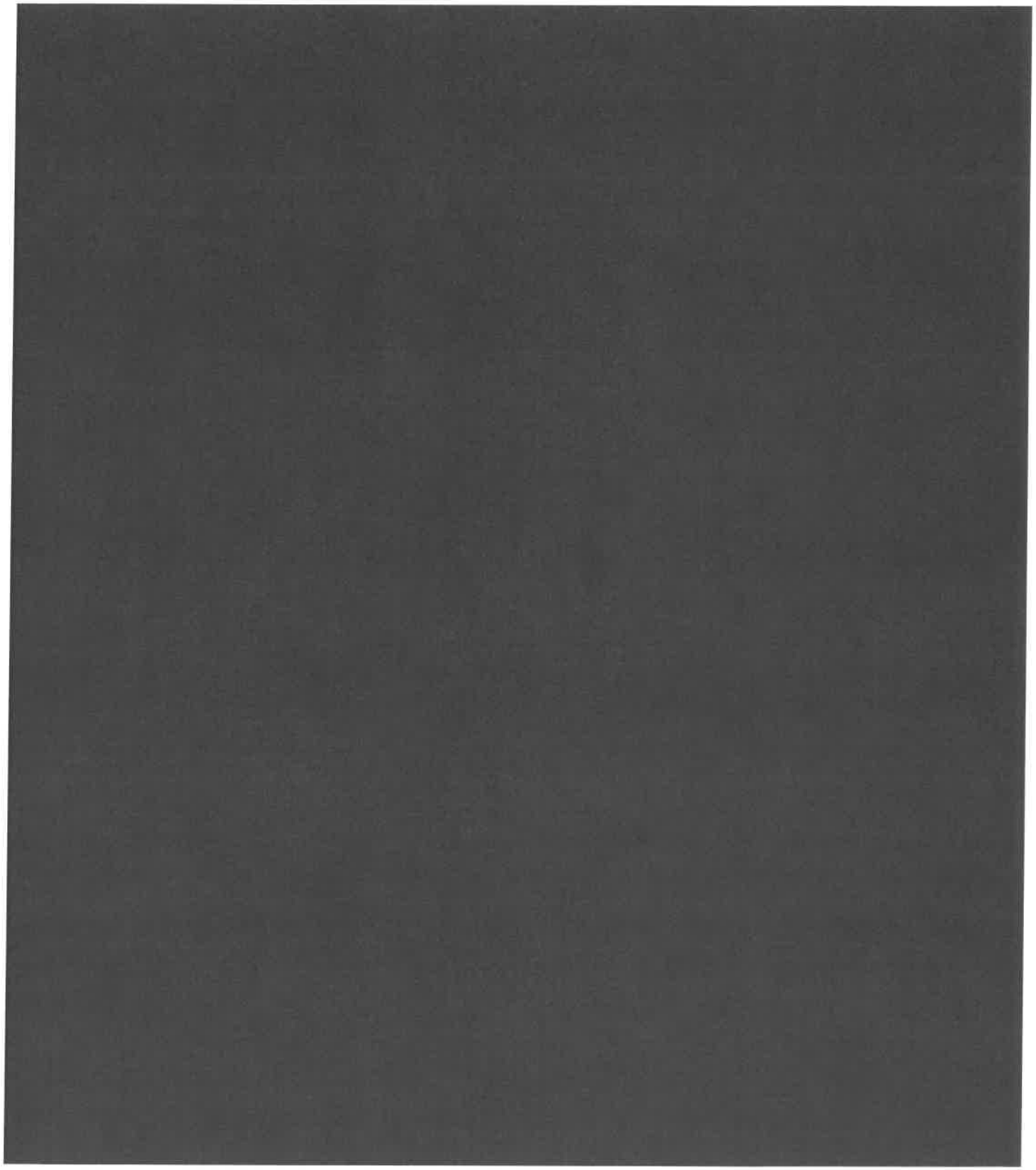


CONFIDENTIAL PROPRIETARY INFORMATION

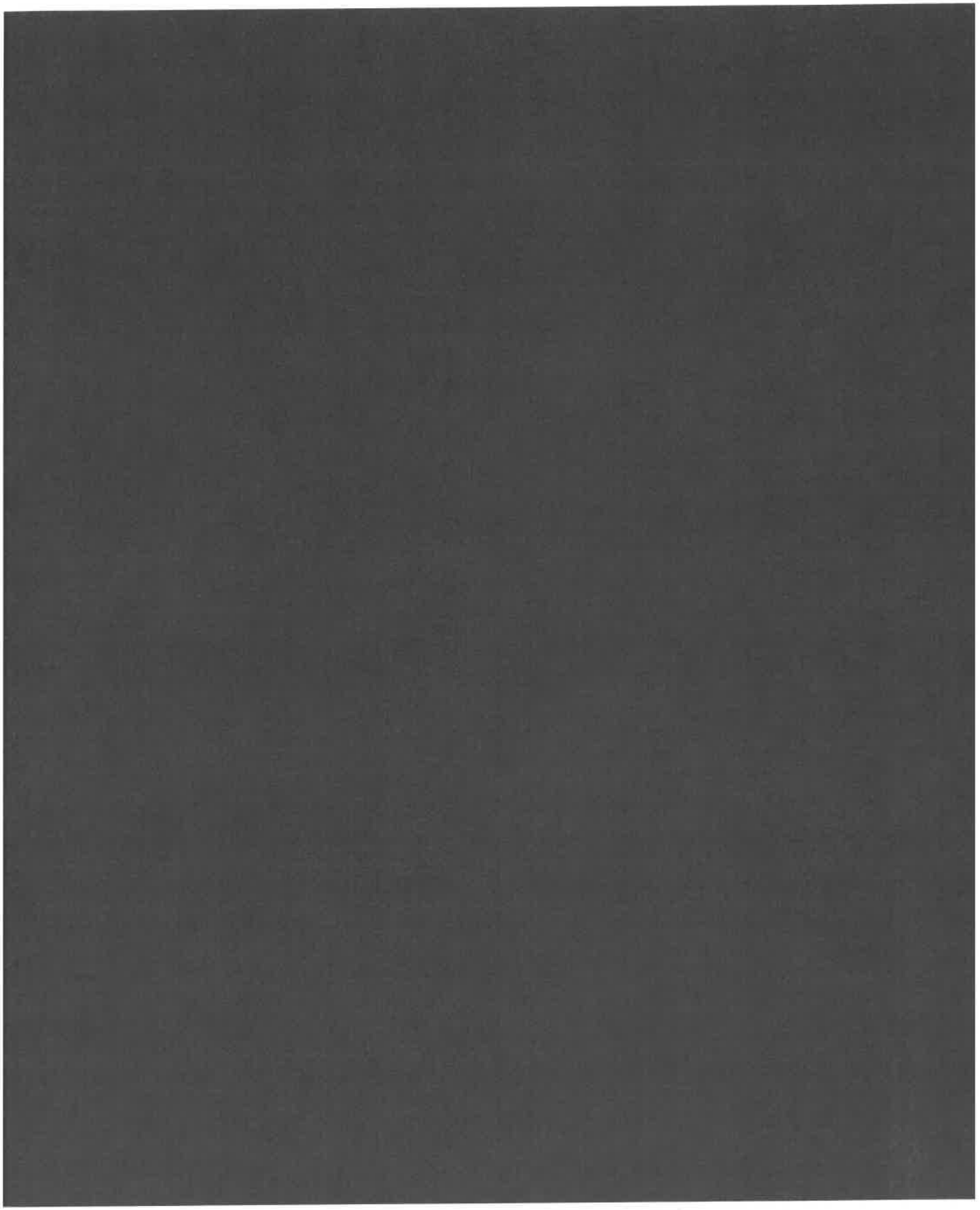
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



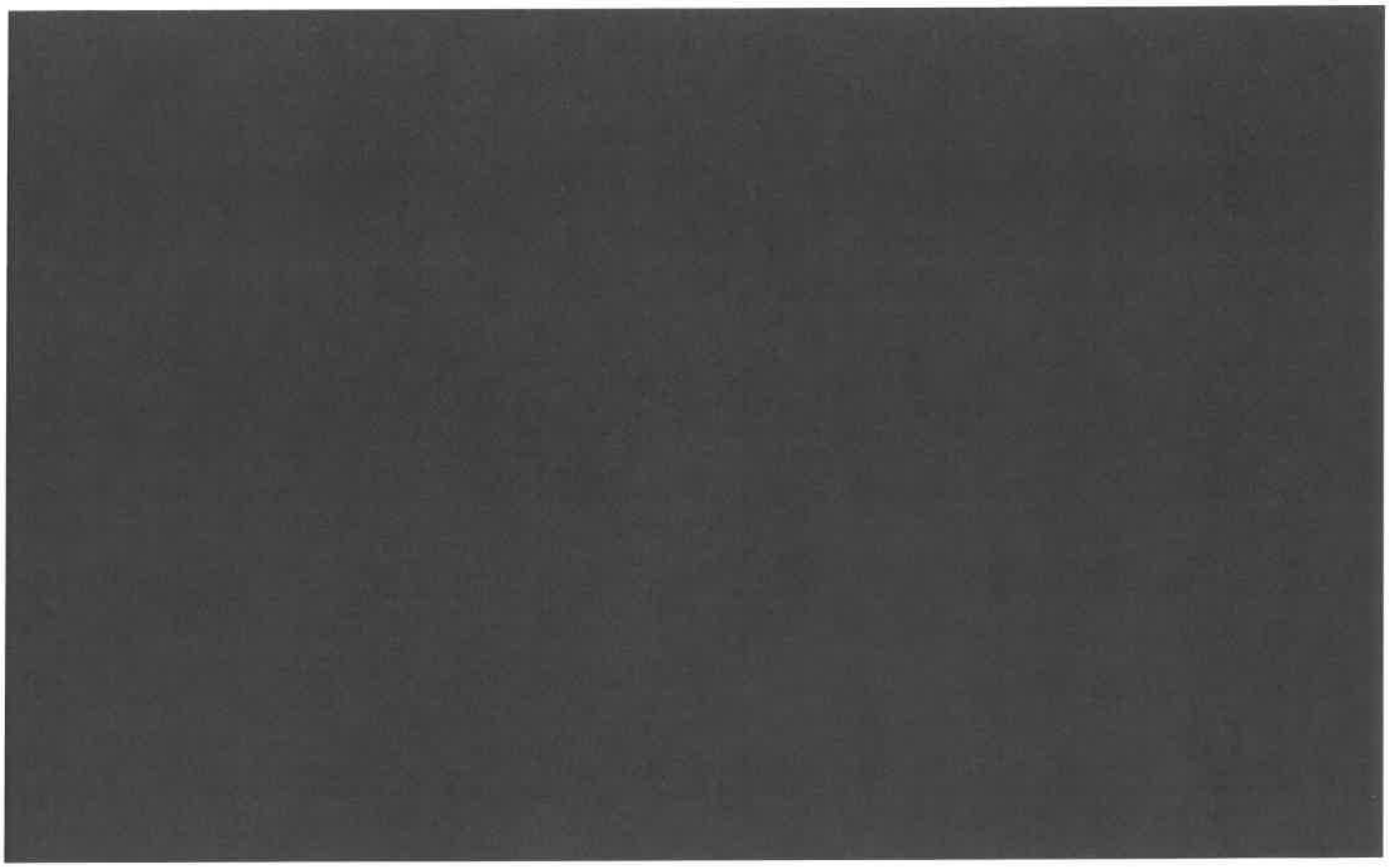
CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



CONFIDENTIAL PROPRIETARY INFORMATION
All information contained in these documents is considered confidential and proprietary for the use of only the intended receiver.



SECURITY AND HOSTING OVERVIEW

June 2015

SAP Fieldglass

SAP

Table of Contents

1 INTRODUCTION 4

1.1 SCOPE OF OPERATIONS 5
1.2 SECURITY MANAGEMENT 6
1.2.1 SECURITY POLICIES, STANDARDS AND PROCEDURES 6
1.2.2 RISK MANAGEMENT 6
1.2.3 ASSESSMENTS 7
1.3 APPLICATION SECURITY 8
1.3.1 ENCRYPTION 8
1.3.2 DATABASE SEGMENTATION 8
1.3.3 DOCUMENT ENVELOPES 8
1.3.4 PAGE-LEVEL ACCESS CHECKING 9
1.3.5 URL ENCRYPTION 9
1.3.6 ACTIVITY LOGGING 9
1.3.7 APPLICATION TESTING 9
1.3.8 PASSWORD MANAGEMENT 10
1.3.9 EMAIL APPROVALS 10
1.3.10 APPLICATION PENETRATION TESTING 11
1.4 PHYSICAL SECURITY 11
1.4.1 INTERNET DATA CENTER CONSTRUCTION 11
1.4.2 ACCESS CONTROL 11
1.4.3 MAN TRAPS 12
1.4.4 KEY CONTROL 12
1.4.5 ALARM SYSTEM 12
1.4.6 CLOSED CIRCUIT TELEVISION SYSTEM 12
1.4.7 BACKGROUND CHECKS 12
1.4.8 HOSTING FACILITY SECURITY PERSONNEL 13
1.5 NETWORK SECURITY 13
1.5.1 REDUNDANT COMPONENTS 13
1.5.2 PRIVATE VIRTUAL LANS 13
1.5.3 FIREWALL 13
1.5.4 24/7 MONITORING 14
1.5.5 ENTERPRISE SIEM 14
1.5.6 NETWORK PEN TESTING 14
1.6 DATA MANAGEMENT 14
1.6.1 DATA BACKUPS AND REPLICATION 14
1.6.2 DATA ARCHIVING 14
1.6.3 DATA DELETION 15
1.6.4 DATA USAGE 15
1.6.5 DATA SCRUBBING 16
1.6.6 DATA ACCESS 17

1.6.7 DATA LOSS PREVENTION 18
1.6.8 CUSTOMER TERMINATION 18

2 RELEASE MANAGEMENT 19

2.1 RELEASE MANAGEMENT PROCESS 19

3 DISASTER RECOVERY AND BUSINESS CONTINUITY PLAN 21

3.1 DISASTER RECOVERY 21
3.2 BUSINESS CONTINUITY 21

1 Introduction

This document provides a general overview of the SAP Fieldglass security and hosting infrastructure. It is effective as of the revision date indicated below. However, as security needs continue to evolve, the specific information relating to the topics covered may be subject to change over time.

Security

The SAP Fieldglass solution was architected to be the most reliable and secure Vendor Management System available today.

SAP Fieldglass is proud to offer our customers, subject to review and acceptance by our audit partner, the following assurances:

- ISO 27001 certified since 2011
- SSAE 16/ISAE 3402 Type 2 SOC1 audits conducted since 2005
- SSAE 16 Type 2 SOC2 audits in the Trust Services Principles for:
- Security – the system is protected, both logically and physically, against unauthorized access
- Availability – the system is available for operation and use as committed or agreed to
- Processing Integrity – system processing is complete, accurate, timely, and authorized
- Confidentiality – information that is designated as "confidential" is protected as committed or agreed
- SSAE 16 Type 1 SOC2 audit in the Trust Services Principle for Privacy (Type 2 audit scheduled for Q3 2015)
- Annual third party pen testing of our network and application

This document provides an understanding of how SAP Fieldglass handles the following areas across its global operations:

- Scope of Operations
- Security Management
- Application Security
- Physical Security
- Network Security
- Data Management
- Release Management
- Disaster Recovery
- Business Continuity

1.1 Scope of Operations

SAP Fieldglass has global operations located in the following regions:

United States

Business office

SAP Fieldglass
111 N. Canal Street
Suite 600
Chicago, IL 60606

Active and passive datacenters

Century Link
2425 Busse Road
Elk Grove Village, IL 60007

Equinix / ServerCentral
1735 Lundy Avenue
San Jose, CA 95131

APAC

Business office

SAP Fieldglass
Suite 5, 48 Lovett Street
Manly Vale
NSW 2094
Australia

European Union

Business office

SAP Fieldglass
One Valentine Place
London
SE1 8QH
United Kingdom

Active and passive datacenters

ServerCentral c/o Equinix Laarderhoogtweg 57 1101EB Amsterdam, Netherlands	ServerCentral c/o Telehouse North 14 Coriander Avenue London E14 2AA United Kingdom

The terms "active" and "passive" designate which of the production hosting environments is being used as the primary (active) and which is being used as the backup (passive or disaster recovery). These designations are not static and SAP Fieldglass will occasionally fail over the active hosting environment to the passive hosting environment. This practice ensures that SAP Fieldglass is capable and ready in the unlikely event a disaster occurs and we need to fail over to the passive site.

1.2 Security Management

SAP Fieldglass' Security Team is responsible for implementing and maintaining the security controls to ensure that SAP Fieldglass information systems are secure. SAP Fieldglass has based its security program on industry standards and best practices. For our established datacenters, these practices are audited annually by a third party with results available to customers in October.

1.2.1 Security Policies, Standards and Procedures

SAP Fieldglass maintains a comprehensive set of policies that define the information security goals and objectives. Each policy may be supported by a standard that dictates the required security requirements to ensure the uniform application of technologies and processes.

1.2.2 Risk Management

SAP Fieldglass manages risk by the identification of threats and vulnerabilities to its information systems and through a control selection process. Controls selected fall into the following categories:

- Policy
- Physical and Environmental Security
- Organizational Security
- Communications and Operations Management
- Acceptable Use
- Access Control
- Third Party Access
- Information Systems Acquisition, Development and Maintenance
- Asset Management
- Incident Management
- Personnel Security

- Compliance

As an element of our ISO 27001 compliance, SAP Fieldglass conducts an enterprise-wide risk assessment. Key individuals from every department are interviewed so that risks can be identified. Risks are then evaluated and entered into a risk treatment plan. This plan is managed by the Security team with oversight by the Security Steering Committee. The Security Steering Committee meets on a quarterly basis.

1.2.3 Assessments

SAP Fieldglass periodically assesses the security controls to review the effectiveness of each control in addressing risk. If SAP Fieldglass' assessment suggests a need for changes, the baseline standard may be changed to include additional controls.

Internal Audit

SAP Fieldglass conducts quarterly internal audits for critical controls. Evidence is reviewed by our Sr. Compliance Analyst and a formal assessment report is prepared. Failed controls are made visible by this process so they can be remediated. Executive sign off on the internal audit reports is required.

External Audit

SAP Fieldglass also contracts with third parties on an annual basis to perform formal security audits on the following:

- ISO 27001 surveillance audit
- SSAE 16/ISAE 3402 Type 2 SOC1 audit
- SSAE 16 Type 2 SOC2 audits in the Trust Services Principles for:
- Security
- Availability
- Processing Integrity
- Confidentiality
- SSAE 16 Type 1 SOC2 audit in the Trust Services Principle for Privacy (Type 2 audit scheduled for Q3 2015)
- Network penetration test
- Application penetration test

These assessments allow SAP Fieldglass to maintain an appropriate security posture in order to protect the company and its systems, as well as its customers' data.

We are currently working with our third party audit partner in bringing our EU datacenters into scope for our 2015 ISO 27001 audit and SSAE 16/ISAE 3402 Type 2 SOC1 and SOC2 examinations.

1.3 Application Security

Our application provides application-level security through a combination of encryption, page-level access checking, document envelopes, and activity logging. Application security is handled through a combination of programming checks, application server configuration, and database server configuration. SAP Fieldglass uses 128-bit SSL (HTTPS) encryption for all data transmissions over the public Internet, including data shared between the product and end users and data shared between the product and back-end systems.

Passwords are encrypted using a one-way hash with salt based on the SHA-256 encryption algorithm. The hash value is saved within the database; not the password.

The base SAP Fieldglass application does not require data that would require breach notifications if compromised. If the customer chooses to store sensitive data, custom fields may be defined by the customer that can be encrypted with AES-256. These fields can also be optionally masked from view while entering and viewing the fields in the application.

1.3.1 Encryption

By default, the application utilizes SSL encryption for all data transmissions over the public Internet.

In addition, the SAP Fieldglass hosted application encrypts sensitive data stored on the database so that only properly authorized users (or systems) will be able to decrypt the data. Because no state information is stored on the application server, in the unlikely event of unauthorized access to the database, the sensitive data is still encrypted.

1.3.2 Database Segmentation

SAP Fieldglass is a SaaS and utilizes a multi-tenancy database. Each customer is assigned a unique company code. Every record written to the database is keyed using this company code. After a user authenticates into the system, a session ID is generated which holds vital information about the user including their company code, user role, and data visibility restrictions. The session ID is cached server side to eliminate any ability for a malicious user to modify its contents.

1.3.3 Document Envelopes

Throughout the system, there are a number of events that generate "documents." These are digital representations of their real-world counterparts. For example, job postings, work orders, time sheets, and invoices are all represented in the system as documents.

Each document in the system has an accompanying digital envelope that stores all access to that document. For example, when a job posting is created, an envelope entry is added for creation that records the date, time, and person. When it is submitted, another entry is added recording the date, time, and person.

1.3.4 Page-Level Access Checking

The application has been designed so that every single web page checks for access rights before displaying itself. Additionally, each page performs a second check to ensure that an authorized user will only have access to those data elements and functionality that has been expressly authorized by the system administrator.

The post-authentication session ID that is generated and cached server-side is validated prior to showing each page. SAP Fieldglass stores a non-persistent cookie in the browser and compares back to the server-side session ID. If they no longer match due to malicious activity, the user is redirected to a "You are not authorized" page.

Authorization is handled through the use of user-defined User Roles. User Roles provide the customer, through its designated administrators, the flexibility to specify the type of access given to a member of that user group based on the definitions configured by the administrator. The User Role controls what areas of the application are accessible to the user group and what actions they can perform in those areas (e.g. job posting create, time sheet approve, etc.).

1.3.5 URL Encryption

SAP Fieldglass does not pass any sensitive data in its URL query strings. Parameters that are used to identify users in the system are protected by anonymizing the field variable and then encrypting the associated value using AES-256.

1.3.6 Activity Logging

As users access the system, all of their business significant activities are tracked and logged including failed login attempts, successful logins, approvals, submissions, etc. This activity log provides a full audit trail of what actions a particular user performed within the system and the timestamp as well.

1.3.7 Application Testing

Upon request, SAP Fieldglass will provide customers with a sandbox environment where system testing can occur outside of production. This is useful when testing out configuration changes, new integrations, and/or new reports prior to making the changes live in the customer's production instance.

Upon request, customer's data can be anonymized. SAP Fieldglass has the ability to scrub the data such that it is unrecognizable. Data element replacement is accomplished by an automated SAP Fieldglass utility that replaces the customer's company code, user names, business units, cost centers, and sites from a store of random variables. Any or all of these elements may be chosen for replacement.

Sensitive data that has been designated by the customer to be stored in the SAP Fieldglass application is encrypted with AES-256. The encryption and decryption keys are different between production and test environments and are different between the US and EU datacenters. These keys are stored in the corporate password vault and are accessible only by the Database Administrators and the Lead Architect.

Once customer testing has been completed, the Environment Management team (a team within Professional Services) destroys the environment. The database is purged and the VM is returned into circulation.

1.3.8 Password Management

The SAP Fieldglass application provides each customer the ability to define a Password Policy. This policy contains custom-defined password rules that each user in the customer's instance must adhere to. The policy provides 20 different password rules such as minimum length, user lockout preference (hard lockout vs. time-based reset), days to expiration, minimum password age, etc. Also included is the ability to specify a regex pattern(s). This pattern dictates the password value syntax that each user must follow.

When customer chooses to use a test instance ("sandbox"), all user password values remain unchanged from their production values. All passwords and visibility restrictions remain unchanged to ensure that users in the test instance are not able to gain access to data they're not privileged to see in production. Also, the password policy that is enforced in in the production instance is also enforced in the test instance.

New user invitations are sent via email. Recipients enter their 1-time passcode and are then forced to specify a new password that complies with the customer's password policy rules. User invitations expire after 21-days.

1.3.9 Email Approvals

In order to better support our growing mobile workforce, SAP Fieldglass offers customers a supplementary method for approving their work items. Via email, approvers are able to submit their approval or rejection response by simply replying to the approval work item that was sent to them. This method has been proven to reduce approval cycle times by several days since the approver does not have to be in the office. This feature has been architected with the following security controls:

- Only the original recipient can approve/reject the work item. If the recipient forwards the email to another person, the system will not accept the response.
- Email spoofing is not a risk. A unique ID is generated for each approval request. This unique ID along with the person ID of the intended recipient is stored encrypted with AES-256. So even if the email address sending the approval/rejection response is legitimate but the sender is not, the system will detect this anomaly and not accept the response.
- A SAP Fieldglass approver can identify another user as their Proxy and/or Delegate when they will be out of the office and unable to handle the approval requests. By design, neither of these roles receive approval work items via email. So only the original recipient can ever submit an approval/rejection response via email.
- If the customer created custom fields where sensitive information is stored encrypted, those fields and associated values are not allowed to be selected for inclusion in these email approval notifications.
- The system audit trail is updated with all user actions including approval/rejection activities via email. This audit trail is accessible by privileged customer users and can be used to monitor user activity.

In order to compromise the security of our email approval feature, a malicious user would need to hack into another user's email account, locate the SAP Fieldglass approval request email, and then submit the approval/rejection response.

1.3.10 Application Penetration Testing

SAP Fieldglass uses a combination of manual and automated testing to ensure the application is secure. Various automated commercial tools are used prior to each major release of the SAP Fieldglass system (three times per year).

On an annual basis, SAP Fieldglass engages a 3rd party security company to conduct pen testing services against our application. This is in addition to SAP Fieldglass' own internal penetration testing efforts.

SAP Fieldglass has several test environments available for customers to conduct their own application penetration testing if requested.

1.4 Physical Security

The SAP Fieldglass data center provides physical security through its secure hosted facilities. The application is hosted within a secure unmarked cage. SAP Fieldglass manages everything from the cage in. Meaning, SAP Fieldglass manages all servers, devices, and software in the cage. The hosting provider provides physical security, internet connectivity, and HVAC.

1.4.1 Internet Data Center Construction

Exterior perimeter walls, doors and windows are constructed of materials that afford UL Standard #752, Level V Ballistic Protection.

1.4.2 Access Control

The data center uses an Access Control System (ACS), which supports a networked card reader and alarm system. The ACS uses proximity card readers to control access into perimeter doors, shipping/receiving areas, storerooms and other areas. Biometric hand scanners are installed to control access into the network control center, telecommunications node room and customer vaults. Additional access control measures include:

- Designated with signage as controlled access areas
- Areas within the internet data center are designated as restricted
- Access into the internet data center and restricted areas is controlled by biometric hand scanners, and is limited to authorized personnel
- Card access badges or contractor/visitor badges are required to gain entry
- All employees, customers, vendors, contractors and visitors must be sponsored by a facilities pre-approved sponsor to gain access
- Visitors are escorted at all times within the controlled access area perimeter

1.4.3 Man Traps

The system includes the following key features:

- Anti-passback
- Integrated metal & explosive detection
- Video monitored / recorded
- Two-way intercom audio to Security Control Room
- Level V ballistic protection
- Weight sensors limit entry to one person at a time (no tailgating)
- ADA compliant
- Intrusion / tampering alarm monitoring by Security Control Room
- Integrated card access & biometric access control systems limits access to persons verified by hand geometry
- All systems are supported by redundant power management system (generators).

1.4.4 Key Control

Facilities security staff is the custodian of all security and cage keys. These keys are maintained and tracked through a comprehensive issue, retrieval, audit, and storage process. The listing of all customers, customer employees and cage assignments is updated in real-time maintained to ensure that cage access is restricted to authorized personnel.

1.4.5 Alarm System

The ACS is used to monitor and log security alarms. The ACS monitors all:

- Perimeter doors
- Restricted Area doors
- Shipping / receiving doors

1.4.6 Closed Circuit Television System

Facilities employ an extensive closed circuit television system to monitor the exterior and interior of the internet data center. Exterior cameras provide views of critical support equipment and perimeter doors. Interior cameras are positioned to monitor all internet data center aisle ways, requests for entry and entry into the internet data center, shipping / receiving areas, high-security vaults and the internet data center lobby. All cameras are recorded on digital video recorders 24 x 7.

1.4.7 Background Checks

SAP Fieldglass requires background checks be performed at the time of hiring on all personnel. These background checks are performed by a nationally recognized third party company. SAP Fieldglass initiates the background check request for all potential employees and independent consultants. If the independent contractor is placed through

an agency, the agency will conduct a background check and confirm with Human Resources whether the results were completed with/without discrepancies. If the independent contractor is placed directly, SAP Fieldglass will conduct the background check.

Background checks include the following:

- Social Security Trace
- Statewide & National Criminal Report (7 years)
- Sex Offender Registry & Terrorist Watch
- Compliance Authorities Database Checks – Global (OFAC level verification)
- Education verification
- Employment verification (7 years)
- Global Sanctions & Prohibited Parties
- Credit (only for specific finance roles)

1.4.8 Hosting Facility Security Personnel

The security office duties include:

- Response to calls for assistance
- Security facility inspections
- Fire and safety patrols
- Shipping / receiving security
- Physical security audits and assessments

1.5 Network Security

The SAP Fieldglass network infrastructure includes redundant components, firewalls, and 24/7 monitoring.

1.5.1 Redundant Components

Most network components are internally redundant. For example, routers have redundant power supplies; servers have redundant drives, power supplies, and NIC cards. Additionally, all network components are redundant to provide redundancy and security in the event of a component failure.

1.5.2 Private Virtual LANs

The application network architecture has been designed with multiple private virtual LANs using redundant Cisco routers. Every major network layer is placed on its own virtual LAN with rules about which protocols and ports are accessible.

1.5.3 Firewall

SAP Fieldglass has implemented dual-vendor redundant firewalls between the public internet and the SAP Fieldglass private network, as well as between each virtual LAN. This

firewall has been configured to enforce protocols and ports that are able to cross LANs with a default deny stance.

1.5.4 24/7 Monitoring

SAP Fieldglass provides 24/7 monitoring of suspicious activity. Any failure is promptly reported and, after an initial analysis, escalated to the next appropriate level.

1.5.5 Enterprise SIEM

Our security incident and event management (SIEM) tool has been configured to collect logs and events from all systems and devices within the SAP Fieldglass network. Forwarders are used to collect, filter, normalize and forward relevant data to an Indexer. Each installation listens for Syslog data and actively pulls WMI information from its respective environment. Security related issues are monitored and alerted on where required.

1.5.6 Network Pen Testing

On an annual basis, SAP Fieldglass engages a 3rd party security company to conduct pen testing services on our network.

1.6 Data Management

1.6.1 Data Backups and Replication

SAP Fieldglass has a highly available backup solution that guarantees data can be restored as expediently as possible. Our solution performs a continuous replication of data to our passive production hosting facility. SAP Fieldglass takes incremental SQL backups every 15 minutes and full backups on a nightly basis. Backups are transferred to the passive production hosting environment over a secure channel. SAP Fieldglass' solution offers continuous protection of customer data geographically without imposing performance degradation or scaling limitations. Data is encrypted both at rest and in transit with AES-256.

Data backups and replication are performed between the active and passive production environments. The US-based active production environment replicates data to the US-based passive environment. Likewise, The EU-based active production environment replicates data to the EU-based passive environment.

Also refer to section 3.1 Disaster Recovery.

1.6.2 Data Archiving

Data is archived throughout the year. Eligible transactional and reporting data are moved from the active database to an archive database after 24 months. Archived data can be accessed only by customer users with a user role of Administrator. Archive data is accessed using the same login screen and user interface that is used to access current data. Reports can also be generated using archive data from the standard interface.

The criteria for archiving data are as follows:

- Data remains in the active database for 24 months, at which point eligible data is moved to the archive database.
- Data remains in the active report database for 24 months, at which point eligible data is moved to the archive report database.
- Archiving begins with the worker. When a worker's end date is more than 24 months old, the worker and all associated data including the worker's work orders, job seeker record, job posting, time sheets, expense sheets, and payment-related items such as invoices are archived.
- The archive process is run as a batch job on a weekly basis to move data from the active databases to the archive databases.
- Data cannot be moved back from the archive database to the active database.

SAP Fieldglass does not delete data from its archive databases and has data older than 7 years. In the future, if SAP Fieldglass decides to delete archived data, we will ensure that a minimum 7 years of data is retained.

1.6.3 Data Deletion

Data deletion occurs only when required by a customer. SAP Fieldglass' data deletion capabilities allow customers to remain compliant with data privacy, data protection, and other related data directives.

- Deletion logic is based solely on a customer's business requirements. A custom script is developed by SAP Fieldglass.
- Results are verified in a non-production environment by both SAP Fieldglass and the customer prior to executing in production.
- A "Preservation" flag is available for use. Customers can set this flag on any data to override logic that would otherwise delete the data. This is useful during times when litigation or eDiscovery efforts are in progress and certain data must be preserved.
- Script execution frequency is determined by the customer.

SAP Fieldglass is contractually obligated to retain at least 7 years of data for customers.

1.6.4 Data Usage

Customer data is required in non-production environments for various reasons:

- Second level help desk support for customer defect investigation and resolution.
- Supporting customer requests for updating data, whether it be for desired changes or corrections for data modified by the customer in error.
- Customer sandboxes – these are non-production environments configured only with the customer's data (customer's data is "sliced" out from the multi-tenancy production database). These sandboxes are required for many

reasons, including testing of new or changed integration connectors, reports, and/or application configuration changes such as revised approval workflows. New application features can also be turned on and reviewed in the sandbox before turning on in the live production instance.

- Any data deletion scripts that are developed between the customer and SAP Fieldglass must be tested in a non-production environment prior to executing in production.
- Customer Preview testing – this is an opportunity for customers to gain early access to a future upgrade of the SAP Fieldglass application. This allows customers to gain confidence that the system is working as expected prior to the release date. Customer participation is optional.
- SAP Fieldglass regression testing – the SAP Fieldglass application is offered in a Software as a Service (SaaS) model. One of the services we provide is testing of the application prior to each production release. To ensure a customer's configuration, integrations, and reports are working as expected with the new codebase, SAP Fieldglass Quality Assurance uses a scrubbed production copy of the database in our regression testing. Regression testing is where we execute test cases against the current production codebase and the future codebase using a common data input. Output files from each test are compared to ensure any changes are expected.

Customers may opt out of this process. However, all responsibility in ensuring the customer's SAP Fieldglass instance is properly working and maintained is transferred to the customer.

To date, all SAP Fieldglass customers have declined to assume this responsibility.

1.6.5 Data Scrubbing

In order to properly service our customers, access to production data is required. All customer data is classified as Confidential. SAP Fieldglass takes every possible precaution to ensure data is protected from unauthorized access and misuse.

Data is protected in the following ways:

- First names and last names of buyers, suppliers, and workers are anonymized by replacing with a test value.
- Email addresses of buyers, suppliers, and workers are changed to a single false email address such as qatest8@SAP Fieldglass.com which is configured to automatically purge all email sent to it.
- Buyer and supplier company names are anonymized.
- Any custom fields created by the customer remain unchanged. Custom fields that contain sensitive data are encrypted with AES-256 and optionally display masked when entering and displaying values in the user interface. There is no way to decrypt these values since the decryption keys between production and test are different. Keys are stored in the corporate password vault and

access is limited to only select senior members of the technology team. This access list is reviewed quarterly by the internal audit team and by a third party in our annual SSAE 16 / ISAE 3402 Type 2 SOC1 and SOC2 audits.

The data scrubbing process is:

- A backup of the data is taken at the location where the source database resides
- Data is filtered where only the most recent 3 months of data remain
- Data is scrubbed as described above
- Data is then securely transferred from the production system to the test system

Once scrubbed, all personally identifiable information (PII) has been removed and any sensitive custom field data cannot be read.

Our test systems reside in secure third party data centers with the same controls as our production data centers.

1.6.6 Data Access

Direct access to production data is required in specific cases. Access is provided based on business need and not by role alone. Access reviews are conducted monthly and reviews are subject to recurring quarterly reviews by the SAP Fieldglass internal audit team. Executive review and sign off is performed for all quarterly reviews.

Access is required for the following puposes:

- Professional Services Data Services team – this team receives a customer's master and/or worker data and executes data uploads into test and/or production environments. Once the data are successfully uploaded and customer has signed off on the accuracy and completeness of the upload, the data are destroyed.
- First level help desk – when customers call our help desk, the caller may require the help desk agent to to view data or log in as the caller in order to help them with their problem. This is only performed when authorized by the caller.

SAP Fieldglass has help desk locations in the following regions:

United States

SAP Fieldglass
111 N. Canal Street
Suite 600
Chicago, IL 60606

Europe and APAC

Merlin-IT Hungary Information Technology Services Kft. Vagohid u. 2., 4034 Debrecen, Hungary	Merlin Information Systems Philippines Inc. 6th Floor C ommerce and Industry Plaza Building, McKinley Hill Cyberpark, Taguig City, Philippines

The SAP Fieldglass Security team conducted an onsite security audit in 2014 at Merlin Hungary. Contractually, Merlin must meet SAP Fieldglass' security requirements. The following security controls are in place:

- Help desk agents are not able to cut/paste using their secured workstation.
- External media including any USB drive is disabled.
- Printing is not supported.
- Help desk agents have been background checked by Merlin using SAP Fieldglass' background check requirements (see section 1.4.7 Background Checks).

1.6.7 Data Loss Prevention

Our DLP solution has been installed and configured for use on devices subject to exposure to sensitive information. It has been implemented to guard data at its endpoints and to ensure leakage of information classified as Confidential does not occur. Policies can be pushed from the central management console or pulled from an individual endpoint client. Client installs are configured to update (pull) policy changes every 90 minutes.

Our enterprise SIEM tool is configured to pull data in real time from the DLP database. Dashboards are created to allow quick overviews of agent statuses/details, alert details, and logging details.

The SIEM is configured to notify the Security Team in real time when an alert is detected. The Analyst then logs into the SIEM and investigates the alert to determine whether it's legitimate or a false positive.

1.6.8 Customer Termination

If a customer were to terminate their contract with SAP Fieldglass, the customer's data could be sliced out of the production database and delivered to the customer on a media of their choice. The size of the data will determine what media is appropriate.

2 Release Management

2.1 Release Management Process

The SAP Fieldglass Release Management team is responsible for the management of all delivables required in upgrading the production SAP Fieldglass system. This team is comprised of key members from the Development, Quality Assurance, Product Management, Professional Services, and executive teams. SAP Fieldglass customers benefit from our release management in that the release deployment schedule repeats itself year over year; releases are deployed over the same weekends of predetermined months.

SAP Fieldglass has several different release types:

Major Releases

In the US, Major releases occur on the second Fridays in March, July, and November. In the EU, Major releases occur on the third Fridays in March, July, and November

These releases can include new product features, new or changed functionality, user experience enhacements, and changes to the user interface. These are our most formal releases and the only type of release that requires an extended maintenance window. The Release Manager and the Release Management team closely monitor all phases of the Software Development Lifecycle and analyze PKIs at each phase transition. Release notes are provided as well as an opportunity for customers to optionally participate in a customer preview opportunity. This is where users can log into a non-production environment that is running the future codebase. The benefit of participating is that customers can gain confidence the system is behaving as expected prior to the official release date.

Minor Releases

Minor releases occur on the second Fridays in January, May and September.

These releases do not require the formalities of major releases. This type of release is used when deploying customer-specific product features and integrations to production. These releases are deployed to both US and EU customers at the same time.

Service Packs

Serivce packs are deployed as required to resolve product defects. These releases are deployed to both US and EU customers at the same time.

All releases are deployed to production by a central deployment team located in the US. During the deployment process, the codebase is replaced with the new codebase and data transformation scripts are executed. During this process, customer data is not viewed or accessed. Upon completion of the deploy, the Quality Assurance team executes a post-deploy verification checklist to ensure the system is ready for general availability. One such verification is verifying an MD5 hash to ensure the certified codebase was installed in production without modification. Test companies are used in conducting all testing.

3 Disaster Recovery and Business Continuity Plan

3.1 Disaster Recovery

SAP Fieldglass maintains a disaster recovery plan with backup, hardware repair, and data restoration, along with the ability to bring up the SAP Fieldglass application at a hot backup site in the event of a declared disaster (as described in the SAP Fieldglass disaster recovery plan) where the primary site is destroyed or disabled. This plan is tested on a yearly basis. Lessons learned are recorded in the test results and the plan is adjusted and improved accordingly.

SAP Fieldglass has the concept of active and passive production hosting facilities. The active environment is the live production hosted facility that all SAP Fieldglass users are actively using. The passive environment is a hot production hosting environment. Our data replication solution ensures that the passive environment is ready at anytime to be failed over to. In a disaster scenario, SAP Fieldglass changes the DNS to the passive hosting center's set of IPs. Users are then seamlessly routed to the other datacenter. There is not multi-day data migration that has to occur due to the ongoing data replication that is in place.

SAP Fieldglass proactively conducted a datacenter failover from the active datacenter to the passive datacenter in April 2015. The entire failover process was conducted in just over 8 hours with zero data loss. SAP Fieldglass plans to repeat this proactive datacenter failover between 1 and 3 times per year.

Also refer to section 1.6.1 Data Backups and Replication.

3.2 Business Continuity

The primary objective of our business continuity plan (BCP) is to enable SAP Fieldglass to recover all functions within their respective Recovery Time Objectives (RTOs) after any type of disruption occurs which prevents SAP Fieldglass personnel from engaging in ongoing business operations. A Recovery Point Objective (RPOs) has also been defined to identify our tolerance for any data loss. This Plan is designed to support the employees responsible for leading recovery efforts to enable SAP Fieldglass to resume daily operations following a disruption.

A business impact analysis (BIA) has been developed to fully quantify and prioritize restoration of mission-critical processes.



Privacy Policies and Procedures

Revision History

Virtru's Privacy Policies and Procedures were adopted as of **[Date]**.

Name

Virtru's Privacy Policies and Procedures were revised as of **[Date]**.

Name

Virtru's Privacy Policies and Procedures were revised as of **[Date]**.

Name

Virtru's Privacy Policies and Procedures were revised as of **[Date]**.

Name

Virtru's Privacy Policies and Procedures were revised as of **[Date]**.

Name

Virtru's Privacy Policies and Procedures were revised as of **[Date]**.

Name

Table of Contents

- Revision History
- Company
  - Document Control
  - Security Document Library
- Management and Protection of Personally-Identifiable Information
  - Overview:
  - Purpose:
  - Applicability:
  - Definitions:
  - Policy:
  - Enforcement:
- Administrative Requirements for HIPAA Implementation
  - Overview:
  - Purpose:
  - Applicability:
  - Policy:
  - Documentation Requirements:
  - Enforcement:
- Minimum Necessary Standard
  - Overview:
  - Purpose:
  - Applicability:
  - Policy:
  - Procedures:
  - Enforcement:
- Business Associate Agreements
  - Overview:
  - Purpose:
  - Applicability:
  - Policy:
  - Enforcement:
- Business Associate Subcontractor Agreements
  - Overview:
  - Purpose:
  - Applicability:
  - Policy:
  - Enforcement:
- Receipt, Use and Disclosure of Personally-Identifiable Information
  - Overview:
  - Purpose:
  - Applicability:
  - Special Definition:
  - Policy:
  - Procedures:
  - Enforcement:
- Complaint Process

Overview:
Purpose:
Applicability:
Policy:
Procedures:
Enforcement:
Scanner and Fax Policy
Overview:
Purpose:
Applicability:
Special Definitions
Corporate Policies:
Procedure:
Enforcement:
Scanner Policy
Overview:
Purpose:
Applicability:
Special Definitions
Corporate Policies:
Procedure:
Enforcement:
Training Policy
Overview:
Purpose:
Applicability:
Policy:
Enforcement:

I. Company

Virtru may be referred to as "**Company**."

A. Document Control

A staff copy of this document is available with the **Virtru** Privacy Officer, Will Ackerly, willackerly@virtru.com or (202) 577-3683.

B. Security Document Library

These policies and procedures and related privacy and security practice information will be kept in our Security Documentation Library (SDL). The Library is located in Google Drive and backed up to a local NAS.

Outdated and superseded materials from the Security Documentation Library (or Notebook) will be kept in an archive (the Security Documentation Archive) for at six (6) years after the date when they are first outdated or superseded.

II. Management and Protection of Personally-Identifiable Information

A. Overview

The Privacy Rules place certain restrictions on the acquisition, use and disclosure of Personally-Identifiable Information (PII). These policies establish the minimum care with which PII in the custody of **Virtru** personnel must be maintained.

B. Purpose

The purpose of this document is to provide basic instruction to all **Virtru** employees regarding the management and protection of Personally-Identifiable Information.

C. Applicability

This policy applies to all **Virtru** employees, which are defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru.**

D. Definitions

Covered Entity means a health plan, a health care clearinghouse, or a health care provider that transmits any health information in electronic form relating to any covered transaction.

Personally-Identifiable Information (PII) means any information about an individual maintained by **Virtru,** including:

1. Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

2. Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information

Treatment, Payment and Health Care Operations (TPO) include all the following:

1. *Treatment* means the provision, coordination, or management of health care and related services, consultation between providers relating to an individual, or referral of an individual to another provider for health care.
2. *Payment* means activities undertaken to obtain or provide reimbursement for health care, including determinations of eligibility or coverage, billing, collections activities, medical necessity determinations and utilization review.
3. *Health Care Operations* includes functions such as quality assessment and improvement activities, reviewing competence or qualifications of healthcare professionals, conducting or arranging for medical review, legal services and auditing functions, business planning and development, and general business and administrative activities including the creation of de-identified health information as defined by these regulations.

Disclosure means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Personal Representative means a person who has authority under applicable law to make decisions related to health care on behalf of an adult or an emancipated minor, or the parent, guardian, or other person who is authorized under law to make health care decisions on behalf of an un-emancipated minor.

Employees means all employees of **Virtru** as well as its temporary employees, interns, independent contractors, trainees, and other persons in the performance of work for the **Company**, its offices, programs or facilities.

Privacy Rules means the rules adopted by various state and federal agencies to implement the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations promulgated under this Act as well as those obligations that arise under the privacy and security standards adopted by the Health Insurance Marketplaces, pursuant to 45 C.F.R. §155.260.

E. Policy

For details on specific requirements, refer to the appropriate policies in this manual as indicated in *[brackets]*.

1. Generally: Personally-Identifiable Information shall not be obtained, used or disclosed except as permitted or required by law.

2. Permitted and Required Uses and Disclosures: Personally-Identifiable Information may or shall be disclosed as follows:

   a) To the individual

   b) To carry out TPO activities as allowed under HIPAA and/or pursuant to and in compliance with a current and valid Authorization *[Receipt, Use and Disclosure of Personally-Identifiable Information].*

   c) In keeping with a Business Associate Agreement *[Business Associate Agreement].*

   d) As otherwise allowed or required under the HIPAA Rules or other federal and/or state laws concerning privacy of information that is used by **Virtru** in the course of its business operations.

3. Minimum Necessary: Generally, when obtaining, using or disclosing Personally-Identifiable Information, or when requesting PII from another entity, reasonable efforts must be made to limit the PII used or disclosed to the minimum necessary to accomplish the intended purpose. However, the Privacy rules were not intended to severely complicate business processes and **Virtru** may, where appropriate, use a single format to provide data containing PII for our various services *[Minimum Necessary Standard].*

4. De-identified Personally-Identifiable Information: PII may be considered not to be individually identifiable in the following circumstances:

   a) The following identifiers of the individual (and relatives, employers or household members) are removed. (This is the "Safe Harbor" method that **Virtru** will generally use.)

      - Names
      - Information relating to the individual's geographic subdivision if it contains fewer than 20,000 people
      - Elements of dates (except year) directly related to the individual
      - All ages and elements of dates that indicate age for individuals over 89, unless aggregated into a single category of age 90 and older
      - Telephone numbers
      - Fax numbers

- Email addresses
- Social Security Numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate or license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers; full face photographic images
- Any other unique identifying number, characteristic or code.

b) As allowed in the Privacy Rules, **Virtru** shall provide a number of longitudinal identifiers in the de-identified data. These identifiers shall not allow identification of the individual who is the subject of this data in that:
   1) These identifiers will be encrypted using industry level encryption techniques
   2) The method of encryption shall not be divulged to the receiver of the de-identified data

5. Complaint Process: **Virtru** has put into place a process for individuals to make complaints about our Privacy Policies and Procedures and/or our compliance with those Policies and Procedures.

6. Documentation: **Virtru** must maintain written or electronic copies of all policies and procedures, communications, actions, activities or designations as are required to be documented under this manual for a period of six (6) years from the later of the date of creation or the last effective date.

F. Enforcement

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access or use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies. *[Sanction Policy]*

III. Administrative Requirements for HIPAA Implementation

A. Overview

The Privacy Rules require that a Business Associate have in place appropriate administrative safeguards to protect the privacy of Personally-Identifiable Information.

B. Purpose

To provide instructions regarding **Virtru**'s obligations relating to the implementation of administrative requirements of the Privacy Rules.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru**.

D. Policy

1. Personnel Designations: **Virtru** has designated and documented designations of the following:
   a. Will Ackerly has been designated as the Privacy Officer.
      1) He is responsible for the development and implementation of corporate-wide policies and procedures relating to the safeguarding of Personally-Identifiable Information.
      2) He will also be responsible for receiving complaints relating to Personally-Identifiable Information and for providing information about the **Company's** privacy practices.

   b. Persons with access to Personally-Identifiable Information are listed by title and department including a listing of individuals' names on the Risk Assessment; and will be updated if **Virtru** makes any major changes to processes, staff, programming or company location; or at a minimum annually. **Virtru** will retain the previous listing for a period of not less than six (6) years.

2. Training Requirements: **Virtru** shall document the following training actions: All **Virtru** employees shall receive training on applicable policies and procedures relating to Personally-Identifiable Information as necessary and appropriate for such persons to carry out their functions within the **Company**.

   a. Each new employee shall receive the training as described above within 30 days after joining **Virtru**.

b. Each employee whose functions are impacted by a material change in the policies and procedures relating to Personally-Identifiable Information, or by a change in position or job description, shall receive the training as described above within 30 days after the change becomes effective.

c. Complaints handled by Committee...

3. Safeguards: **Virtru** shall have in place appropriate Administrative, Technical, and Physical Safeguards to reasonably safeguard Personally-Identifiable Information from intentional or unintentional unauthorized receipt, use or disclosure.

4. Complaint process: **Virtru** shall have in place a process for individuals to make complaints about the **Company**'s HIPAA Policies and Procedures and/or **Virtru**'s compliance with those Policies and Procedures, and shall document all complaints received and the disposition of each complaint. (See Complaint Process)

5. Sanctions: Our Privacy Policies call for our workforce that has access to Personally-Identifiable Information to perform certain duties and to refrain from certain actions. Failure to do so will be sanctioned according to the policy below.

These sanctions apply to the designated workforce members including managers, supervisors, and staff who have access to Personally-Identifiable Information.
It is intended as guidance for our business management in sanctioning information security policy infractions. We reserve the right to implement sanctions differently if, in our judgment, the situation warrants it.

We define a serious infraction as one that results in known significant damage or that threatens imminent significant damage. Other infractions are simple infractions.

First security infraction

If the infraction is:

a. A simple infraction, and
b. The first infraction in the last 3 years

The sanction will be retraining the workforce member on the appropriate policy/procedure and placement of a written letter of reprimand in the employee file. The letter will notify the person of the nature of this infraction and of sanctions for future potential infractions.

Second security infraction or first serious infraction

If the infraction is:

a. A serious infraction, or

b. The second infraction of either type within 3 years

The sanction will include a written letter of reprimand that is given to the person at fault, placement of a copy of the letter in the employee file, and one week's suspension without pay. The letter will notify the person of the nature of this infraction and of sanctions for future potential infractions.

Third security infraction or second serious infraction

If the infraction is:

a. A second serious infraction within 3 years, or
b. A third infraction of any type within 3 years.

The sanction will be dismissal from the workforce.

Virtru makes exceptions for disclosures made by employees who qualify as whistleblowers or certain crime victims.

6. Mitigation efforts required: **Virtru**, to the extent practicable, shall mitigate any harmful effects of unauthorized uses or disclosures of Personally-Identifiable Information by the **Company** or any of its Business Associate Subcontractors.

7. Prohibition on intimidating or retaliatory acts: Neither **Virtru** nor any employee shall intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise of their rights or participation in any process relating to HIPAA compliance, or against any person for filing a complaint with the Secretary of the U.S. Department of Health and Human Services, participating in an investigation, compliance review, proceeding or hearing, or engaging in reasonable opposition to any act or practice that the person in good faith believes to be unlawful under the Privacy Rules as long as the action does not involve disclosure of Personally-Identifiable Information in violation of the regulations.

Virtru shall document the following actions relating to its policies and procedures:

a. Required policies and procedures: **Virtru** shall implement policies and procedures to assure appropriate safeguarding of Personally-Identifiable Information in its operations.
b. Changes to policies and procedures: **Virtru** shall change its policies and procedures as necessary and appropriate to conform to changes in law or regulation. **Virtru** may also make changes to policies and procedures at other times as long as the policies and procedures are still in compliance with applicable law. Where necessary, **Virtru** shall make correlative changes in its Privacy Notice.

E. Documentation Requirements

Virtru must maintain the required policies and procedures in written or electronic form, and must maintain written or electronic copies of all communications, actions, activities or designations as are required to be documented hereunder, or otherwise under the Privacy Rules, for a period of six (6) years from the later of the date of creation or the last effective date.

F. Enforcement

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

IV. Minimum Necessary Standard

A. Overview

The Privacy Rules place certain restrictions on the receipt, use and disclosure of Personally-Identifiable Information in regards to the amount reasonably necessary to accomplish the task being performed. However, the Privacy Rules also allow Personally-Identifiable Information to be disclosed for business appropriate needs.

The policies developed by **Virtru** will follow this business appropriate philosophy as well as that of administrative simplification, which is the subsection of the HIPAA law under which the Privacy Rule was developed. **Virtru** shall use standard data formats for information acquisition or disclosure and tailor these formats to contain a business reasonable minimum necessary amount of Personally-Identifiable Information. The **Company's** policies establish the minimum necessary use provisions for Personally-Identifiable Information in the custody of **Virtru** employees.

B. Purpose

To issue instructions regarding **Virtru's** obligations relating to the Privacy Rules to obtain, use and disclose only the minimum amount of Personally-Identifiable Information (PHI) necessary to accomplish the intended purpose.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of the **Company**.

D. Policy

Virtru will make reasonable efforts to ensure that the Minimum Necessary amount of Personally-Identifiable Information is disclosed, used, or requested to accomplish the intended purpose. Exceptions to the Minimum Necessary Standard include disclosures:

1. To the individual who is the subject of the information;

2. Made pursuant to an authorization provided by the individual;
3. To healthcare providers for treatment purposes;
4. Required for compliance with the standardized HIPAA transactions;
5. Made to the Secretary of HHS or his agent pursuant to a privacy investigation;
6. Otherwise required by the Privacy Rules or other law.

Employees shall be trained on the policies and procedures developed to apply these principles to the use or disclosure of, or requests for Personally-Identifiable Information.

E. Procedures

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of **Virtru**.

1. Each user of a system which accesses Personally-Identifiable Information shall be identified and the classes or types of PII to which access is needed and any conditions appropriate to such access will be established. It will be the responsibility of the Privacy Officer to maintain this information using the *Employee Access Request Form* [**Forms for Employees**] and *System Access Log* [**Change Control Logs for Security**].

2. Reasonable efforts will be taken to limit the access of each user of Personally-Identifiable Information to the amount needed to carry out the individual's duties. These efforts will include internal use of PII.

3. For situations where Personally-Identifiable Information disclosure occurs on a routine and recurring basis, the PII disclosed will be limited to the amount of information reasonably necessary to achieve the purpose of the disclosure.

4. Requests for disclosures that are not routine and recurring and thereby covered by **Virtru** standard procedures (other than to the individual, the Secretary of HHS or his agent, or where required by law) shall be reviewed by the Privacy Officer to determine that the Minimum Necessary Standard is applied to the extent reasonable.

5. Questions regarding these procedures should be directed to the **Virtru** Privacy Officer, Will Ackerly, willackerly@virtru.com, or (202) 577-3683.

F. Enforcement

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access or use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

V. Business Associate Agreements

A. Overview

The Privacy Rules impose certain requirements on Business Associates who create, receive, use or disclose Personally-Identifiable Information on behalf of their Covered Entity partners. **Vitru** must comply with the requirements in this section.

B. Purpose

To provide instructions to all **Virtru** employees regarding the necessity of and the requirements for Business Associate Agreements relating to Covered Entities.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru.**

D. Policy

1. Generally: A Covered Entity may disclose Personally-Identifiable Information to **Virtru**, or allow **Virtru** to create or receive PII on the Covered Entity's behalf. **Virtru** will appropriately safeguard the PII obtained from the Covered Entity. **Virtru** will document these assurances through a written agreement.

2. Content Requirements: The agreement between the Covered Entity and **Virtru** must meet the following requirements, as applicable:

    a. Establish permitted and required uses or disclosures of Personally-Identifiable Information that are consistent with those authorized for the Covered Entity, except that the agreement may permit **Virtru** to use or disclose Personally-Identifiable Information for its own management and administration if such use or disclosure is required by law, or **Virtru** provides reasonable assurance to the Covered Entity to which the Personally-Identifiable Information is disclosed that the confidentiality of the PII will be maintained.

    b. Provide that **Virtru** will:

        1. Not use or disclose the Personally-Identifiable Information except as authorized under the agreement or required by law.
        2. Use safeguards to prevent unauthorized use or disclosure.
        3. Report unauthorized uses or disclosures to the Covered Entity.

4. Pass on the same obligations relating to protection of Personally-Identifiable Information to any subcontractors.
5. Make Personally-Identifiable Information available for access by the Covered Entity in accordance with relevant law and policy.
6. Make Personally-Identifiable Information available to the Covered Entity for amendment, and incorporate any approved amendments to Personally-Identifiable Information, in accordance with relevant law and policy.
7. Make information available for the provision of an accounting of uses and disclosures in accordance with relevant law and policy.
8. Make its internal practices, books and records relating to its receipt or creation of Personally-Identifiable Information available to the Secretary of HHS for purposes of determining **Virtru's** compliance with Privacy Rules.
9. Authorize termination of the agreement by the Covered Entity upon a material breach by **Virtru**.

3. Compliance Responsibilities: Virtru agrees to report any use or disclosure of Personally-Identifiable Information not permitted by this agreement and any successful security incident to Covered Entity within a commercially reasonable period, but in no event later than within thirty (30) business days, after it is discovered.

E. Enforcement

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access or use of Personally-Identifiable Information was or may have been involved, these individuals may additionally be reported to the appropriate law enforcement agencies.

VI. Business Associate Subcontractor Agreements

A. Overview

The Privacy Rules impose certain requirements on Business Associate Subcontractors who create, receive, use or disclose Personally-Identifiable Information on behalf of **Virtru**. All Business Associate Subcontractors of **Virtru** must comply with the requirements in this section.

B. Purpose

To provide instructions to all **Virtru** employees regarding the necessity of and the requirements for Business Associate Subcontractor Agreements relating to Business Associate Subcontractors who receive, use or disclosure Personally-Identifiable Information on behalf of **Virtru**.

C. Applicability

This policy applies to all **Virtru** employees and Business Associate Subcontractors, which are defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru** and the Business Associate Subcontractor.

D. Policy

1. Generally: **Virtru** may disclose Personally-Identifiable Information to a Business Associate Subcontractor, or allow a Business Associate Subcontractor to create or receive PII on **Virtru**'s behalf, if adequate assurances are obtained by **Virtru** that the Business Associate Subcontractor will appropriately safeguard the PII. **Virtru** must document these assurances through a written agreement. This requirement does not apply with respect to:
   a. Disclosures made to a provider concerning the individual's treatment, payment or health care operations; or
   b. Uses or disclosures made to a governmental agency for purposes of public benefit eligibility or enrollment determinations where such company is authorized by law to make these determinations.

2. Content Requirements: The agreement between **Virtru** and a Business Associate Subcontractor must meet the following requirements, as applicable:

   a. Establish permitted and required uses or disclosures of Personally-Identifiable Information that are consistent with those authorized for the entity, except that the agreement may permit the Business Associate Subcontractor to use or disclose Personally-Identifiable Information for its own management and administration if such use, or disclosure is required by law, or the Business Associate Subcontractor obtains reasonable assurance from the entity to which the Personally-Identifiable Information is disclosed that the confidentiality of the PII will be maintained.

   b. Provide that the Business Associate Subcontractor will:
      1) Not use or disclose the Personally-Identifiable Information except as authorized under the agreement or required by law.
      2) Use safeguards to prevent unauthorized use or disclosure.
      3) Report unauthorized uses or disclosures to **Virtru**.
      4) Pass on the same obligations relating to protection of Personally-Identifiable Information to any subcontractors or agents.
      5) Make Personally-Identifiable Information available for access by **Virtru**, in accordance with relevant law and policy.

6) Make Personally-Identifiable Information available to **Virtru** for amendment, and incorporate any approved amendments to PII, in accordance with relevant law and policy.
7) Make information available to **Virtru** for the provision of an accounting of uses and disclosures in accordance with relevant law and policy.
8) Make its internal practices, books and records relating to its receipt or creation of Personally-Identifiable Information available to the Secretary of HHS for purposes of determining the Business Associate Subcontractor's compliance with Privacy Rules.
9) If feasible, return or destroy all Personally-Identifiable Information upon termination of contract; if any PII is retained, continue to extend the full protections specified herein as long as the PII is maintained.
10) Authorize termination of the agreement by the entity upon a material breach by the Business Associate Subcontractor.

3. Compliance Responsibilities: If **Virtru** knows of a pattern or practice of the Business Associate Subcontractor that amounts to a material violation of the Agreement, **Virtru** and the Business Associate Subcontractor must attempt to cure the breach to end the violation, and if unsuccessful, terminate the agreement. If terminating the Agreement is not feasible, **Virtru** must report the problem to the Secretary of HHS.

E. Enforcement

An employee of **Virtru** or an employee of the Business Associate Subcontractor found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access or use of Personally-Identifiable Information was or may have been involved, these individuals may additionally be reported to the appropriate law enforcement agencies.

VII. Receipt, Use and Disclosure of Personally-Identifiable Information

A. Overview

The Privacy Rules impose certain requirements on Covered Entities and Business Associates who create, receive, use or disclose Personally-Identifiable Information on behalf of their Covered Entity partners.

B. Purpose

To provide instructions to all **Virtru** employees regarding the receipt, uses and disclosures of Personally-Identifiable Information, which are permitted or required by HIPAA.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of the **Company**.

D. Special Definition

Public Health Authority means a governmental company or authority, or a person or entity acting under a grant of authority from or a contract with such a public company, including the employees or agents of the public company, its contractors and those to whom it has granted authority, that is responsible for public health matters as part of its official mandate.

E. Policy

State and federal law permit and require certain receipt, uses and disclosures of Personally-Identifiable Information such as those related to Business Associate Agreements. Additional uses and/or disclosures are allowed or required that related to public responsibility that require no agreement or authorization on the part of the individual who is the subject of the PII. It is the policy of **Virtru** to obtain, use and disclose PII only as permitted and/or required by law or regulation including the following situations:

1. Treatment, Payment or Healthcare Operations: Personally-Identifiable Information may be used or disclosed for the purposes of providing treatment, payment or healthcare operations. Such disclosures will be made only as allowed by and pursuant to prevailing state and federal law.
    a. Discussions involving Personally-Identifiable Information shall be conducted only in appropriate business areas including but not limited to offices, conference rooms and other non-public areas;
    b. Conducted only for the purpose of fulfilling a legitimate business need; and
    c. Conducted with regard to and in compliance with the "Minimum Necessary Standard." *[Minimum Necessary Standard]*

2. Contained in a Business Associate Agreement: For permitted and required uses or disclosures of Personally-Identifiable Information that are consistent with those authorized by the Covered Entity in a Business Associate Agreement.

3. Required by Law: Personally-Identifiable Information may be used or disclosed to the extent such use or disclosure complies with and is limited to the requirements of such law.

4. Abuse and Neglect: Except for reports of child abuse or neglect, Personally-Identifiable Information about an individual believed to be a victim of abuse, neglect, or domestic violence may be disclosed to a governmental authority authorized to receive such reports if the individual agrees or the reporting entity believes, in the exercise of professional judgment, that the disclosure is necessary to prevent serious physical harm. If the individual lacks the capacity to agree, disclosure may be made if not intended for use against the individual and delaying disclosure would materially hinder law

enforcement activity. The individual whose Personally-Identifiable Information has been released must be promptly informed that the report was made unless doing so would place the individual at risk of serious harm.

5. Judicial Proceedings: Personally-Identifiable Information may be disclosed in response to a court order.

6. Law Enforcement: Personally-Identifiable Information may be disclosed for the following law enforcement purposes and under the specified conditions:
    a. Pursuant to court order or as otherwise required by law, i.e. laws requiring the reporting of certain types of wounds or injuries
    b. Decedent's Personally-Identifiable Information may be disclosed to alert law enforcement to the death if entity suspects that death resulted from criminal conduct
7. Serious Threats to Health or Safety: Consistent with applicable law and ethical standards, Personally-Identifiable Information may be used or disclosed if the entity believes in good faith that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to a person or the public, and disclosure is to someone reasonably able to prevent or lessen the threat, or the disclosure is to law enforcement authorities to identify or apprehend an individual who has admitted to violent criminal activity that likely caused serious harm to the victim or who appears to have escaped from lawful custody. Disclosures of admitted participation in a violent crime are limited to the individual's statement of participation and are not permitted when the information is learned in the course of treatment to affect the propensity to commit the subject crime, or through counseling, or therapy or a request to initiate the same.

8. Specialized Government Functions: National Security and Intelligence: Personally-Identifiable Information may be disclosed to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other activities authorized by the National Security Act.(45 CFR 164.512(k)(2))

9. Protective Services: Personally-Identifiable Information may be disclosed to authorized federal officials for the provision of protective services to the President, foreign heads of state, and others designated by law, and for the conduct of criminal investigations of threats against such persons. (45 CFR 164.512(k)(3));

10. Public Benefits: Personally-Identifiable Information relevant to administration of a government program providing public benefits may be disclosed to another governmental program providing public benefits serving the same or similar populations as necessary to coordinate program functions or improve administration and management of program functions.

11. Workers' Compensation: Personally-Identifiable Information may be disclosed as authorized and to the extent necessary to comply with laws relating to workers' compensation and other similar programs.

F. Procedures

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of **Virtru**.

Any request for disclosure of Personally-Identifiable Information, 1) pursuant to a court order, warrant or subpoena; 2) by a law enforcement agent; 3) by a public health authority; or 4) by a national security, intelligence or other federal company, must be directed to the Privacy Officer and the CEO for review and action. Any such request will include an acknowledgement of receipt to insure that the document was actually received by the appropriate corporate individual and will retain a copy of the request. If the acknowledgement is not received within two working days of submitting to the appropriate corporate individual, then the request will be resubmitted to the Privacy Officer and CEO.

G. Enforcement

An employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

VIII. Complaint Process

A. Overview

The Privacy Rules require that **Virtru** provide a process for individuals to make complaints concerning the **Company**'s policies and procedures required by these regulations and document all complaints received, and the dispositions of these complaints, if any.

B. Purpose

To issue instructions regarding **Virtru** obligations relating to the Privacy Rules to provide a process for individuals to complain about the **Company**'s policies and procedures and the requirement to document complaints received and the disposition of these complaints.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru**.

D. Policy

Virtru shall maintain a process to receive complaints from individuals about **Company** Privacy Policies and Procedures, for complaints from individuals who believe their privacy rights have been violated and from employees or Business Associate Subcontractors who believe that **Virtru** is not abiding by its policies and procedures and/or assurances concerning Personally-Identifiable Information. This process shall include the following:

1. Any complaints or questions should be submitted to the Privacy Officer or his assistant.
2. All service and complaint issues will be stored in the Desk.com app.

Virtru shall work in good faith to resolve complaints received to the satisfaction of the submitter, where possible.

E. Procedures

The following procedures will be implemented to ensure that this policy is enforced effectively across all parts of **Virtru**.

1. Complaints shall be submitted in writing on paper or electronically.

2. Complaints shall be entered into the complaint tracking system either automatically or by the individual designated to provide information on the **Company** complaint process. and when manually entered shall be in the exact words provided by the submitter.

3. The **Virtru** Privacy Officer shall investigate complaints and make a determination as to whether or not the complaint has merit.

4. The **Virtru** Privacy Officer shall present complaints received to **Virtru**'s senior executive for immediate action.

5. If the Privacy Officer has completed the investigation of the complaint and made a determination, such determination shall be presented to the **Virtru** Executive Board

6. If the investigation has not been completed nor a provisional determination made by the Privacy Officer, it shall be the prerogative of the senior executive to make a summary determination or to direct the Privacy Officer to continue with the investigation and to report on the complaint at the next scheduled meeting.

If a determination is made that **Virtru** is in violation of the privacy provisions of the Privacy Rules or that changes are needed in the Privacy Policies or Business Associate Agreement to clarify the allowed practices of **Virtru**, the **Virtru** CEO and Privacy Officer shall determine the actions that the **Company** shall take.

Complaint determinations and actions that **Virtru** takes pursuant to such complaints, if any, shall be reported to the submitter of the complaint, if such person is known. Privacy Officer, or his designated agent, shall update the complaint tracking system with the findings of the Privacy Officer's investigation, any determination made, direction or actions of the **Virtru** CEO and Privacy Officer with regard to the complaint, and a copy of any information provided to the submitter in response to their complaint.

F. Enforcement

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

IX. Fax Policy

A. Overview

The Privacy Rules require that **Virtru** implement appropriate administrative, technical, and physical safeguards to protect the privacy of Personally-Identifiable Information.

B. Purpose

To provide instructions to all **Virtru** employees regarding the use of faxes with respect to Personally-Identifiable Information and the measures necessary to maintain an adequate level of security for such information. This policy defines rules necessary to achieve this level of protection. These standards are designed to minimize the potential exposure to **Virtru** from damages, which may result from unauthorized disclosure of Personally-Identifiable Information through facsimile use.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru**.

D. Special Definitions

Fax: An electronic facsimile of a document stored as a series of zeroes and ones (binary data) that can be transmitted like normal computer data. When received by a fax machine, the incoming stream is translated into dots creating a representation of the original document.

Inappropriate Disclosure: The intentional or unintentional revealing of Personally-Identifiable Information to people who do not have a need to know such information.

E. Corporate Policies

Employees must exercise utmost caution when sending faxes to parties outside of **Virtru**. Faxes containing Personally-Identifiable Information should only be received on and sent to user or departmental specific fax machines and not to systems that have general access.

In cases where Personally-Identifiable Information is received from outside on a non-departmental specific fax machine, the receiving department shall notify the **Virtru** Privacy Officer of the source of such information. The employee shall communicate the approved fax number to the external entity and record such actions. Should PHI be disclosed by fax to an inappropriate party, **Virtru** shall, to the extent possible, remediate such disclosures.

All fax documents sent by **Virtru** employees shall contain the following statement:

This fax is intended for the individual/individuals or entity/entities named above and may be covered by copyrights, business partner confidentiality agreements, non-disclosures or other legally binding instruments. If you are not the intended recipient, do not read, copy, use or disclose the contents of this communication to others. Immediately notify the sender by reply fax, destroy all hard copies and delete this document from all systems. Thank you!

F. Procedure

In the cases where data that contains Personally-Identifiable Information is disclosed by fax machine use to an inappropriate party, the following procedure shall be followed:

1. The receiving party shall be contacted by telephone at the earliest opportunity and requested to destroy the fax without reading.
2. The name of the company, the person contacted, the date and time shall be recorded as well as any comments made by the person receiving such calls.
3. A fax shall also be sent to the receiving party containing the same instructions as detailed for the phone call requesting a return fax message indicating that the requested action was taken.
4. The cause of the inappropriate disclosure shall be determined and reported to the **Virtru** Privacy Officer.

Methods to prevent a reoccurrence of the inappropriate disclosure shall be formulated and put into place.

Any additional actions prescribed by regulations shall be performed to the extent possible.

G. Enforcement

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use

or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

X. Scanner Policy

A. Overview

The Privacy Rules require that **Virtru** implement appropriate administrative, technical, and physical safeguards to protect the privacy of Personally-Identifiable Information.

B. Purpose

To provide instructions to all **Virtru** employees regarding the use of scanners with respect to Personally-Identifiable Information and the measures necessary to maintain an adequate level of security for such information. This policy defines rules necessary to achieve this level of protection. These standards are designed to minimize the potential exposure to **Virtru** from damages, which may result from unauthorized disclosure of Personally-Identifiable Information.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru**.

D. Special Definitions

Scanner: An electronic copy of a document stored as a series of zeroes and ones (binary data) that can be transmitted like normal computer data. When received by a computer, the incoming stream is translated into dots creating a representation of the original document.

Inappropriate Disclosure: The intentional or unintentional revealing of Personally-Identifiable Information to people who do not have a need to know such information.

E. Corporate Policies

Employees must exercise utmost caution when scanning and transmitting these documents to their devices and parties outside of **Virtru**. Scans containing Personally-Identifiable Information should only be received on and sent to user or departmental specific computer in an encrypted format, or sent using **Virtru's** encrypted email application.

F. Procedure

In the case where scanned data that contains Personally-Identifiable Information is disclosed to an inappropriate party, the following procedure shall be followed:

1. The receiving party shall be contacted by telephone at the earliest opportunity and requested to destroy the scan without reading.

2. The name of the company, the person contacted, the date and time shall be recorded as well as any comments made by the person receiving such calls.
3. The cause of the inappropriate disclosure shall be determined and reported to the **Virtru** Privacy Officer.

Methods to prevent a reoccurrence of the inappropriate disclosure shall be formulated and put into place. Any additional actions prescribed by regulations shall be performed to the extent possible.

G. Enforcement

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

XI. Training Policy

A. Overview

The Privacy Rules require that **Virtru** train their employees on the requirements of our Privacy Policies and Procedures developed to protect the Personally-Identifiable Information to which employees are provided access. The **Company** has determined that all employees of **Virtru** shall be trained on Privacy so that we can provide the necessary assurances for the protection of Personally-Identifiable Information to our clients, vendors and business partners as required under the Privacy Rules.

B. Purpose:

To provide instructions to all **Virtru** employees regarding the requirement for HIPAA training.

C. Applicability

This policy applies to all **Virtru** employees, which is defined for the purposes of this document to be employees of all current and future subsidiaries of **Virtru**.

D. Policy

1. General: It is the policy of the **Company** that all employees of **Virtru** and its current and future subsidiaries be trained on Privacy and the **Company** policies and procedures created to protect Personally-Identifiable Information.

2. Duty Specific Training: Privacy training shall be appropriate to the tasks that each employee performs. In the case where an employee does not come into contact with Personally-Identifiable Information as a normal course of the employee's duties, the employee shall be trained on the corporate policies and procedures.

3. New Employees: New employees shall be trained on the corporate policies and procedures as part of their normal employment process and shall be trained on our Privacy Policies and Procedures, if applicable, within 30 days of being employed by **Virtru.** The Assistant ISO, Jordan Duggan, shall document this training and provide the Privacy Officer with documentation of this training within the 30-day period.

4. Transfers: When an employee transfers from one department to another, the employee shall be trained on our Privacy Policies and Procedures within 30 days of being assigned. Jordan Duggan shall document this training and provide the Privacy Officer with documentation of this training, within the 30-day period.

5. Material Change in Policies and Procedures: when a material change in the policies and procedures occurs, each employee shall receive training on such changes within 30 days of the implementation of the change. Jordan Duggan shall document this training and provide the Privacy Officer with documentation of this training, within the 30-day period.

E. Enforcement

Any employee found to have violated this policy shall be subject to disciplinary action, up to and including termination of employment. In the case where inappropriate access, use or disclosure of Personally-Identifiable Information was or may have been involved, such individuals may additionally be reported to the appropriate enforcement agencies.

Security Policies and Procedures



{After choosing where you will store your Security Documents, delete either the **Library** or {Notebook} option throughout this document.}

Revision History

Virtru's Security Policies and Procedures were adopted as of [Date].

Name

Virtru's Security Policies and Procedures were modified as of [Date].

Name

Virtru's Security Policies and Procedures were modified as of [Date].

Name

Virtru's Security Policies and Procedures were modified as of [Date].

Name

Virtru's Security Policies and Procedures were modified as of [Date].

Name

Virtru's Security Policies and Procedures were modified as of [Date].

Name

Security Policies and Procedures

Table of Contents

- Virtru
  - Document control
  - B. Security Document Library
- II. Preface and Background Material
  - Overview
  - B. Policy
- III. Key Concepts
  - Information Security Principles
    - Confidentiality
    - Integrity
    - Availability
    - Provability
  - Definitions
    - Information Security Policy
    - Privacy Policy
    - Acceptable Use Policy for IT Systems Users
    - Employment Policies
- IV. Using These Standards
  - Audience – Who will use this document
    - Technology and business process providers should comply with these Standards as a matter of contractual obligation
    - Employees and Business units within Virtru should comply, unless a Risk Assessment has been done and a deviation is approved by the ISO
  - How the document is used
    - Review of existing controls, procedures and tools against the Standards
    - Documenting compliance or deviations
    - Gap Analysis to determine where improvements are needed
    - A Risk Assessment to validate that the improvements are justified against the costs of the controls and the value of the information involved
    - Creation of a plan to close the gaps OR signoff of a deviation
    - Documentation of the new controls, procedures and tools
  - C. Maintaining this document
- V. Roles and Responsibilities
  - A. Rules for ownership of information
  - B. Information users
  - C. Information Security Officer
    - Manage awareness programs relating to security and privacy topics
    - Maintain a central record of exceptions to this Standards document
    - Manage changes to this Standards document

Security Policies and Procedures

Provide leadership relating to new security risks, controls and technologies
Oversee and approve the sharing and reuse of Personal Identifiable Information (PII) collected by or processed by the company
VI. Information Classifications and Requirements
Overview
B. The Security classification process
IT platforms such as servers and workstations
IT applications including database transaction processing and email
Data sets
Paper copies of information
Information types typically known to workforce members, such as customer information
Development, acquisition or deployment of software
Connections of computers or networks to outside systems or networks
Granting of access to any outside organizations
C. The classes of information for Security and Privacy
Data Types
Company-owned data that relates to such areas as corporate financials, employment records, payroll, etc.
Setting requirements for business continuity
Required uptime for the information asset
Required restoration time if the data must be restored
Required frequency of backups
Requirements for storage of backups
Requirements for testing of the recovery process
Enforcement
VII. Handling Rules for the Information Classifications
Overview
Inventory of Information Assets and Electronic Asset Management Log
Rules for access to information assets
VIII. Access Control Policy
Overview
Access levels
Granting access
The ISO will provide accounts with the matching technical privileges and give the workforce member the account information including a one-time-use password that the user must change to a private password upon first use of the account.
1. Only the person assigned to an account will be allowed to use that account.
Vendors, contractors and other outsiders
Individuals
Policy

Security Policies and Procedures

IX. Rules by Data Classification
- Public/unclassified data
- B. Private/internal data
- C. Confidential or protected data
- D. Managing data sources
- E. Retention of media
  - Agent of Record letters and Letters of Authorization requests are held for no less than ninety (90) days
  - New Business Group documents are held for no less than ninety (90) days
  - General documents are held for no less than ninety (90) days
  - Banking statements are held for seven (7) years
  - Workforce member records are held for seven (7) years
- F. Sanitization of Media
- G. Information sharing and privacy
- H. Release of company information

X. Risk Analysis and Management
- Risk reviews
- B. Risk management
  - Increasing a protection to a level higher than what is listed in this document
  - Improving oversight or monitoring of the risk to limit impact and minimize response time
  - Limiting transactions or other events to minimize the possible impact of the risk event

XI. IDs and Accounts
- User IDs
- B. ID and account creation
  - Expiration dates for the User ID
  - Renewal process for the User ID
  - Documentation of the role, business process and job function relating to the User ID
- C. Account management
- Application Specific IDs

XII. Authentication and Passwords
- Overview
- Password format
- Rules

XIII. Authorization and Rights Management
- General Access Roles
  - Super Admin Access: Access to all front and backend products as well as product metrics
  - Admin Access: Access to all front end products as well as product metrics
  - General Access: Access to product metrics

Security Policies and Procedures

Low Access: Access to corporate email, sales, and marketing data only
Amazon Web Services (AWS)
Cloudant
Github
ELK Stack
Mixpanel
Kissmetrics
Salesforce
Access Rules
Limiting access to datasets and types
Limiting access to operating systems
Limiting times of access
Temporary Privileged Users and Accounts
D. Assignment and Revocation Procedure
An Employee Access Log for all new hires and/or workforce member change of status.
An Exit Checklist for all terminations.
E. Logout After Inactivity
XIV. Breaches or Impermissible Uses/Disclosures
Definitions
Penetrations of systems, applications, networks or databases
Denial of service attacks
Misuse or mishandling of assets
Virus or other malware contamination
Transaction errors
Breaches of confidentiality agreements or contracts
Legal or regulatory violations
XV. Breach Response
A. Overview
Confidential Reporting:
Calling (may leave voice message) the ISO or AISO
Sending an email to the ISO or AISO, or;
XVI. Personnel Security
Screening for newly hired personnel, third parties, vendors
Professional qualifications
Identity checks
Criminal checks
Confirmation of academic and professional experience
B. Training and Awareness
Managing malicious software (e.g. viruses)
Using workstation(s) securely

Security Policies and Procedures

Managing passwords and
Monitoring and reporting suspicious use of account(s)
C. Terms of employment
D. Acknowledgement
E. Exit process for users
Relinquish all access to control devices
Report all User IDs in use by the person
Relinquish all information stored, whether on paper or on backup media
Relinquish all information processing devices, including workstations, all Virtru-owned mobile devices and others
All systems access will be revoked.
Security Sanction Policy
First Security Infraction
A simple infraction, and
The first infraction in the last 3 years
Second Security Infraction or First Serious Infraction
A serious infraction, or
The second infraction of either type within 3 years
Third Security Infraction or Second Serious Infraction
A second serious infraction within 3 years, or
A third infraction of any type within 3 years
The sanction will be dismissal from the workforce.
XVII. Legal and Regulatory Issues
Legal processes
Copyrights and licenses
C. Export controls
XVIII. Malware and Antivirus
Definitions
Operating system anti-malware requirements
Macintosh, Linux and iPhones:
PC Operating Systems:
Android and Windows Phone Operating Systems:
Affiliates
Infected devices
Employees' Requirements
Workforce members will not load software on our Company's information equipment without permission from the ISO.
Workforce members will not open electronic files from unfamiliar sources.
Enforcement
XIX. Change Control Logs
Preface

Security Policies and Procedures

B. Policy
Sufficient information is available for proper investigation of use, misuse, incidents and performance
User ID, event type, date and time are maintained
Time is according to a known time stamp so that events across systems can be coordinated
4. End-to-end accountability is always maintained
Changes to operating systems, application code or other tools
Backup and restore events
Changes affecting any cryptographic keys or devices
Stop or start of critical processes
Transaction failure, retry or duplication
KissMetrics
Segment.io
Sendgrid
XX. Encryption
Preface
Application Encryption Policy
Key Rotation Policy
D. Device Encryption Policy
Mac OS Devices:
Windows OS Devices:
Linux OS Devices
Android Devices
Windows Phone
iPhone
E. Wi-Fi network encryption
F. Email encryption
G. Enforcement
XXI. Assessments and Testing
Overview
B. Penetration testing
Operating systems
Applications
Databases
C. Vulnerability assessment testing
A new system, application or network is installed inside the Company
Changes are made to firewalls, VPNs or other security control tools
Changes are made to a web server's operating system
Changes are made to email servers
Configuration changes are made to databases

Configuration changes are made to critical applications
Changes are made to encryption scheme(s)
D. Wireless access testing
E. Password testing
XXII. Use of Email, Internet, Messaging, Public Sites, Blogs, Social Media
Policy
Sexually explicit material
Confidential, Private or Protected Information or Internal Use material, except as meets the Handling Rules section
Viruses
Threats
Inappropriate or unlawful language, including:
Offensive language
Language inappropriate for the Company environment
Discriminatory or harassing language
Tools usable for hacking, password cracking, vulnerability scanning or penetration testing
XXIII. Hardware
Definitions
B. Policy
C. Asset management
D. Enforcement
XXIV. Networks
Overview
Denial of service attacks
Improper access
Virus infections
Unauthorized software installations, email, FTP or other improper usage
Administration of network and communications connections
Operations of all devices
Monitoring
Timely review of audit logs and response to alerts or alarms
Review of unusual patterns of usage or activity
Monitoring
Access control and physical security
Access limited to authorized personnel only
Physical security, including RFID or passcode controlled locks, are in place
Modifications, updates
Documentation
Network design
Segmentation

Security Policies and Procedures

Firewalls
Internet
Approved by the ISO
Periodically reviewed and tested for vulnerabilities
Protected by firewalls, intrusion detection systems and anti-malware tools
VPN-remote access
Wireless
Telework Policy
Patching of systems and applications
Network hardening
XXV. Physical and Environmental Protections
Definitions
Computing centers
Network connection points
Media storage locations
Locations containing platforms which carry high-value or critical information or transactions
B. Secure Sites Policy
Media libraries
Electrical supplies and controls
Environmental and mechanical controls
XXVI. Physical Security Policy
A. Entry Policy
Loss of RFID key
Mobile devices
D. Video monitoring
Alarm system
Fire protection
XXVII. Software
Overview
B. Acquisition of software
C. Open Source Software
It is not used in a production environment OR
Prior to use it is fully tested, documented and Virtru's personnel are assigned to support it. Checks to be performed include:
The source of the software is documented
URL
Project lead
Contributors
The ISO approves of the use
D. Documentation

Security Policies and Procedures

E. Change control and maintenance
F. Operating Systems
G. Applications
Access control
Authorization
Information classification
Storage controls
Backup and restoration
Confidentiality and integrity requirements
Audit logs
Privacy, export control and other such requirements
H. Asset management for software
I. Enforcement
XXVIII. Removable Media Device Policy
Purpose
B. Scope
C. Definitions
D. Policy
E. Using Removable Media Devices
F. Exceptions
G. Refusal
H. Enforcement
Application Recovery Plan
Overview
Scope
Data durability and reliability
Encryption
Load balancing
Restoration of data
G. Testing and revision of plan
Network Attached Storage and Workstation Backup Plan
Overview
Policy
Backup software
Remote backups
Local backups
Encryption of backups
Restoring data
H. Enforcement
Information Integrity Management Policy
Overview

Security Policies and Procedures

B. Policy
Security Incident Management Policy
Overview
Procedures
C. Policy
Security Plan Review Policy
Overview
Procedures
Appendices
Change Logs
B. Information Security Committee

Security Policies and Procedures

I. Virtru

Virtru may be referred to as "**Company**."

A. Document control

A staff copy of this document is available with the Information Security Officer (ISO), Will Ackerly, willackerly@virtru.com (202) 577-3683, and Assistant Information Security Officer(AISO), Jordan Duggan, jordan@virtru.com (202) 577-3683.

B. Security Document Library

These policies and procedures and related security practice information will be kept in our **Security Documentation Library** (SDL). The **SDL** is located in google drive and backup to the Synology NAS.

Documentation about security practices (logs of activities, etc.) will either be kept in this SDL (or Notebook) or in a short file in the SDL that will describe where the security practice documentation resides. The intended result is that anyone with access to the SDL will be able to locate any piece of documentation associated with our security program.

Outdated and superseded materials from the SDL will be kept in an archive (the Security Documentation Archive) for at least seven (7) years after the date when they are first outdated or superseded.

II. Preface and Background Material

A. Overview

It is vital to the reputation and profitability of **Virtru** that our information and our clients' information, in all forms, be protected from unauthorized use, modification, loss, copying, etc. This document sets out the default standards, which must be met to ensure that control.

Our information may exist on paper, in voice systems, on IT systems and networks, in the minds of our people, and in other forms. The information which needs protection includes, but is not limited to:

1. Client information (both for customer companies and for people as individuals)
2. Financial information, including credit cards, salaries, banking, transactions and more
3. Medical information of all types
4. **Company** patents, business plans and other intellectual property

5. **Company** business records and planning materials, including our customer list, marketing and sales efforts, product line plans and more
6. Copyrighted materials, both which our **Company** creates and those which we obtain under license from others

B. Policy

Compliance with these standards is mandatory. Any deviation from these standards must be approved beforehand by the ISO.

III. Key Concepts

A. Information Security Principles

The protection of information can be described in several key dimensions:

1. Confidentiality
2. Integrity
3. Availability
4. Provability

In this document, the standards given are the **Company** defaults. They must be applied where appropriate, but always balanced against the cost of implementing the control, and the value of the information involved.

B. Definitions

To prevent confusion, these are the definitions used throughout this document.

Policies: Corporate documents which set out **Virtru's** position regarding business processes, behavior of personnel and similar topics. Policies are a high-level statement of **Virtru's** position. Some of **Virtru's** policies, which relate to information security are:

1. Information Security Policy
2. Privacy Policy
3. Acceptable Use Policy for IT Systems Users
4. Employment Policies

Standards: Rules that must be followed to enable an effective information security program. Compliance with the Standards is mandatory, but deviation is possible if approved by the ISO.

Standards define the minimum baseline procedures, practices and configurations for systems, applications, controls, networks and related topics. Standards are designed to provide a single reference point for use during software development and adoption,

installation of systems and tools, and during the contracts process with vendors and service providers. Standards do not, however, give detailed command-line instructions on how to meet the **Virtru's** policies. Those are given in the guidelines.

Guidelines: Built for each application and platform; to be followed when implementing that particular tool. A Guideline may vary a bit from one implementation to another, as long as the Security Standards are met and justification is given and properly documented.

Combined, these three levels of documents provide a method for **Virtru** to audit itself and ensure proper controls are in place, without excess cost or risk. They also provide a means for **Virtru** to explain to regulators, examiners, external auditors or investors how our **Company** is safe, trustworthy and efficient.

IV. Using These Standards

A. Audience – Who will use this document

This document applies to **Virtru's** employees, business units and any Business Associate Subcontractor supporting **Virtru**:

1. Technology and business process providers should comply with these Standards as a matter of contractual obligation
2. Employees and Business units within Virtru should comply, unless a Risk Assessment has been done and a deviation is approved by the ISO

B. How the document is used

This Standards document is a reference point to ensure a consistent framework of protections is in place. Implementing these standards involves:

1. Review of existing controls, procedures and tools against the Standards
2. Documenting compliance or deviations
3. Gap Analysis to determine where improvements are needed
4. A Risk Assessment to validate that the improvements are justified against the costs of the controls and the value of the information involved
5. Creation of a plan to close the gaps OR signoff of a deviation
6. Documentation of the new controls, procedures and tools

No signoff or approvals are needed if a level of protection higher than what is given in this Standard is determined to be needed for a given information asset.

C. Maintaining this document

This document must be reviewed at least once a year or anytime there are significant changes in software or security. Updates must be made to keep it in accord with **Virtru's** overall business goals and risk position. The document will be reviewed by the ISO or AISO. Any updates, improvements or suggestions should be sent to the ISO.

V. Roles and Responsibilities

A. Rules for ownership of information

The information and systems provided by **Virtru** to workforce members, contractors and representatives are owned by **Virtru**, which also determines appropriate usage and access rules. All data on **Virtru's** systems and networks is owned by **Virtru**, with the exception of software that the ISO has approved to be open sourced or otherwise transferred to another entity through code escrow or code exchange and/or trade.

In this document, the words 'information owner' refer to the person who owns the responsibility for the information. The information itself remains the property of **Virtru**.

B. Information users

Every user of **Virtru's** information must protect that information and ensure that it is used for **Virtru's** business purposes only. Any incidents or questionable issues in the security of our information must be reported to the ISO or AISO.

Information users may not assign access rights, authorize destruction or copying of information, or change the protections given to information assets. Information users must comply with all laws, regulations and **Virtru's** policies and procedures.

C. Information Security Officer

Virtru's ISO and AISO will:

1. Manage awareness programs relating to security and privacy topics
2. Maintain a central record of exceptions to this Standards document
3. Manage changes to this Standards document
4. Provide leadership relating to new security risks, controls and technologies
5. Oversee and approve the sharing and reuse of Personal Identifiable Information (PII) collected by or processed by the company

See Appendices for further information and *Information Security Committee* for a current listing of members.

Security Policies and Procedures

VI. Information Classifications and Requirements

A. Overview

Information is classified by system to ensure that the controls applied to it are sufficient and also to ensure that the controls applied do not impair **Virtru's** business, ability to compete or **Virtru's** image.

All information must have a classification for security and must have requirements set for business continuity.

B. The Security classification process

Each information asset will go through the following classification process. Information assets include, but are not limited to:

1. IT platforms such as servers and workstations
2. IT applications including database transaction processing and email
3. Data sets
4. Paper copies of information
5. Information types typically known to workforce members, such as customer information

In general, an information asset includes both the raw information itself (paper, oral or data entry), the location where it resides, the business processes which handle it and the systems and tools that handle it.

Information assets will also be reviewed during:

1. Development, acquisition or deployment of software
2. Connections of computers or networks to outside systems or networks
3. Granting of access to any outside organizations

The security classification of an information asset is assigned according to the highest of these dimensions. As an example, if an asset is regulated by law, then it needs the highest classification, even if the asset is not critical to the Company's business.

C. The classes of information for Security and Privacy

This policy applies to all workforce members, management, contractors, vendors, business partners and any other parties who have access to Company or client data.

Data Types

The security classification of an information asset is assigned according to the highest of these dimensions. As an example, if an asset is regulated by law, then it needs the highest classification, even if the asset is not critical to **Virtru's** business. **Virtru** deals with two main kinds of data:

1. **Company-owned data** that relates to such areas as corporate financials, employment records, payroll, etc.

2. **Personally Identifiable Information (PII)** that is the property of our clients or workforce members, such as Protected Health Information, social security numbers, credit card information, contact information, etc.

D. Setting requirements for business continuity

The requirements for an information asset relating to business continuity are not set by classification, but are specific to that asset. They include:

1. Required uptime for the information asset
2. Required restoration time if the data must be restored
3. Required frequency of backups
4. Requirements for storage of backups
5. Requirements for testing of the recovery process

The default requirements for business continuity are listed in the information handling rules' section. See *Handling rules for the information classifications* in this document and *Disaster Recovery Plan* for detailed information.

This section outlines the basic rules for handling information types according to the classifications. More specific standards for platforms, processes and networks appear in each topic section of this standards document.

E. Enforcement

It is the responsibility of everyone who works at **Virtru** to protect our data. Even unintentional abuse of classified data will be considered punishable in accordance with the extent and frequency of the abuse.

VII. Handling Rules for the Information Classifications

A. Overview

This section outlines the basic rules for handling information types according to the classifications. More specific standards for platforms, processes and networks appear in each topic section of this standards document.

B. Inventory of Information Assets and Electronic Asset Management Log

An inventory is maintained of all significant information assets belonging to, or used by **Virtru**. This inventory includes:

1. Serial numbers/license numbers
2. MAC Addresses
3. Model
4. Device Type
5. Manufacturer
6. The information owner
7. Username
8. Location
9. OS Version
10. The custodian of the information and repository location (database, file cabinet, etc.)
11. Purpose in our systems
12. Asset value in dollars or other suitable measurement
13. The sensitivity of the asset, due to regulations, laws, customer expectations or other requirements
14. Requirements for the asset regarding availability, uptime, etc.
15. Contact information for one or more parties who can repair, restore, replace, or recover this asset. Examples are hardware/software vendors, IT support vendors, and/or staff members

This asset list contains information that is restricted to executives and super-admins, and therefore is stored securely on the Synology NAS, which itself is backed up to AWS Glacier.

This inventory will be reviewed and updated quarterly, or as new assets and devices are added. Logs are maintained as the *Inventory of Information Assets Log* and the

Organizational Chart/Electronic Asset Management Log. A current copy of this inventory will be kept at a separate location as described in our *Disaster Recovery Plan.*

C. Rules for access to information assets

If any given security incident involves a breach of Personally Identifiable Information (PII), the ISO will follow our security policies and *Incident and Breach Policy* for handling such a breach.

If a security incident includes the potential that personal information may have been obtained by unauthorized individuals, the ISO will work with the client to notify affected persons of this event, in compliance with relevant federal and/or state law.

See also *Breaches or Impermissible Uses/Disclosures* within these Security Policies and Procedures.

VIII. Access Control Policy

A. Overview

This policy defines how **Virtru** manages access to electronic information and systems. **Virtru** provides access to electronic data relative to the workforce member's job requirement. We limit access to categories of data and systems that each person needs to do his/her job. We require that each workforce member restrict his/her access to only those specific records and functions needed to carry out his/her job. For the purposes of this policy workforce members are anyone in **Virtru** who has access to Personally Identifiable Information (PII).

B. Access levels

The ISO will qualify the workforce member to have one of these forms of access based on the job role (in order of increasing access permissiveness):

1. Low Access to Corporate Email and Salesforce Data
2. General Access to product metrics
3. Admin Access to all front end products as well as product metrics
4. Super Admin Access to all front and backend products as well as product metrics

The access will match the person's job responsibilities The ISO will keep a record of the type of access provided to each workforce member. The record will include a date and justification and will be kept in our *Employee Access Request Log* in the **Security Documentation Library.**

The granting of access to Business Associate Subcontractors will be done in the same way as it is done for workforce members.

C. Granting access

The ISO will provide accounts with the matching technical privileges and give the workforce member the account information including a one-time-use password that the user must change to a private password upon first use of the account.

1. Only the person assigned to an account will be allowed to use that account.

2. Each time a user logs in to a system, a log will be maintained by that specific program with the following information
    a) When the user accessed the system
    b) What information the user accessed while in the program
    c) Tracking will be done by using the User ID and IP Address
    d) The ISO will maintain this log for a period of 1 year

3. The ISO and AISO will each have a special account that allows them to create new accounts. The accounts will be used:
    a) In an emergency when all other accounts have been disabled or locked out;
    b) To either reset the passwords on locked accounts; or
    c) To create new accounts that provide needed access.

4. When a change in the role of a workforce member requires a change in access privileges, the ISO will reassess the needs and provide new access privileges based on the policy in Access Levels in this section.
    a) If a workforce member leaves **Virtru**, the ISO will remove that member's access as soon as the access is no longer needed.
    b) If a workforce member takes a leave of absence and is not expected to require access, the ISO will disable the workforce member's account when he/she leaves and re-enable it upon his/her return to work.
    c) For other people who work around protected electronic information but are not qualified to access it, the ISO will decide which of the following two steps to take:
        1) Train the person to understand his/her responsibilities
        2) Supervise while he/she is exposed to the data
    d) For cases in which the provision of individual accounts is not feasible {e.g. access by any one person of a large help desk staff of a vendor}, the ISO will make:
        1) A serially reusable account and provide a one-time-use password to the vendor's representative for each time that access is needed; and

2) The password will be changed by the ISO on the account after each use of the account to a value not known to the vendor.

D. Vendors, contractors and other outsiders

Any outside organization that wishes to gain access to our or our client's Private/Internal, Confidential or Protected information must:

1. Sign a Business Associate Subcontractor Agreement; AND
2. Be willing and able to show that their privacy and security controls are at least as stringent as **Virtru's** controls.

See *Business Associate Subcontractor Agreement* for details of Agreement.

A written history of incidents reported by Business Associate Subcontractors (BAS) will be maintained. If the ISO becomes aware of a pattern of activity in which the BAS is not carrying out the contractually required safeguards, then the ISO will do one of the following:

1. Attempt to remedy this failure
2. Terminate the contract, if attempt to remedy is not feasible
3. Report the situation to the U.S. Secretary of Health and Human Services, if terminating the contract is not feasible.

If any given security incident involves a breach of Personally Identifiable Information, the ISO will follow our privacy policies and incident management plan for handling such a breach.

If a security incident reported by a BAS includes the potential that personal information may have been obtained by unauthorized individuals, the ISO will work with the BAS to notify affected persons of this event in compliance with relevant federal and/or state law.

See also *Breaches or Impermissible Uses/Disclosures* within these Security Policies and Procedures.

E. Individuals

Individual persons who work for such an organization must also be bound to the outside organization's controls. Such individuals must:

1. Have Business Associates Subcontractor Agreement with their own company; OR
2. Have a contract with their company; AND
3. Have appropriate background checks and bonding in place.

F. Policy

Virtru will not knowingly accept any confidential information belonging to third parties until that information is reviewed against our protections and the appropriate agreements put into place and signed by the information owner. The agreements should include all requirements for controls over the third-party information and the processes to be followed.

IX. Rules by Data Classification

A. Public/unclassified data

This type of information does not require special marking or storage, except to ensure that it is available when needed. It does need to be kept safe from unauthorized modification.

B. Private/internal data

Access is granted on a need-to-know basis, as authorized by the manager of the user of the information. Some types of jobs are automatically granted access to data in this class.

Paper products and backup media containing this type of information must be stored and handled in a secure manner. This includes:

1. Printing this class of information only to a known printers located in secure areas on secure networks.
2. Encrypting or physically securing backup media
3. Keeping paper copies of information locked or otherwise secured

This class of information is not released to anyone outside **Virtru** without a non-disclosure agreement, a Business Associate Subcontractor Agreement, and/or without the approval of the information owner. Private/Internal use information must not be transmitted across any unsecured outside network or path without proper controls. This means encryption for files and emails or secured packaging for paper copies.

C. Confidential or protected data

Access to this type of information is on a need-to-know basis, as approved by the ISO or information owner.

This class of information is not released to anyone outside the Company without a non-disclosure agreement and without the approval of the information owner.

Confidential or Protected information must not be transmitted across any unsecured outside network or path without proper controls. This means encryption for files and emails, or secured packaging for paper copies.

Paper products and backup media containing this type of information must be stored and handled in a secure manner. This includes:

1. Printing this class of information only to a known, secure printer
2. Encrypting and physically securing backup media
3. Keeping paper copies of information locked or otherwise secured

D. Managing data sources

The key to managing **Virtru's** business' media and documents is to first consider the source of the information, then the media type. **Virtru's** media and documents containing Protected Information (PHI, CJIS, or other) require protection from inception through disposition. Regardless of the owner relationship, the Company will be cognizant of the following Media Types:

1. **Hard Copy:** paper printouts, printer and facsimile ribbons, drums, etc.
2. **Electronic:** the bits and bytes contained on hard drives, flash drives, phones and tablets.

E. Retention of media

Retention: The length of time documentation and/or information is retained according to the level of confidentiality and to the business continuity requirements. System/ information owners should consult with the ISO to ensure compliance with the record retention regulations.

Virtru's hard copy record retention policy is as follows:
We will digitize and encrypt these records for secure storage on the Synology NAS, which will be backed up to AWS Glacier.

Virtru's electronic record retention policy is as follows:

1. Agent of Record letters and Letters of Authorization requests are held for no less than ninety (90) days
2. New Business Group documents are held for no less than ninety (90) days
3. General documents are held for no less than ninety (90) days
4. Banking statements are held for seven (7) years
5. Workforce member records are held for seven (7) years

F. Sanitization of Media

When media (hard copy and electronic) becomes obsolete, is no longer required or no longer usable, it is critical that proper sanitization is accomplished.

Sanitization Types

Disposal: the act of discarding media. This is often done via recycling paper containing "non-confidential" material.

Reinitializing: Re-formatting drives so information cannot be retrieved by recovery utilities or any other forms including keystroke recovery attempts. This is achieved by overwriting the disk with zeros for no less than one (1) time.

Purging: exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains, this is also known as degaussing.

Destroying: destruction of media so it cannot be reused as its original purpose.

Virtru's electronic disposal policy is as follows:

1. Hard-drives are purged, reinitialize or destroyed
2. CD or DVD disks are destroyed
3. Flash drives are re-initialized or destroyed
4. Backup tapes are purged, reinitialized or destroyed

Any systems that are leased must be securely sanitized of all Company data prior to being returned to the leasing company. Any additional media (e.g. hard drives, USB drives etc.) will be reformatted then written with zeros for no less than one (1) time to ensure that the data contained on the media has been destroyed.

Virtru shall maintain appropriate records of sanitization. This entails validating how, where and when media is sanitized. See *Media Sanitization*.

G. Information sharing and privacy

In most cases the sharing and reuse of Personally Identifiable Information is governed by law, regulation and customer expectation. To ensure **Virtru** meets those requirements, no Personally Identifiable Information will be shared with outside companies, vendors or personnel without written approval from the ISO.

Personally Identifiable Information includes:

1. Names
2. Addresses

3. Phone Numbers
4. Email Address
5. Dates of birth
6. Social Security Numbers
7. Ages
8. Gender
9. Personal Financial Information
10. Personal Medical Information
11. Criminal History Information
12. Personal Employment Information
13. Personal Buying Histories
14. IP Addresses

Aggregated and statistical data developed from this personal information is not personally identifiable and, thus, does not need the approval of the ISO for sharing and re-use.

Virtru will comply with all applicable laws and regulations regarding the privacy of personal information, including such laws as:

1. Health Insurance and Portability and Accountability Act (HIPAA)
2. Health Information Technology for Economic and Clinical Health (HITECH)
3. Family Educational Rights and Privacy Act (FERPA)
4. Criminal Justice Information Systems (CJIS)
5. Federal Information Security Management Act (FISMA)

Virtru's workforce members, contractors, vendors and suppliers may come into possession of Personally Identifiable Information as a part of their relationship with **Virtru**. Each person must comply with all laws, regulations and policies and ensure such information is properly protected.

H. Release of company information

Virtru's information may only be released with the approval of the ISO or the information owner. This includes the posting of **Virtru's** information of any type onto bulletin board systems, public networks, social media or other open sharing tools. Any information released must contain proper copyright, trademark, disclaimer and patent notices as appropriate.

X. Risk Analysis and Management

Risks to **Virtru's** assets and environment should be addressed proactively rather than reactively. The controls applied to the risks must also be periodically reviewed to ensure the controls are working properly and efficiently.

Security Policies and Procedures

A. Risk reviews

The job of reviewing risks and setting requirements for controls is the ISO's. Risks should be reviewed or assessed when:

1. Developing or deploying new applications, systems, networks or software
2. When significant changes are made to that same list
3. When business processes change
4. When **Virtru** enters a new geographical area of business
5. When **Virtru** enters a new line of business
6. When incidents occur or new risks emerge
7. When new regulations or standards are set

B. Risk management

Risks may be accepted, avoided or mitigated.

Accepting the risk is appropriate when the cost of avoiding or mitigating the risk is greater than the expected loss. The losses considered should include the less tangible items such as **Virtru's** reputation, loss of market share and loss of public trust in **Virtru**. Acceptance of a risk requires complete documentation of the risk analysis and approval by the information owner.

Avoiding the risk is appropriate when the cost of insurance is less than the cost of incremental controls. However, basic controls must always be in place.

Mitigating the risk is appropriate in most situations. These situations are those where compensating controls are possible, cost-effective and manageable. These mitigating controls may include:

1. Increasing a protection to a level higher than what is listed in this document
2. Improving oversight or monitoring of the risk to limit impact and minimize response time
3. Limiting transactions or other events to minimize the possible impact of the risk event

The method chosen for managing the risk (acceptance, avoidance, mitigation) must match the business value and costs involved and must be approved by the information owner.

For further detail, see the *Risk Management Policy* and the *Disaster Recovery Plan*.

Security Policies and Procedures

XI. IDs and Accounts

A. User IDs

Each user shall be assigned a unique identification, called the User ID. This User ID is not considered to be sensitive, unless the User ID relates to an authentication process, systems or application management role.

On sensitive systems or applications the User ID should not be easily identifiable, thus making unauthorized usage more difficult.

Sharing of User IDs is not permitted, unless justified by business requirements and approved by the ISO. For any such shared User ID, the password will be shared using LastPass, and the password will not be shared with the additional user. If this password is shared, it must be changed immediately after the User ID is used to keep the shared User ID from becoming generally available and a risk to **Virtru**.

Guest and anonymous User IDs are not allowed, unless the system involved is not connected to any of **Virtru's** networks and the system does not have any **Company** information on it. Typically, these guest or anonymous User IDs are only used during development or during marketing/sales demonstrations.

B. ID and account creation

User IDs are only to be created following a process approved by the information owner. This User ID creation process should include:

1. Expiration dates for the User ID
2. Renewal process for the User ID
3. Documentation of the role, business process and job function relating to the User ID

User IDs are to be created for the purpose needed and not in a manner to compromise segregation of duties.

A record of all User IDs and their owners will be maintained by the ISO. See the **Change Control Logs for Security** for further detail.

C. Account management

A periodic check will be made of all User IDs and any redundant, dormant or unused IDs will be removed. The ISO must review the privileges set up for User IDs no less than once every year.

D. Application Specific IDs

Application Specific IDs and logins are used in support of automated applications, transactions, processes or batch jobs. These have non-expiring passwords.

1. Application Specific IDs must not be used by individuals.
2. Application Specific IDs must be created only with the approval of the ISO, must be documented and have strictly limited access rights.
3. Application Specific IDs must not have ad hoc or interactive capabilities on the applications, systems, transactions or data involved.

XII. Authentication and Passwords

A. Overview

All systems, applications, databases or other information repositories shall require users to authenticate themselves prior to granting access. Authentication may be via an approved password scheme or via an access control device. All systems that support 2-factor authentication must have them enabled.

The authentication method used must suit the value of the information asset, matching the cost of the authentication method against the level of protection required. In general, administrative and other high-value User or Service IDs will use the most secure methods of authentication.

B. Password format

Must be at least twenty (20) characters in length and must contain characters from all of the following four (4) categories:

1. English uppercase characters (A through Z)
2. English lowercase characters (a through z)
3. Base 10 digits (0 through 9)
4. Non-alphabetic characters (for example, ! , @, #, $)

C. Rules

Users are forced to create a new password every 3 months. Users must not write down on paper or store any passwords; they must also never share their passwords with other users. Software is provided to securely store user passwords, with encryption.

A maximum 5 attempts will be permitted prior to disabling the account. New passwords must be different from the previous three (3) passwords. Passwords must be changed immediately upon first use of a new ID. Passwords must never be stored or transmitted in clear text. Systems must not echo back the password as it is entered.

Passwords must not be retained by any system or application longer than is needed to grant access. Initial passwords must be transmitted separately from the ID.

XIII. Authorization and Rights Management

A. General Access Roles

Access roles are defined as:

1. *Super Admin Access:* Access to all front and backend products as well as product metrics
2. *Admin Access:* Access to all front end products as well as product metrics
3. *General Access:* Access to product metrics
4. *Low Access:* Access to corporate email, sales, and marketing data only

Amazon Web Services (AWS)
Users who have access to AWS have Super Admin Access. User sessions will expire after one (1) hour of inactivity

Cloudant
Users who have access to Cloudant have Super Admin Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

Github
Users who have access to Github have General Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

ELK Stack
Users who have access to ELK Stack have Admin Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

Mixpanel
Users who have access to Mixpanel have General Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

Kissmetrics
Users who have access to Kissmetrics have General Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

Salesforce
Users who have access to Salesforce have General Access. User sessions automatically time out after twenty (20) minutes.

Segment.io
Users who have access to Segment.io have General Access. User sessions do not automatically time out, the user is required to log out at the end of a session.

B. Access Rules

User IDs and accounts must be authorized to access only those elements needed for the user's role, including:

1. Limiting access to datasets and types
2. Limiting access to operating systems
3. Limiting times of access

Access to operating systems, ad hoc transaction capabilities, software development tools, and other system devices must be controlled and limited to only those User IDs which require that access.

Segregation of duties shall be established for all information asset controls to minimize the possibility that one person is responsible for an entire asset.

A user (and hence User ID) that changes role or job function must have access rights updated to match the new job role or function. Any changes will be documented in the *Responsibility Change Log*.

C. Temporary Privileged Users and Accounts

Temporary privileged users are defined as those who:

1. Have any control over security tools on an application, system or network
2. Can update operating systems or similar tools
3. Can directly modify data within a database or application
4. Have any special capabilities built in by the vendor of the application software, operating system or platform

Access at a temporary privileged user level shall be granted only on a need-to-know, need-to-perform basis, and then only to the assets required. Temporary privileged user access shall only be granted to those supporting **Virtru's** applications, networks and systems.

D. Assignment and Revocation Procedure

The ISO shall electronically complete:

1. An Employee *Access Log* for all new hires and/or workforce member change of status.
2. An *Exit Checklist* for all terminations.

E. Logout After Inactivity

The ISO shall verify that all users have activated a password-protected screensaver that automatically prevents unauthorized users from viewing or accessing electronic protected information from any system or device that can be used to access electronic information systems. After a maximum of 10 minutes of inactivity the system should log off and lock the device, making information inaccessible. Once logged off a user must re-enter a password to gain access to electronic protected information.

XIV. Breaches or Impermissible Uses/Disclosures

A. Definitions

Incident is defined as any breach of security, privacy, continuity, legal or regulatory controls over information assets of any type. Examples of such incidents include but are not limited to:

1. Penetrations of systems, applications, networks or databases
2. Denial of service attacks
3. Misuse or mishandling of assets
4. Virus or other malware contamination
5. Transaction errors
6. Breaches of confidentiality agreements or contracts
7. Legal or regulatory violations

Breach is defined as an impermissible access, use or disclosure, which compromises the privacy or security of PHI.

XV. Breach Response

A. Overview

Virtru will maintain an effective method so that all information users, custodians and owners can readily report incidents.

Incidents will be reported to the person's immediate manager or the ISO. Once the ISO has been notified, said Officer will then follow the directions in the *Incident and Breach Policy*.

The ISO will investigate incidents and will log or report significant losses or threats immediately. The appropriate authorities will be contacted by the ISO depending on the severity of incident.

Incidents involving misuse by workforce members will be investigated by the ISO.

Depending on the severity of the incident, the Emergency Contact list may provide additional contacts. See the *Emergency Contact List* located in the *Disaster Recovery Plan*.

Confidential Reporting:

Confidential reporting may be done either by:

1. Calling (may leave voice message) the ISO or AISO
2. Sending an email to the ISO or AISO, or;
3. Google Form for anonymous reporting

XVI. Personnel Security

A. Screening for newly hired personnel, third parties, vendors

Proper verification checks must be made prior to granting any new workforce member, contractor, vendor, agent or affiliate access to Private, Internal, Confidential or Protected information. These verification checks will meet the requirements set forth by the **Company** and may include:

1. Professional qualifications
2. Identity checks
3. Criminal checks
4. Confirmation of academic and professional experience

The ISO is responsible for ensuring that background checks are made biannually on parties who are not newly hired workforce members. A third party will conduct background checks.

B. Training and Awareness

Virtru will provide security awareness training to each new member of our workforce with access to electronic **Company**-owned or private data (Refer to Data Types information Classifications) whose activities in the business we directly control. The training will be provided prior to that person assuming his/her duties. The training is designed to inform the person of his/her responsibilities under **Virtru's** security policies. At a minimum, this training will include the workforce member's role in:

1. Managing malicious software (e.g. viruses)
2. Using workstation(s) securely
3. Managing passwords and
4. Monitoring and reporting suspicious use of account(s)

Virtru's employees will also be trained annually on **Virtru's** Policies and Procedures. A record of successful completion of this training and annual retraining will be kept online by **Total HIPAA Compliance**.

Within 30 days of starting, individuals who are employed as developers will receive training on the security measures and mechanisms used to protect the company's systems and service. All new developers will be required to take and pass online training modules covering secure coding when using Node.js. Developers who will be managing or developing operational aspects of the company's systems will also be required take the Security Operations on AWS training course from Amazon.

A record of training will be kept of training that lists the employee, type of training, date of completion, the employee's signature, and an admins signature asserting successful completion of the training.

C. Terms of employment

Compliance with **Virtru's** policies regarding security and privacy are a condition of employment.

D. Acknowledgement

All users shall be required to sign an acknowledgement after being trained on **Virtru's** security and privacy policies.

E. Exit process for users

Upon exiting employment or any relationship with **Virtru**, all users who have been granted access to any information asset shall:

1. Relinquish all access to control devices
2. Report all User IDs in use by the person
3. Relinquish all information stored, whether on paper or on backup media
4. Relinquish all information processing devices, including workstations, all **Virtru**-owned mobile devices and others

All systems access will be revoked.

The ISO will verify termination is completed, and document this procedure has been followed. See *Exit Checklist.*

F. Security Sanction Policy

Virtru's security policies call for the workforce that has access to electronic Protected Employee or Client Data and others to perform certain duties and to refrain from certain actions. Failure to do so will be sanctioned according to the policy below.

If the infraction involves the unauthorized use or disclosure of electronic Protected Employee or Client Data, the sanctions below apply to the designated workforce members including managers, supervisors, and staff who have access to Protected Employee or Client Data.

We define a serious infraction as one that results in known significant damage or that threatens imminent significant damage. Other infractions are simple infractions. The process below is intended as guidance for our business management in sanctioning Security Policies and Procedure infractions. We reserve the right to implement sanctions differently if, in our judgment, the situation warrants it.

First Security Infraction

If the infraction is:

1. A simple infraction, and
2. The first infraction in the last 3 years

The sanction will be retraining the workforce member on the appropriate policy/procedure and placement of a written letter of reprimand in the employee file.

The letter will notify the person of the nature of this infraction and of sanctions for future potential infractions.

Second Security Infraction or First Serious Infraction
If the infraction is:

1. A serious infraction, or
2. The second infraction of either type within 3 years

The sanction will include a written letter of reprimand that is given to the person at fault, placement of a copy of the letter in the employee file, and one week's suspension without pay. The letter will notify the person of the nature of this infraction and of sanctions for future potential infractions.

Third Security Infraction or Second Serious Infraction
If the infraction is:

1. A second serious infraction within 3 years, or
2. A third infraction of any type within 3 years

The sanction will be dismissal from the workforce.

XVII. Legal and Regulatory Issues

A. Legal processes

Responses to subpoenas, deposition requests and other legal issues will be referred to and handled by the CEO. The ISO will not respond to such legal processes without company legal counsel.

B. Copyrights and licenses

Virtru may have agreements in place governing the use and handling of software, information and other tools that are owned by other entities. All users and information owners will comply with those agreements.

Users are responsible for complying with copyrights regarding any material obtained via the Internet. This includes files, graphics, software, audio and video materials.

Users may not agree to a new copyright license, unless given permission by the ISO.

Licensed software must be used in accordance with the license agreement and only the number of copies licensed must be created or used.

C. Export controls

Information may not be exported across country boundaries without prior written approval of the **Company**'s ISO.

XVIII. Malware and Antivirus

A. Definitions

Anti-Malware: malicious software that may reside on a computer, steal information or cause destruction. This can include a virus, trojan horse, keylogger, hijacker or dialer.

Sandbox: A highly controlled area where programs and software can be tested before being allowed access to the rest of the system.

B. Operating system anti-malware requirements

Macintosh, Linux and iPhones:
Virtru has determined that software for anti-malware scanning on Macintosh, Linux and iPhones is not necessary due to the low probability of encountering malware, the demand on computer processing power, and loss of productivity by the user. This policy will be reviewed annually or as needed to determine if this is still valid.

PC Operating Systems:
Data entering **Virtru's** Window-based systems must be subject to an up-to-date anti-malware scanning tool that is scheduled to run at regular intervals. In addition, all emails, attachments, disks, backup media, USB memory devices and other data carrying tools must be scanned before they are downloaded or allowed access to the system. All incoming data must be sandboxed by the anti-malware program before it is allowed access to the system. The anti-malware pattern files must be regularly updated.

Android and Windows Phone Operating Systems:
All such devices must have anti-malware tools in place prior to being connected to **Virtru's** networks. These systems must be subject to an up-to-date anti-malware scanning tool that is scheduled to run at regular intervals. In addition, all emails, attachments, and SD cards must be scanned before they are downloaded or allowed access to the system.

C. Affiliates

Virtru and all of its affiliates, contractors, consultants, vendors, representatives or other service providers must make certain that adequate controls are in place to guarantee that data coming from their systems and networks is free from malware.

D. Infected devices

The ISO will use approved tools to monitor and remove malicious software from **Virtru's** assets. Virus-infected computers, tablets or phones must be removed from the network immediately until they are verified as virus-free.

E. Employees' Requirements

1. Workforce members will not load software on our **Company's** information equipment without permission from the ISO.
2. Workforce members will not open electronic files from unfamiliar sources.
3. Will exercise best practices when using the **Virtru** network. The employee will not:
    a. Circumvent user authentication on any device
    b. Sniff network traffic
    c. Access data, servers, or accounts they are not authorized to access
    d. Cause a disruption of servers
    e. Violate copyright law by transmitting copyrighted pictures, music, video and/or software
    f. Export or import software, technical information, encryption software, or technology in violation of international or regional export control laws
    g. Use the Internet or network in a manner that violates **Virtru's** Security Policies, or local laws
    h. Intentionally introducing malicious code; including, but not limited to, viruses, worms, Trojan horses, e-mail bombs, spyware, adware, and keyloggers

The workforce will be trained to know and carry out these malware protections. The ISO will generally provide permissions as required above only for actions that are intended for our **Company's** business and only under conditions that limit the potential for the introduction of malware.

F. Enforcement

Any activities with the intention to create and/or distribute malicious programs into **Virtru's** networks (e.g., viruses, worms, Trojan Horses, e-mail bombs, etc.) are prohibited, and user will be subject to **Virtru's** Sanction Policy, and will be reported to the proper state and federal authorities.

XIX. Change Control Logs

A. Preface

The ISO is required to maintain logs of systems that document any changes and access users may have to sensitive systems. The following are the retention policies for these logs.

B. Policy

Audit logs will be retained for at least one (1) year in raw format, preferably electronic, to preserve evidence. Audit logs must be configured to prevent overflow, erasure or tampering. Audit logs will be configured to record information such that:

1. Sufficient information is available for proper investigation of use, misuse, incidents and performance
2. User ID, event type, date and time are maintained
3. Time is according to a known time stamp so that events across systems can be coordinated
4. End-to-end accountability is always maintained

Events to be recorded include, but are not limited to:

1. Login and activity by any other privileged accounts
2. Changes to operating systems, application code or other tools
3. Backup and restore events
4. Changes affecting any cryptographic keys or devices
5. Stop or start of critical processes
6. Transaction failure, retry or duplication

All systems and tools involved in the protection process are required to always have change logs enabled and properly configured. This includes:

1. Firewalls
2. Email servers
3. Anti-malware tools especially the administration tools
4. Security administration tools such as password resets and account modifications
5. Monitoring tools
6. Routers and other network devices
7. Github
8. Amazon Web Servers (AWS)

9. IBM Cloudant
10. SalesForce
11. Elk Stack
12. Mixpanel
13. KissMetrics
14. Segment.io
15. Sendgrid
16. Customer.io

Logs will be reviewed and analyzed by delegates of the ISO.

Reports of problems and incidents will follow the incident reporting method, listed in the *Incident and Breach Policy*.

XX. Encryption

A. Preface

Encryption is the process of encoding messages of information is such a way that only authorized parties can read it.

B. Application Encryption Policy

Virtru encrypts all client data using NIST-approved cryptographic modules. **Virtru** uses AES 256 encryption for its application. **Virtru's** key length requirements shall be reviewed annually as part of the yearly security review and upgraded as technology allows.

The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the ISO.

C. Key Rotation Policy

Virtru requires the following key rotation policy to protect all external systems. The following is the list of policies for the following keys:

1. **Secure Socket Layer (SSL)Keys**
   Virtru uses SSL keys to enable Transport Layer Security (TLS) traffic between clients and **Virtru's** servers.

   Rotation Policy

Rotation of SSL Keys is done upon SSL Key expiration. They are set to expire at 1 (one) year and rotated at that time. If there is an incident or the security keys are thought to be compromised, the keys will be rotated immediately.

2. **Secure Shell (SSH) Keys**
   The SSH keys provide a layer of authentication to get into the production servers. SSH Keys are used as the authentication mechanism to remotely login to a server. They are also used as the first factor of authentication to assume root access on the production servers. Each developer has his/her own SSH key and is responsible for keeping this key secure.

   Rotation Policy
   All SSH keys are rotated at a minimum of every three (3) months. If there is an incident or the SSH keys are thought to be compromised, keys will be rotated immediately.

3. **Amazon Web Services (AWS) Access Keys**
   Unique AWS Access Keys are given to each developer with a unique AWS Login. This allows the developer to make Application Protocol Interface (API) calls to AWS. Currently, 1-2 AWS Access keys exist per developer. Where are these stored? How do you know how many keys each developer has?

   Rotation Policy
   These keys are rotated at a minimum of every 90 days. If there is an incident or the AWS keys are thought to be compromised, keys will be rotated immediately

4. **Application Keys**
   Virtru uses these keys to encrypt sensitive key data stored in the CouchDB database managed by IBM. There is only one copy of this key.

   Rotation Policy
   No rotation requirement.

   Backup Policy
   Backup of the key is kept with **Virtru's** Super Administrators.

The export of encryption technologies is restricted by the U.S. government. Residents of countries other than the United States should make themselves aware of the encryption technology laws of the country in which they reside.

Security Policies and Procedures

D. Device Encryption Policy

Virtru requires devices have encryption enabled for any files, folders, drives, databases, or other stored data that may have sensitive information including protected personally identifiable information.

The implementation of any encryption scheme is performed by the user and the deployment of the encryption tool, including all keys, must meet industry best practices and be properly documented. Currently the minimum standard is 128-Bit encryption. Encryption keys will be managed by the user and a log will be maintained by the ISO.

Mac OS Devices:
Mac OS devices that store Protected Information (PHI, CJIS, etc), are required to use full disk encryption using FileVault 2. Users must provide a copy of their key to the ISO; both will maintain the key in a secure location.

For devices that do not store Protected Information (PHI, CJIS, etc), full disk encryption is at the discretion of the user. However, if this is used, a copy of the encryption key will be stored by both the user and the ISO in a secure location.

Windows OS Devices:
Windows OS devices that store Protected Information (PHI, CJIS, etc) are required to use full disk encryption with the program Bitlocker. The encryption key will be maintained in a secure location by both the user and the ISO.

For devices that do not store Protected Information (PHI, CJIS, etc), full disk encryption is at the discretion of the user. However, if this is used, a copy of the encryption key will be stored by both the user and the ISO in a secure location.

Linux OS Devices
Linux OS devices that store Protected Information (PHI, CJIS, etc) are required to use full disk encryption. This will be encrypted at a minimum of 128 bit encryption. The encryption key will be maintained in a secure location by both the user and the ISO.

For devices that do not store Protected Information (PHI, CJIS, etc), full disk encryption is at the discretion of the user. However, if this is used, a copy of the encryption key will be stored by both the user and the ISO in a secure location.

Android Devices
All Android devices that store Protected Information (PHI, CJIS, etc) will have encryption turned on and will be password protected at all times. The encryption key will be maintained in a secure location by both the user and the ISO.

Windows Phone
All Windows Phones that store Protected Information (PHI, CJIS, etc) will have encryption turned on and will be password protected at all times. The encryption key will be maintained in a secure location by both the user and the ISO.

iPhone
iPhones are natively encrypted. These devices are required to be password protected and/or biometrically protected at all times.

E. Wi-Fi network encryption

All wireless access points owned by **Virtru** are required to be protected using Wi-Fi Protected Access 2 with Advanced Encryption Standard (WPA2-AES). This password will be changed quarterly and will not be shared with users that are not employees or authorized Business Associates. Any outside users are required to use guest access points.

Employees that access **Virtru** resources from home are required to use Wi-Fi Protected Access 2 with Advanced Encryption Standard (WPA2-AES) to protect their devices. This password should be changed quarterly.

F. Email encryption

Virtru requires the use of its secure, encrypted email service to communicate with our employees about their Personally Identifiable Information, and to communicate any sensitive data. All email communication that includes personally identifiable data, and potentially sensitive data will be encrypted.

Virtru uses only its secure, encrypted email service to communicate with clients about their Personally Identifiable Information.

Virtru forbids the use of chat, texting or instant messaging programs by devices that store PHI.

G. Enforcement

Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.
See *Sanction Policy*.

XXI. Assessments and Testing

A. Overview

The Security Rule of HIPAA mandates that covered entities implement appropriate information security policies and procedures to protect PI from "reasonably anticipated threats and hazards."

B. Penetration testing

Penetration testing of all servers containing PII will be conducted monthly by internal personnel, and by an external 3rd party at least annually or whenever there is a major system update. Testing shall validate the security of:

1. External connections
2. Operating systems
3. Applications
4. Databases
5. Network controls
6. Security procedures, including monitoring and incident response

C. Vulnerability assessment testing

Vulnerability assessments will be conducted periodically on all network-connected systems devices. Any vulnerability found must be corrected in a timely manner. Vulnerability assessments also shall be conducted when:

1. A new system, application or network is installed inside the Company
2. Changes are made to firewalls, VPNs or other security control tools
3. Changes are made to a web server's operating system
4. Changes are made to email servers
5. Configuration changes are made to databases
6. Configuration changes are made to critical applications
7. Changes are made to encryption scheme(s)

NOTE: *Vulnerability and penetration tests will not be conducted except with the prior approval of the ISO. No user will have vulnerability or penetration testing tools loaded onto any* ***Company*** *system without prior permission from the ISO.*

D. Wireless access testing

Testing of wireless access points (war-driving) shall occur regularly, to cover all wireless access points under the control of **Virtru**.

E. Password testing

Password cracking software shall be run periodically to validate the enforcement of password rules.

F. 3rd Party Security Management

A comprehensive list of 3rd parties with which the company does business with shall be maintained. Any 3rd party who handles or holds sensitive data or who provides a service which is critical to operations shall be required to assert that their own security practices and procedures meet or exceed that of the company's. Each 3rd party shall be assessed for conformance annually.

XXII. Use of Email, Internet, Messaging, Public Sites, Blogs, Social Media

A. Policy

Confidential, Private or Protected information and Internal Use information must not be transmitted across any unsecured outside network or path without proper controls. **Virtru** requires encryption for files and emails, or secured packaging for paper copies.

Users are responsible for ensuring that their use of these tools complies with all of **Virtru's** policies, and with applicable laws and regulations. This includes all employment policies such as sexual harassment, stalking, ethics and appropriate use.

These tools may not be used to access, send or receive, store or display:

1. Sexually explicit material
2. Confidential, Private or Protected Information or Internal Use material, except as meets the *Handling Rules* section
3. Viruses
4. Threats
5. Inappropriate or unlawful language, including:
    a. Offensive language
    b. Language inappropriate for the **Company** environment
6. Discriminatory or harassing language
7. Tools usable for hacking, password cracking, vulnerability scanning or penetration testing

These tools are the property of **Virtru** and are to be used only for **Virtru's** business. Access may be unavailable at any time, at the **Company's** discretion. Users must not assume that access to these tools will be available for incidental personal use.

All content transmitted over these tools is the property of **Virtru**. Content, including emails, may be inspected by **Virtru**. Such inspections will occur with the approval of the ISO or of the **Company** legal department. **Virtru** may monitor, filter or block content on these tools.

Users of blogs, social media sites such as Facebook, and other such tools must follow the guidelines outlined in **Virtru's** Social Media Policy. See *Social Media Policy*.

Users of blogs, social media sites such as Facebook, and other such tools must not represent their comments as coming from, or being representative of, the business or opinions of **Virtru**.

XXIII. Hardware

A. Definitions

Workstations: PCs, desktop computers, tablets and mobile computing devices that are located at **Virtru's** home office, or at remote locations. These devices are easily attacked and therefore must have access controls and anti-malware as specified in those sections of this document.

Servers: Devices that may or may not be housed at **Virtru** locations. Regardless of their location, these must secured in a manner that prevents them from being physically accessed without the appropriate level of security clearance.

B. Policy

A current copy of the *Organizational Chart/Electronic Asset Management Log* (**Risk Assessment**) will be kept at an off site location so it can be accessed quickly in the case of theft, fire, flood or other events that may make inventory information useful.

The ISO will keep a log of events noting when a physical security mechanism is repaired, replaced, installed, removed, modified, or maintained. This *Maintenance Log* will contain the: who, what, when, where, and why of the change and be kept in the **Security Documentation Library**.

Users of these devices are required to ensure that all appropriate protections are in place, including:

1. Physical security to prevent theft or misuse
2. Access controls suitable for the class of information on the device
3. Anti-malware
4. Keeping the devices locked to a desk or other secure location when outside

5. Keeping control over backup media, as to minimize the possibility of theft or loss
6. Ensuring that the transport of these devices is secure and is safe from damage - for example, these devices should only travel in padded containers and should be locked and shut down during transit
7. Keeping all operating systems and tools up-to-date, with all updates and patches. Specific requirements for these topics are in the appropriate sections of this document

Virtru's devices must not be used by people who are not authorized, including family members and friends.

Software loaded onto such devices must follow the rules in the *Software* section of this document. In general, only approved software may be loaded, and shareware, games and other such software are not permitted.

International travel with these devices may require special approvals or configurations, especially in regards to encryption and licensed software. Before traveling internationally, users must contact the ISO to determine if such special considerations exist.

Connecting these devices to **Virtru's** networks must follow the rules in the *Networks* section of this document. In general, all such devices must be approved prior to connecting.

Remote access from these devices to **Virtru's** networks and devices must meet the controls specified in the *Networks* section of this document. In general, such access must be approved, and must have adequate controls over the security of information in transit.

Devices of these types that are owned by contractors, vendors or other third parties must meet all **Virtru** requirements prior to being connected.

C. Asset management

The ISO is responsible for maintaining an inventory of devices; as such he shall employ software to aid in the management of hardware and software asset. See *Handling Rules for the information classifications*

D. Enforcement

Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. See *Sanction Policy*.

XXIV. Networks

A. Overview

Virtru's networks and devices shall designed, deployed and operated in a manner so as to provide proper levels of protection for the data being accessed and transported. Significant changes in network designs must be piloted before deployment.

Mechanisms must be in place to alert the ISO of possible attacks and breaches, to include:

1. Denial of service attacks
2. Improper access
3. Virus infections
4. Unauthorized software installations, email, FTP or other improper usage

Analysis must be conducted at least annually to validate the failure mode and recovery for all devices, network circuits and protocols. See *Change Logs* for details.

Responsibilities must be defined for:

1. Administration of network and communications connections
2. Operations of all devices
3. Monitoring
4. Timely review of audit logs and response to alerts or alarms
5. Review of unusual patterns of usage or activity

To minimize risks, any network connections or network segments should be disconnected when not in use.

B. Monitoring

Virtru uses AlienVault's Unified Security Management System to monitor all traffic on their network. Notifications are set to alert the IT staff of any unusual traffic and vulnerabilities, as well as log any security events that may occur.

C. Access control and physical security

Sites where **Virtru's** network equipment or communications lines exist are considered to be high-value and are subject to the access control and physical security rules

outlined in the *Physical Security* section of this document. In general, these rules will require:

1. Access limited to authorized personnel only
2. Physical security, including RFID or passcode controlled locks, are in place

D. Modifications, updates

Changes to the network architecture which affect the protections must be approved by the ISO. Examples of such changes include firewalls, wireless configurations, ports and proxies.

E. Documentation

The ISO shall maintain an accurate set of documentation of the networks and their components. This documentation is considered to be highly valuable and will be classified "Protected".

F. Network design

The goal for network design is to facilitate **Virtru's** business, while still providing protection for **Company** assets.

G. Segmentation

Virtru's networks will be segmented, in order to limit access to Confidential and Protected Information, without impacting the **Company's** business. There will be a guest network that will have no access to **Virtru's** Network Attached Storage, and other vital network resources.

H. Firewalls

Virtru's network and workstations in the DC office is protected using the Fortinet FortiGate 100D Firewall appliance. This device is configured to monitor and log all unusual traffic and warn **Virtru** of any network irregularities or attacks.

Definitions

Firewall: A part of the computer operating system or network that is designed to block unauthorized access while permitting outward communication. There are two different types of firewalls.

1. *Software Firewall:* Part of the operating system or can be a software add-on.
2. *Hardware Firewall:* Built into a router or a stand alone device. All computing devices will access a network through this point.

Firewall Settings

1. *Whitelisting:* Blocks all incoming traffic, and only allows traffic from good, or known IP addresses. The user will be required to authorize connections to their device.

2. *Blacklisting:* Authorizes all traffic as a default, and the user is responsible for denying unauthorized connections to their computing device from unrecognized or unknown IP addresses.

Software Firewall Policy

Virtru requires every device to have their internal software firewall activated at all times, and set to only allow whitelisted traffic. This will require the user to authorize any connections to their device. Any workforce member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

I. Internet

Connections to the Internet must be:

1. Approved by the ISO
2. Periodically reviewed and tested for vulnerabilities
3. Protected by firewalls, intrusion detection systems and anti-malware tools

Some Internet tools, such as FTP, Internet Relay Chat, Telnet and Remote Procedure Call are restricted in use and must be approved for use by the ISO.

J. VPN-remote access

Virtual private networks (VPNs) will be used for traffic flowing over public networks to ensure the proper level of protection of **Virtru's** data.

K. Wireless

All wireless connections must have WPA2 with Advanced Encryption Standard (AES) turned on. This applies to all networks for **Virtru's** home office, and all telecommuting employees.

L. Telework Policy

If a staff member is allowed to telework/telecommute, they must comply with the **Virtru's** various employment policies, remote security measures and use the provided web portal via HTTPs, VPN and SSL. They must also make sure their home WI-FI is encrypted properly.

If they are accessing sites while on an unsecure router, they must make sure the sites they visit have a valid SSL certificate before proceeding.

M. Patching of systems and applications

Microsoft Windows OS Patches

Security Policies and Procedures

To manage the patching of Microsoft Windows operating systems (OS), Windows Software Update Service (WSUS) is used. The WSUS server automatically checks for patches once a day not during business hours. Then downloaded patches are manually released from the WSUS server to be downloaded and applied on the workstations. The ISO will evaluate all patches before they are applied; workstations will not automatically download OS patches from the WSUS server and updates will not be automatically installed. Installation of OS patches is done within a planned downtime.

Apple OS Patches
All Macintosh Operating System (OS) patching will be done through the App Store, and is the responsibility of the individual user to install. These should be applied within one (1) week of release from Apple.

Linux OS Patches
These patches should be applied and tested in an app staging environment before they are applied systemwide. The User is required to document where they received the patch, who downloaded it, what version of patching they are using, and when the patch was applied to the system. This documentation should be submitted to the ISO upon completion of the patching.

iPhone iOS Patching
All iPhone (OS) patching will be done through the App Store, and is the responsibility of the individual user to install. The device should be fully backed up prior to installing these patches either in the cloud or locally. All backups are required to be encrypted and password protected. These patches should be applied within one (1) week of release from Apple.

Android Phone Patching
All Android patching will be done through the Google Play Store, and is the responsibility of the individual user to install. The device should be fully backed up prior to installing these patches either in the cloud or locally. All backups are required to be encrypted and password protected. These patches should be applied within one (1) week of release from Google.

Windows Phone Patching
All Windows Phone patching will be done through the Windows Phone Store, and is the responsibility of the individual user to install. The device should be fully backed up prior to installing these patches either in the cloud or locally. All backups are required to be encrypted and password protected. These patches should be applied within one (1) week of release from Windows.

Patching of applications is done on a weekly basis, unless a zero-day exploit is found in an application that is used within the domain. If such an exploit is found and a patch is released for said exploit, an emergency planned downtime will be called for at the conclusion of the business day to patch the application in question.

N. Network hardening

Upon adding new devices to the network, installation procedures and set-up must be followed. Hardening will be done on network devices as well as systems (e.g. laptops, workstations and servers) and handled by the ISO or AISO.

Hardening will be broken down into the following categories which include, but are not limited to:

1. Preparation and installation
2. Updates to: software, firmware and hardware
3. Setting of appropriate account and auditing rules
4. Setting of appropriate security rules
5. Turning on the internal firewall
6. Turning on full disk encryption (If device will have access to PHI)
7. Other internal operations such as:
    a. Installation of appropriate software for workstation, server or laptop

The ISO will notify all affected staff when making changes to the hardening policy and will update the Security Policies and Procedures at that time. Written approval for hardening procedures above and beyond what is currently mandated is not necessary.

XXV. Physical and Environmental Protections

A. Definitions

Secure sites: These are locations that require the highest level of protection. These sites include:

1. Computing centers
2. Network connection points
3. Media storage locations
4. Locations containing platforms which carry high-value or critical information or transactions

Physical Security: These may occur within **Virtru** where the overall building is operated to a lower level of security, but a certain area is more controlled due to documents, assets or processes which occur in that area.

B. Secure Sites Policy

Secure sites shall be established for all computing centers and other locations where there is a concentration of high-value or sensitive information, systems or networks.

Sites will be designed and operated according to best practices and in consideration of threats appropriate to the site such as hurricanes, tornados, power outages and intruders.

This standard is not to be construed as a complete list of requirements for a secure site. It should be used in conjunction with expert advice, architects, fire marshals, OSHA and other regulations.

Separate, isolated areas will be created within the secure site for:

1. Media libraries
2. Electrical supplies and controls
3. Environmental and mechanical controls

Access to these sub-areas will be on a need-only basis. Critical assets and operations must be conducted in a secured area or secured site, with protections implemented in accordance with the risks and value of the assets, information and operations.

C. Data Centers

All data centers used by the company must provide proof that they meet or exceed the security requirements and standards of the company.

XXVI. Physical Security Policy

A. Entry Policy

All **Virtru's** workforce members are allowed access to the physical site at any time of the day, and any day of the week. The site is secured with an electronic door lock that accepts RFID cards and a numeric passcode. RFID cards are issued by the ISO or AISO by request and after approval.

B. Loss of RFID key

If a workforce member loses their RFID key, they will notify the ISO or AISO as soon as possible so the key may be deactivated. Any workforce member found to have violated

this policy may be subject to disciplinary action, up to and including termination of employment. See *Sanction Policy*.

C. Mobile devices

Mobile devices (laptops, netbook, tablets, iPhones, iPads, etc.) must have the appropriate encryption. Devices must have a power-on password or PIN, data encryption, auto-lock and role-based access per user. See *BYOD Policy* (**Forms for Employees**).

D. Video monitoring

Virtru's main office is monitored by a video camera. The data is stored in the Network Attached Storage which is physically secured in a locked cage in the IT closet. This data is stored for up to one (1) month.

E. Alarm system

Virtru's main office is monitored by an alarm system. It is attached to all doors and windows, and requires a 4-digit pin plus a modifier to deactivate. Once triggered, there is a 45-second delay before the local authorities, ISO and CEO are notified by the monitoring company. ADT is the company that is responsible for monitoring **Virtru's** main office.

The alarm pin code is changed quarterly, or at the time that an employee is fired or leaves the Company.

Virtru requires that this alarm be set by the last person to exit the office, and should be active anytime there is not an authorized employee on the premises.

F. Fire protection

Fire protection meet all regulations, including federal, state and local. Fire extinguishers shall be deployed in accordance with regulations of OSHA and fire inspectors. Periodic testing of alarms, fire extinguishers and fire evacuation procedures shall be conducted.

XXVII. Software

A. Overview

This section outlines the standards applying to operating systems, applications, databases and other software tools.

B. Acquisition of software

It is up to the developer to decide which software tools they will require for their workstation. All regulated software will only be download from trusted sources, such as the Apple App Store, Windows Store, or directly from reputable websites, etc.

Unregulated software is allowed, but must be fully documented and approved for use by the ISO. Documentation will include:

1. The source of the software
2. When it was downloaded
3. Who downloaded it for use and;
4. The date the ISO approved the use of the software

All software for Windows OS devices is required to be screened for malware prior to installation.

Any unauthorized software must be approved and validated, or removed.

Users of workstations, netbooks, wireless and other personal devices must not install unapproved software.

C. Open Source Software

The use of open source shareware or open source freeware may only occur if:

1. It is not used in a production environment OR
2. Prior to use it is fully tested, documented and **Virtru's** personnel are assigned to support it. Checks to be performed include:
    a. Verify usage license (no strong or weak copyleft licenses)
    b. Review open CVEs and available patches
    c. Perform internal security evaluation
    d. Flag for external security evaluation during next penetration test
3. The source of the software is documented
    a. URL
    b. Project lead
    c. Contributors
    d. Whether the project is actively maintained
4. The ISO approves of the use

D. Documentation

Documentation for sensitive applications and the operating systems which run those systems shall be stored securely. Backups of all documentation shall be maintained off

site. Access to the documentation for sensitive applications and the operating systems will be on a need-to-use basis.

E. Change Control and Maintenance

All proposed changes to production systems must be registered in the companies issue tracking system. Changes shall be categorized as standard, normal, or emergency. Standard changes are those that are performed frequently and considered low risk. Standard changes are reviewed quarterly and pre-approved for the following quarter. Normal changes are those which are not performed frequently and may pose some risk to the business. Each normal change must be reviewed by a minimum of two super-admins, the CTO and/or VP of engineering prior to being made. Reviewers are responsible for assessing the impact of the change in regards to the functionality, availability, durability, and security of the system. If a consensus among reviewers is reached, the proposed change is sized, sorted, and executed through the standard engineering workflow. Emergency changes are those that are required to rectify some form of degradation of the system. Emergency changes must be reviewed by a minimum of two super-admins. If a consensus is reached, emergency changes can bypass the standard engineering workflow and be made immediately. All changes to production systems must be captured in the company's issue tracking system without exception.

F. Operating Systems

Only approved operating systems will be loaded onto **Virtru**-owned assets. Before major upgrades to systems, authorization by the ISO and AISO will be required.

Default settings must be reviewed prior to installation to identify any security vulnerabilities. These settings will be communicated with all workforce members, or they will surrender their devices to the ISO or AISO for configuration.

G. Applications

All applications, whether developed or purchased, must comply with **Virtru's** policies and protection standards. The information owner is responsible for ensuring that these requirements are included during the development or acquisition of software.

The protection requirements for applications include:

1. Access control
2. Authorization
3. Information classification
4. Storage controls
5. Backup and restoration
6. Confidentiality and integrity requirements
7. Audit logs
8. Privacy, export control and other such requirements

All product associated applications must use HTTPS to communicate with all remote hosts, both Virtru hosted services and external third parties. HTTP and other non-encrypted communications are not allowed under any scenario.

Virtru applications shall treat user credentials with the utmost sensitivity and must follow security best practices for storing and transmitting user credentials. All credentials which are shared with a client device must be sent over HTTPS or another encrypted communication channel. All user credentials which are stored in a data store, must be stored in a benign state so that leakage of information from the data store does not compromise user accounts.
All application logs must be sent to a central logging cluster for aggregation and analysis.

H. Configuration Management

Where possible, Virtru applications and infrastructure follow an immutable paradigm. All changes to production infrastructure and application code is deployed on a brand new Amazon Machine Image (AMI). This allows all changes which are deployed to be tracked and audited. This also means that no configuration or application code will be modified on a production instance. All application servers have osquery installed and configured to monitor key files on the system for any change (File Integrity Monitoring). Any changes to configuration are logged and sent to AWS Cloudwatch Logs, where they trigger an alarm and cause an email to be sent to the Virtru DevOps team for further investigation.

Where possible, Virtru utilizes Terraform, Ansible, and other similar tools to define their infrastructure as code. This allows the production infrastructure to be versioned in a git repository and easily audited for change over time.

I. Asset management for software

The ISO is responsible for maintaining an inventory of software; as such it shall employ software to aid in the management of software assets.

J. Enforcement

Any workforce member found to have violated these policies may be subject to disciplinary action, up to and including termination of employment. See *Sanction Policy*.

XXVIII. Removable Media Device Policy

A. Purpose

The purpose of this policy is to minimize the risk of loss or exposure of Confidential or Protected Information maintained by **Virtru** when it is stored, transferred or accessed on a removable media device. This policy also aims to reduce the risk of acquiring malware infections on computers operated by Company. Any questions or comments about this policy should be directed to the ISO

B. Scope

This policy covers all removable media that contains **Virtru's** data or that is connected to **Virtru's** network.

C. Definitions

Removable media: devices or media that is readable and/or writable by the end user and are able to be moved from computer to computer without modification to the computer. This includes flash memory devices such as thumb drives, SD cards, cameras, MP3 players or any other storage medium; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks.

Encryption: a procedure used to convert data from its original form to a format that is unreadable and/or unusable to anyone without the tools/information needed to reverse the encryption process.

Malware: software of malicious intent/impact such as viruses, worms, and spyware.

D. Policy

Workforce members may use removable media in their work computers if they take all reasonable and prudent measures to ensure the safety and confidentiality of all information that is downloaded to any removable media or portable device

E. Using Removable Media Devices

PHI should be stored on removable media only when required in the performance of assigned duties or when responding to legitimate requests for information. When

Protected and Confidential information is stored on removable media, it must be encrypted in accordance with **Virtru's** Encryption Standards.

The workforce member shall take all reasonable and prudent measures to physically secure all removable media or to portable devices. Users shall not open or attempt to open the encasement of any removable media or portable devices nor otherwise circumvent any lock system that secures the device or its components. Users should take reasonable measures to secure device at all time and report any lost or stolen removable media or portable devices immediately.

Workforce members may not copy information or other sensitive data onto personal devices, unless approved by management in conjunction with the *Confidentiality Agreement for Employees*.

F. Exceptions

Exceptions to this policy may be requested on a case-by-case basis by petition to the ISO.

G. Refusal

Virtru reserves the right to refuse the ability to connect removable media devices to the Company network if such media is being used in such a way that puts **Virtru's** systems, data, users and customers at risk.

H. Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to technology resources or termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in action up to and including termination of their contract or assignment with **Virtru**.

XXIX. Application Recovery Plan

A. Overview

Virtru backs up of all production data hourly and stores it remotely on two separate Amazon Web Server (AWS) Accounts. These backups are a combination of both differential and full backups. These backups are durable a the same rate as S3 data, each snapshot is 99.99999% durable.

B. Scope

These policies apply to all production servers and data that **Virtru** is responsible for maintaining on behalf of our clients.

C. Data durability and reliability

Virtru uses Amazon S3 to provide a highly durable storage infrastructure designed for mission-critical and primary data storage. Amazon S3 redundantly stores data in multiple facilities and on multiple devices within each facility. To increase durability, Amazon S3 synchronously stores **Virtru's** data across multiple facilities before confirming that the data has been successfully stored. In addition, Amazon S3 calculates checksums on all network traffic to detect corruption of data packets when storing or retrieving data. Amazon S3 performs regular, systematic data integrity checks and is automatically self-healing.

D. Encryption

Virtru uses Server-side encryption to protect data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption by encrypting each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses 256-bit Advanced Encryption Standard (AES-256) to encrypt **Virtru's** data.

E. Load balancing

Virtru uses Amazon Web Services' Elastic Load Balancing (ELB) to automatically distribute incoming application traffic, to automatically route traffic across multiple instances. and multiple Availability Zones. This is used to insure that only healthy servers are receiving traffic.

F. Restoration of data

Restoration of production data is done on an as-needed basis. The following employees are responsible for restoration of the application if it is needed:

1. Reuven Gonzales, Lead Developer, or
2. Conor Gilsenan, Developer Ops.

The needed backup data will not be restored "on top of" the current "bad" data. The restores will be redirected to a new location, and first verified. Upon verification, the "bad" data will be removed from the drive, and stored and relabeled as "old data." Then the backup data will replace the "old data" on the drive. Once the restored data has been verified once more, the "old data" will be destroyed.

G. Testing and revision of plan

Once every quarter, after doing a full backup, **Virtru** will recover the saved data. During hours when the business is closed, we will operate the application using this recovered data in a test mode. The tests will consist of a set of tasks that are designed to exercise the main system functions to confirm that the data is usable and as up-to-date as we expected given the backups that were used to do the recovery. This testing process

should take an hour. The restore process should take an hour or two, once the files are retrieved.

If the process does not work as documented in our policy, it will be updated to reflect the actual procedure we need to implement to achieve successful recovery and operation.

Whenever we make changes to software or hardware, we will create/update and test using our *Inventory of Devices/Software Assets* and store this checklist in the **Security Documentation Library**.

XXX. Network Attached Storage and Workstation Backup Plan

A. Overview

Virtru recognizes that the backup and maintenance of data in the Network Attached Storage (NAS) and individual workstations are critical to operations. It is essential that certain basic standard practices be followed to ensure that data files are backed up on a regular basis.

B. Policy

Virtru will be using a Synology DS1515+ Network Attached Storage for backing up all workstations, firewall logs, and video surveillance footage. This data will also be backed up to a Amazon Web Services Glacier account.

C. Backup software

Virtru uses Cloud Station software to perform all backups. This will be installed on all workstations and must not be disabled by the user for more than one (1) business day. The software will maintain one month of file versions for restoring purposes

D. Remote backups

Virtru will provide a Virtual Private Network (VPN) for employees to login to for backing up their devices. Credentials for the VPM will be provided to remote employees, and they will be expected to configure their devices properly. If they are unsure, or have issue in setup, the IT department will be available for configuration assistance.

E. Local backups

Virtru encourages all users to do daily local backups of their data. These backups are to be encrypted using the encryption standards listed below. Any local backups must be surrendered at the time an employee no longer is employed by **Virtru**.

F. Encryption of backups

The backups of data will be encrypted on the NAS using AES 256 bit encryption. Any local backups that employees make must be encrypted at a minimum of 256 bit encryption.

G. Restoring data

In the event that a workstation fails, is stolen, or is damaged whether physically or by malware. It is the policy of **Virtru** that this device will be replaced within 24 hours. The IT department will be responsible for reprovisioning this device, and testing that the workstation is functioning properly before giving the device to the employee.

H. Enforcement

Anyone found to have violated this policy may be subject to disciplinary action, up to and including suspension of access to technology resources or termination of employment. A violation of this policy by a temporary worker, contractor or vendor may result in action up to and including termination of their contract or assignment with **Virtru**.

XXXI. Information Integrity Management Policy

A. Overview

The other policies in this document contribute to the integrity of the data in our systems. Notably, the Data Backup Plan, the Access Control Policy, and the Malware Management Policy contribute to data integrity. In addition to these, we add the following policy elements.

B. Policy

Virtru will configure our applications software to use the available edits on data that is entered into our systems. These edits will check for internal data consistency, reasonableness of data, and logical relations among data items.

XXXII. Security Incident Management Policy

A. Overview

Virtru recognizes that, despite having reasonable security safeguards, we may have security incidents.

B. Procedures

To manage these incidents, **Virtru** will do the following:

Security Policies and Procedures

1. We will train each workforce member to recognize the common telltale signs of a security incident. When a member of the workforce detects one of these signs, he/she will be responsible for notifying the ISO.
2. The ISO will maintain a set of tests to detect events in the system logs that may indicate security incidents. These tests will be written into a script and run against the system log on a daily basis or whenever needed. The tests currently are:
   a) Account creation/deletion
   b) High volume of unsuccessful logon attempts
   c) Alerts from our malware monitoring systems
   d) High volume of file or database access/creation/deletion activity for the time of day, or for day of the week
   e) Account activity at unusual times of the day or night
   f) Absence of expected log records of activity when expected
   g) Unusual level of record access for a given account
   h) Daily logs will be tested by the firewall in real time,
   i) User data will be reviewed weekly
   j) Logs for the past month will be retained. When anomalies are discovered, the script will provide a report that is immediately brought to the attention of the ISO or designee as a potential security incident.
   k) Account lock out due to excessive password retry failure.

The ISO will determine, in consultation with others if needed, whether an event is a security incident.

If an event is a security incident, the ISO (or designee) will proceed to contain and repair damage from the incident by working with staff, vendors, and Business Associates as needed. The security incident will be tracked in JIRA and treated as an application defect. A log of relevant actions taken to contain and repair the damage will be stored in JIRA. The permanent home of this log will be in the **Security Documentation Library**. The ISO will determine if the event involves a workforce member action that is covered under the sanction policy and will follow that policy. The ISO will determine if the event represents a security incident for which a Business Associate is responsible. If so, the ISO will follow our *Incident and Breach Policy* in this area.

C. Policy

If an event is a security incident, the ISO (or designee) will proceed to contain and repair damage from the incident by working with staff, vendors, and Business Associate relations in order to further deter future incidents of the same type.

XXXIII. Security Plan Review Policy

A. Overview

We recognize that our underlying security risk will change and our ability to manage this risk will improve over time. To ensure that we adjust our policies and procedures to take these two factors into account, we will review our Security Policies and Procedures annually. The ISO will lead this review and involve others as needed. Documentation of the review will be contained in a document called *Annual Security Review* and restored in the **Security Documentation Library** {or **Notebook**}.

B. Procedures

At a minimum, the review process will consist of:

1. Evaluating changes in the last year that may affect our Security Policy. These will include changes in:
    a) Number, sizes or locations of our business sites
    b) Our workforce size and composition
    c) Hardware/software
    d) State or federal laws that apply to us
    e) Type of medical insurance that we provide
2. Reading each Policy to determine whether or not the changes may affect it and/or the practices driven by the Policy. We will make a list of changes that need to be made, then write a paragraph describing how.
3. Creating a list of changes in Policies and/or Procedures that our **Company** will carry out.
4. Developing and implementing any changes in our Policies and Procedures on a timely basis.

Security Policies and Procedures

Appendices

Security Policies and Procedures

A. Change Logs

The Change Logs are logs and reports that are reviewed, at a minimum, twice a year. It provides information on programs available and which employees have access to which programs. The actual logs are found in the **Change Control Logs for Security** section of the documents.

1. Annual Security Review
2. Application/Database Change
3. Employee Access
4. Incident - Disaster
5. Maintenance
6. Media Sanitization
7. Operating System Changes Audit
8. Organizational Chart/Electronic Asset Management
9. Network Change
10. Physical Entry Access
11. Responsibility Change

B. Information Security Committee

Information Security Officer:
Will Ackerly
willackerly@virtru.com
(202) 577-3683

Information Security Committee:
Jordan Duggan
Jordan@virtru.com
(919) 696-7936

Reuven Gonzales, Director of Operations
Cell: (949) 878-6154
reuven@virtru.com

Conor Gilsenan, Operations Developer
Cell: 973-986-6650
conor@virtru.com

Disaster Recovery Plan for Virtru

We define a disaster as any event that affects our information systems and, as a result, substantially interferes with the operations of our business. Examples are fire, flood, hardware failure of critical elements (servers), software failures, theft, chemical/radiation hazard, and sabotage. Our definition of recovering from a disaster is taking all the actions needed to restore the systems to their normal operational state. Our plan to recover from disasters is described below.

1. What we will do to prepare to perform a disaster recovery:

    A. We will train the workforce to recognize and report a disaster.

    B. We will organize the workforce responsibilities so that during a recovery we are not dependent on only one person for any critical step.

    C. We will report disasters to the ISO and AISO. The ISO will make the formal determination as to whether or not to classify the event as a disaster.

    D. We will store paper backup copies of key disaster related documents with the offsite backups. These documents will include a List of Support Contacts – vendor, reseller, and/or support group contact information for all of our software and hardware.

    E. We will keep an *Inventory of Device/Software Assets* for [Name of Business]-- a detailed checklist for each asset, such as the server, PCs, the router, network switch, databases, and software programs containing tasks that must be completed to recover that asset. The list will include key data about the device including a party responsible for the recovery whose role is to diagnose and, if needed, repair, replace, and/or rebuild a device.

    F. We will have current copies of system data and software available at the off site location, as our data backup plan specifies.

2. Once the ISO (or designee) has certified a disaster, we will:

   A. Use the ISO or designee to facilitate the recovery. The facilitator will direct the recovery process, coordination and communication of the actions of the various parties that are involved in the recovery.
   B. Determine which devices/software (e.g. servers, PCs, power units, AC units) are not functioning normally, conferring with the appropriate staff, vendors, and other support personnel to make this determination. When in doubt about the status of the device, we will either use a test that is described in the IT Assets Recovery Checklist for the device/system or depend on the recovery responsible party to make this determination.
   C. Review the *Inventory of Device/Software Assets* for the devices to be recovered. Each checklist will have as an initial task, "Contact the appropriate parties responsible for restoring the devices/software to be recovered." Guidance and other recovery activities from these parties are key contributors to the recovery process.
   D. After all of the non-functioning assets have been restored, follow the instructions in the part of the Emergency Operations Plan that deals with what to do when the system is available again.

Organization

Emergency Planning & Crisis Management Team (**EPCMT**):

- Will Ackerly, CTO & ISO
- Jordan Duggan, VP of Product & Development & AISO
- Reuven Gonzales, Director of Operations
- Conor Gilsenan, Operations Developer
- Zack Nelson, Director of Development

Primary Disaster coordination handled through:

Crisis Manager 1:

Reuven Gonzales, Director of Operations
Cell: (949) 878-6154
reuven@virtru.com

Crisis Manager 2:

Conor Gilsenan, Operations Developer
Cell: 973-986-6650
conor@virtru.com

Other Members' Contact Information

- Zack Nelson 443-834-3791
- Payam Abedi 703-656-6227
- Tyler Biscoe 301-642-8844
- Jon Gilpen 303-358-6689
- Jason Ghent 803-658-6645

Off-Site Meeting Location

Used if team needs to meet to formulate an action plan.

If primary location is not accessible, we may need to operate from an off-site locations such as:

Employees' Home Offices
Jack Rose Restaurant

Extended off-site locations will be determined after assessing the severity of the disaster.

Disaster Recovery Timeframes

Maximum Tolerable Downtime (MTD)

The total amount of time our company is willing to accept for an outage or disruption, including all impact considerations. This guides our Crisis Management Team in determining the selection of an appropriate recovery method, and the depth of detail which will be required when developing recovery procedures, including their scope and content.

Recovery Point Objective (RPO)

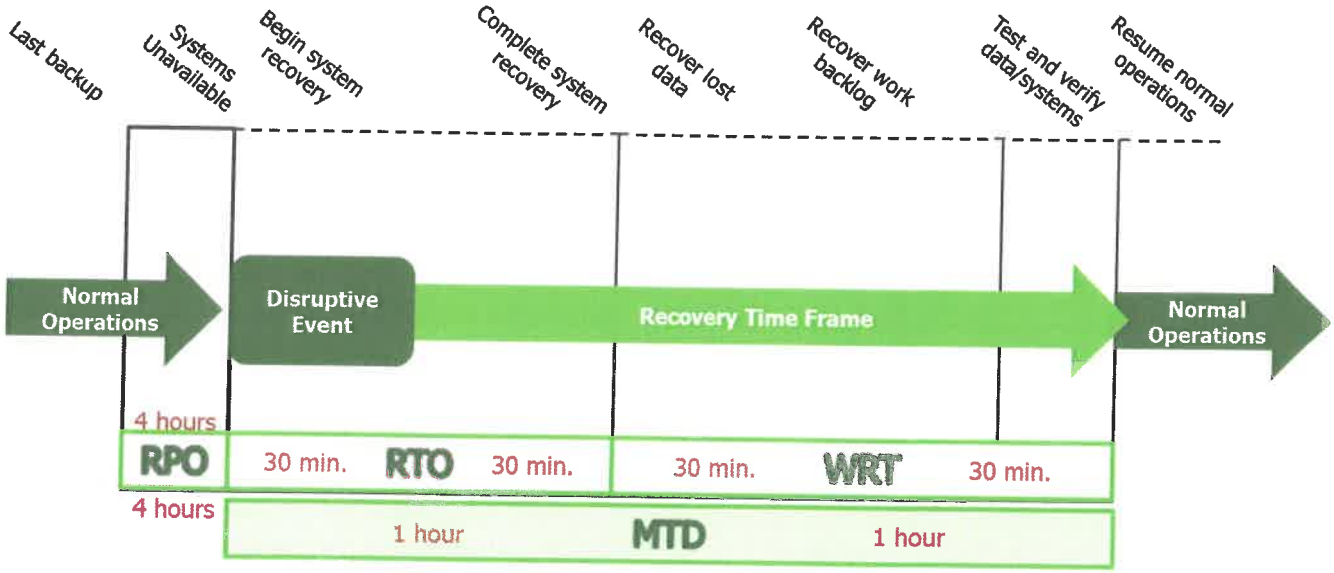
This is the point in time, prior to a disaster or disruptive event, which our company has accepted for data loss. RPO determines the frequency of our data backups. When determining RPO, we need to consider how much newly entered data we can afford to lose. *Therefore, if RPO is set to 4 hours, then we must have offsite backups maintained every 4 hours.*

Recovery Time Objective (RTO)

RTO determines the target time for recommencement of business activity. The Crisis Management Team will determine what business functions (i.e. telecommunications, web servers, etc.) should be restored based on priority.

Working Recovery Time (WRT)

This is the time our company will spend recovering lost data and work backlog, and testing and verifying data and systems. WRT usually is the difference between MTD and RTO.



Physical Security Example Times
Minor Disaster and Major Disaster

(See next page)

Disaster Timeframe Expectations

Internal Network
The server and network must be functioning in order for any of our other information systems to function. We could afford to be without the server/network for ten (10) minutes without materially affecting our business. If the server/network is down for longer than ten (10) minutes, staff will switch over the mobile tethering, or will go to an approved location to continue their work.

Production Servers
Production servers must be functioning at all times in order for our applications to work. We cannot afford to be without the production servers without materially affecting our business. Traffic will be automatically routed to another server via Amazon Web Services' Elastic Load Balancing.

Workstations
If a workstation crashes, we can easily use another one with only modest inconvenience. Ideally, we would like to replace/restore a workstation within 72 hours.

Printer and Fax
We have two multifunction printers. We can lose all printers for up to a week with little effect on data flow.

Email and Web Browser
Currently, we can function for no more than 10 minutes without email or web browsing. We will tether devices via smartphones after that time.

Wireless Network
We have a wireless network and the office depends on it for routine transactions. A backup router is available; it is preconfigured and encrypted using WPA2-AES.

IT Resources
We depend on the availability of certain employees and our IT service provider to diagnose and fix problems quickly. A chain of contacts is available in this document.

Power and HVAC Equipment
We depend on external power and environmental equipment (especially our AC unit) to maintain the power and environmental support for our system. Failure of either of these systems could inhibit the use of our IT systems, and could also stop us from doing business. These failures are not IT-specific risks. We are comfortable enough with the track record of these services not to need more than a short term UPS to allow us to smoothly shut the network down in the event of a sustained power outage. We have to yearly revisit the question of whether or not we need

more power/environmental backup to ensure that the satellite site will able to operate even if power/cooling at the main site is out.

Disaster Timeframes Table

{This is a sample. Please fill in according to Virtru's standards. Functions can include departments, as listed below, or they can include more specific tasks, such as invoicing.}

	Minor Disaster				Major Disaster			
Function	**MTD**	**RTO**	**WRT**	**RPO**	**MTD**	**RTO**	**WRT**	**RPO**
Physical Security (office/suite)	1 hour	30 minutes	30 minutes	4 hours	1 hour	30 minutes	30 minutes	4 hours
IT (server, hardware, equipment)								
Sales and Marketing								
Administration								
HR								

EVACUATION PLAN - during business hours:

For a disaster where you will need to **leave the building:**

If a disaster happens during normal business hours all Company employees will meet at **Jack Rose Restaurant, 2007 18th St NW, Washington, DC 20009.**

This will prevent Company employees from being in the way of emergency crews. A head count by managers will determine if all staff members have fully exited the building.

Headcount numbers will be brought to the ISO or CEO.

If the disaster happens after the meeting location has closed, employees will wait outside of the same address.

For a disaster where you will need to **stay in the building:**

If a disaster happens during normal business hours, all Company employees will meet in the **Basement**. A head count will determine if all staff members have fully exited the suite. See above for head count procedures.

{Please fill in the appropriate personnel for the following responsibilities}

Office/Evacuation Managers	Assembly Managers
Will Ackerly	John Ackerly
John Ackerly as Backup	Will Ackerly as Backup
System Shutdown Manager	**Back-up System Shutdown Manager**
Jordan Duggan	Jordan Duggan
Will Ackerly as Backup	Will Ackerly as Backup

Critical Operation Priority List

If or when a disaster happens, certain contacts will need to be made.

Operation	Employee in Charge	Action Plan
Current enrollment processes (any pending business)	Will Ackerly	Notify carriers of current situation—give cell number if needed.
Communications	Will Ackerly	eBlast to client list
IT—phones, faxes, e-mail	John Ackerly	Set up remote office
Payroll-Banking issues-Commissions	John Ackerly	Notify payroll/banking institutions of disaster and action plan

Potential Purchase List

If or when a disaster happens, certain items may need to be replaced:

1. 3 UPS (Uninterruptible Power Supply)(s)(Batteries)
2. Network Attached Storage (NAS)
3. Network Switch(s)
4. Network cable(s)
5. Power cable(s)
6. Power strip(s)
7. Monitor(s) / Monitor Cable(s)
8. Keyboard(s) / Mouse(s)
9. Firewall
10. Workstation(s) / Laptop(s)
11. Phone(s) & Headsets
12. Security Camera
13. Electronic Door Lock
14. Video Conference Microphones
15. Minifridge
16. Projector
17. Software
    a. OSX
    b. Windows
    c. Acrobat
    d. Office Suite
18. Paper
    a. Printer paper
    b. Sticky notes
    c. New Checks
19. Multifunction Color Printer
20. Office Furniture/Equipment
21. Carrier (Marketing) Supplies
22. Office Supplies

Fire Plan

EVACUATION PLAN - FIRE!

If the fire alarm goes off during business hours, **evacuate the building immediately**. If you discover a fire or smell heavy smoke inside building: **DO NOT ATTEMPT TO FIGHT THE FIRE!!**

1. Pull fire alarm, evacuate the building and call 911 on the way out of the building

2. Perform head count at the designated assembly point

    - If anyone is missing, call their emergency contacts to determine if the missing individual has made contact with them. If they have not, alert the authorities.

3. Action Plan - developed by ***EPCMT***

    - Re-open based on damage
    - If the office must remain closed:
        - Notify employees and/or employees emergency contacts.
        - If there is any impact to customer operations, email all clients with a status update and recovery plan.

NOTE: First Aid kit located in the drawer of the white cabinet located to the right of the spiral staircase.

Earthquake Plan

EVACUATION PLAN - Earthquake!

During an Earthquake

- **DO NOT USE THE ELEVATOR DURING AN EMERGENCY EVACUATION.**
- If you're indoors, stay there. Get under -- and hold onto --a desk or table, or stand against an interior wall. Stay clear of exterior walls, glass, heavy furniture, fireplaces and appliances. The kitchen is a particularly dangerous spot. If you're in an office building, stay away from windows and outside walls and do not use the elevator.
- If you're outside, get into the open. Stay clear of buildings, power lines or anything else that could fall on you.

After an Earthquake

- Perform head count at the designated assembly point
  - If anyone is missing, call their emergency contacts to determine if the missing individual has made contact with them. If they have not, alert the authorities.
- Shut down systems, if time permits, see **Emergency Shutdown Procedures**
  - Check for fire or fire hazards. If you smell gas, shut off the main gas valve. If there's evidence of damage to electrical wiring, shut off the power at the control box.
  - If the phone is working, only use it in case of emergency. Likewise, avoid driving if possible to keep the streets clear for emergency vehicles.

- Be aware that items may fall out of cupboards or closets when the door is opened, and also that chimneys can be weakened and fall with a touch. Check for cracks and damage to the roof and foundation of your home.
- Listen to the radio for important information and instructions. Remember that aftershocks, sometimes large enough to cause damage in their own right, generally follow large quakes.
- If you leave home, leave a message telling friends and family your location.

- Action Plan - developed by ***EPCMT***
  - Re-open based on damage
  - If the office must remain closed:
    - Notify employees and/or employees emergency contacts.
    - If there is any impact to customer operations, email all clients with a status update and recovery plan.

NOTE: First Aid kit located in the drawer of the white cabinet located to the right of the spiral staircase.

Tornado Plan

EVACUATION PLAN - Tornado!

If the city or county signal a tornado warning, move away from the perimeter of the building and any exterior glass.

DO NOT USE ANY ELEVATORS DURING AN EMERGENCY EVACUATION.

1. Move to the basement of the office suite.
2. Shutdown systems, if time permits, see **Emergency Shutdown Procedures**
3. Perform head count at the designated assembly point
    - If anyone is missing, call their emergency contacts to determine if the missing individual has made contact with them. If they have not, alert the authorities.
4. Action Plan - developed by ***EPCMT***
    - Re-open based on damage
    - If the office must remain closed:
        - Notify employees and/or employees emergency contacts.
        - If there is any impact to customer operations, email all clients with a status update and recovery plan.

NOTE: First Aid kit located in the drawer of the white cabinet located to the right of the spiral staircase.

Flood Plan

EVACUATION PLAN - Flood!

1. Evaluate the situation
    - Shutdown systems routine, see **Emergency Shutdown Procedures**
    - Perform head count
        - If anyone is missing, call their emergency contacts to determine if the missing individual has made contact with them. If they have not, alert the authorities.
2. Action Plan - developed by ***EPCMT***
    - Remain open - *based on damage or location*
        - Relocate staff within suite
        - Evaluate IT requirements
    - Close - send staff home
        - Re-open based on damage
        - If the office must remain closed:
            - Notify employees and/or employees emergency contacts.
            - If there is any impact to customer operations, email all clients with a status update and recovery plan.

After Hours Plan

EVACUATION PLAN - after business hours

If the building is in a disastrous state after working hours, the **EPCMT** will notify employees. *See **Virtru** Phone Tree.*

If **re-opening** on a workday at the primary location:

1. Verify location is safe for operations - including systems
2. Communications
    a. Emergency Contact List
    b. Client Blast

If **NOT re-opening** on the following workday at the primary location:

1. The **EPCMT** must decide estimated length of time we will not be able to function
    a. If less than or equal to one day, office is closed.
        i. **[Name of Business]** will open the following work day
        ii. Verify location is safe for operations
        iii. Communications
            1. Emergency Contact List
            2. Client Blast

2. If office needs to move to secondary location or close for a **short** period of time.
    a. The **EPCMT** meets to develop a plan of action
    b. Determine the validity of systems
        i. If valid, move critical systems to secondary location
        ii. If not valid, retrieve necessary items and contact suppliers for new systems
            1. Restore systems from backups
            2. Restore connectivity
                a. Skeleton crew of selected staff members (possibly several from each department)

c. Communications

i. Emergency Contact List

ii. Client Blast

3. If office needs to move to secondary location or close for a **longer** period of time:

a. The **EPCMT** meets to develop a plan of action

b. Determine the validity of Systems

i. If valid, move critical systems to secondary location

ii. If not valid, retrieve necessary items and contact suppliers for new systems

1. Restore systems from backups
2. Restore connectivity

ii. Determine staff needs - full or partial capacity

iii. Communications

1. Emergency Contact List
2. Client Blast

Emergency Contact List

Emergency services—call 911	
Police	**000-000-0000**
Fire	**000-000-0000**
Poison Center	**800-222-1222**
Building	
Building Owner	**000-000-0000**
Alarm Company	**000-000-0000**
Cleaning Company	**000-000-0000**

Technical Issues	
Technologies Company	**000-000-0000**
Website-Programmer	**000-000-0000**
Miscellaneous Internal Operations/Vendors	
Staffing Companies	**000-000-0000**
UPS	**000-000-0000**
Bank	**000-000-0000**
401K Company	**000-000-0000**
Payroll Company	**000-000-0000**

Emergency Shutdown Procedures

If an electrocution occurs while working in server room, staff will pull all of the UPS cords from the outlet by the interior door. If that outlet is inaccessible due to fire or victim's position, staff will shut off the power at the breaker, located in the basement on the wall to the left of the TV.

If there is a fire within the building or suite, staff should concentrate on notifying authorities.

If there is severe flooding that threatens to affect the server room, staff will shutdown and unplug all equipment and move it to the second story platform of the suite.

BRIGHTLINE

CERTIFICATE OF REGISTRATION

Information Security Management System - ISO/IEC 27001:2013

The Certification Body of BrightLine hereby certifies that the following organization operates an Information Security Management System that conforms to the requirements of ISO/IEC 27001:2013

ServiceNow, Inc.

for the following scope of registration

The scope of the ISO/IEC 27001:2013 certification is limited to the information security management system (ISMS), which supports ServiceNow as a provider of cloud-based solutions that define, structure, manage and automate services across the global enterprise, as well as all supporting resources including global data center operations and infrastructure, applications, end-user services, and product development, and in accordance with the Statement of Applicability, approved July 28, 2015. Assets within scope of the ISMS include: internal information assets, customer data, software, hardware, people, and physical assets to host, support and operate the cloud-based solutions. The data centers in the following locations house the infrastructure used to deliver the cloud-based solutions: Virginia, California, Florida, Washington, Montreal, Toronto, London, Amsterdam, Geneva, Zurich, Sydney, Brisbane, Singapore, Hong Kong, São Paulo and Campinas. Additionally, ServiceNow uses Amazon Web Services (AWS) to host some ServiceWatch customers. Excluded from the scope are all operations of third party data centers and AWS.

the scope of this certification includes the following locations:

Santa Clara (HQ): 3260 Jay Street, Santa Clara, California, 95054, United States
San Diego: 4810 Eastgate Mall, San Diego, California, 92121, United States
Kirkland: 4400 Carillon Point, Kirkland, Washington, 98033, United States
Orlando: 3501 Quadrangle Blvd, Suite 150, Orlando, FL 32817, United States
Amsterdam (EMEA HQ): Hoekenrode 3, 1102 BR Amsterdam, The Netherlands
London: 3rd Floor, Future House, The Glanty, Egham, Surrey, TW20 9AH, United Kingdom
Sydney: Level 21, 50 Bridge St, Sydney, New South Wales, 2000, Australia

Certificate Number: **1980700-4**

ISO 27001 CERTIFIED BY BRIGHTLINE

ANAB ACCREDITED

Authorized by:

Christopher L. Schellman
President, BrightLine
1300 N. West Shore Blvd, Suite 240
Tampa, Florida 33607, United States
www.BrightLine.com

Issue Date	Original Registration Date	Expiration Date	Certificate Version
September 29, 2015	December 17, 2012	September 28, 2018	Version 4

CONDITIONS & LIMITATIONS:

1. The aforementioned organization has a perpetual responsibility to maintain compliance with ISO 27001:2013 during the period of certification.
2. This certificate is subject to the satisfactory completion of annual surveillance audits by BrightLine.
3. ISO 27001:2013 compliance audits are not designed to detect or prevent criminal activity or other acts that may result in an information security breach. As such, this certification should not be construed as a guarantee or assurance that an organization is unsusceptible to information security breaches.
4. The information in this document is provided "AS IS", without warranties of any kind. BrightLine expressly disclaims any representations and warranties, including, without limitation, the implied warranties of merchantability and fitness for a particular purpose.
5. This certificate is the property of BrightLine and is bound by the conditions of contract. The authenticity of this certificate can be validated at www.BrightLine.com/Certificate-Directory.

vCLOUD GOVERNMENT SERVICE



Compliant cloud solutions built for government agencies

Whether spurred by the need to increase efficiency, meet government mandates or deal with rapidly expanding data sets and workloads, more and more agencies are moving some or all of their applications or infrastructure to the cloud. However, for many agencies, the most cost-effective, secure and efficient solution is a hybrid cloud model that allows them to not only leverage their existing investments in IT infrastructure, but also extend their systems seamlessly to the technology platform that best meets their needs.

VMware®, the global leader in virtualization and cloud infrastructure, and QTS, a trusted cloud operator and leading provider of hybrid cloud services and managed hosting for government agencies and enterprises, have partnered to deliver VMware vCloud® Government Service provided by Carpathia™ (A QTS Company).

vCloud Government Service is an enterprise-class hybrid cloud service designed to run new and existing applications in exactly the same way, giving government organizations application and data mobility. Being able to use existing people, processes, tools, and automation enables government organizations to focus on the benefits of the cloud to their mission, rather than taking time and resources to re-architect for new infrastructure. Federal organizations can securely extend their data centers to the cloud quickly and confidently, using an integrated cloud infrastructure with the security of a JAB-based FedRAMP Provisional Authorization.

KEY FEATURES

Robust Security and Compliance

- vCloud Government Service is a secure cloud platform that enables customers to maintain security and data protection that meets a broad range of regulations, standards, and best practices including FedRAMP, International Traffic Arms Regulations (ITAR), FIPS 140-2, and AT 101 SOC Type 2.

Efficiency and Manageability

- Agencies can write, deploy, and manage applications in the cloud in the same way they do today, without making any changes or additional investments. With management tools consistent across on premises and cloud environments, you can accelerate application deployments, streamline the deployment and update process, leverage pre-built components, and reuse application models across environments, and clouds.

Seamless Network Integration

- vCloud Government Service is built on a seamless virtualized network that is quickly customizable to support your application and security needs. Network virtualization allows you to configure your firewalls and network as if they were in your own data center so that you can replicate the network your applications need to operate. Get common identity and access management across your onsite and offsite cloud locations.

BENEFITS

- Ease of Use – Leverage your existing investments in applications and infrastructure and avoid the complexity of re-architecting for public cloud infrastructure
- Secure and Compliant – Secure cloud platform, with security controls designed to meet the unique requirements of government customers, most notably the FedRAMP standards
- Hybrid – True hybrid cloud solution enables both onsite and offsite IT environments to run new and existing applications seamlessly
- Fastest Path to Cloud Value – Use a common platform to leverage internal and external cloud resources without having to retrain your staff, and lower overall costs

Why vCloud Government Service?

vCloud Government Service has a FedRAMP Provisional Authority to Operate (P-ATO) and is generally available to U.S. government and defense organizations. It can be used for a variety of applications and workloads including:

- Test and development
- Packaged application hosting
- Backup and Disaster Recovery
- Web hosting and customer service
- On-demand data center expansion

Trusted Cloud Services

QTS is redefining the industry with trusted cloud services that leverage innovation to improve the flexibility, scalability, and cost-effectiveness of cloud services.

- We are a trusted cloud operator with past performance serving the government market -- including DoD, Civilian and Intelligence agencies -- across multiple programs and applications
- QTS data centers deliver the highest levels of security and compliance, and meet many compliance standards including FISMA, DIACAP, PCI, and HIPAA
- We hold a number of certifications and accreditations across multiple federal agencies and programs and support over 50 Federal systems holding active Authorizations to Operate (ATO)

Security

vCloud Government Service operates with a FedRAMP Provisional Authorization to Operate (P-ATO) issued by the Joint Authorization Board (JAB). Built with a defense in-depth strategy that puts our customers' critical applications and data in the innermost ring, our people, processes and procedures ensure 100 percent compliance at implementation and through the lifecycle of the project.

Hybrid Options

vCloud Government Service is a true enterprise-class hybrid cloud service, offering a seamless platform for migrating and managing workloads between dedicated virtualized environments, on-premise infrastructures, third-party data centers and the cloud.

ABOUT QTS

QTS Realty Trust, Inc. (NYSE: QTS) is a leading provider of secure, compliant data center solutions and fully managed services, and the owner of Carpathia Hosting, a leading provider of hybrid cloud services and managed hosting. QTS' integrated technology service platform of custom data center (C1), colocation (C2) and cloud and managed services (C3) provides flexible, scalable, secure IT solutions for web and IT applications. QTS' Critical Facilities Management (CFM) provides increased efficiency and greater performance for data center owners and operators. QTS owns, operates or manages 25 data centers and bsupports more than 1,000 customers in North America, Europe and Asia Pacific.

March 10, 2016

State of Utah Division of Purchasing
3150 State Office Building
Capitol Hill
Salt Lake City, Utah 84114

Mr. Hughes:

As a privately owned company, Carahsoft Technology Corp. does not report to D&B. As such, the information in D&B is incorrect. To support you to determine that we have the financial resource to perform the contract we provide you the following information.

We are a stable, conservative and profitable company. Carahsoft continues to grow as noted by our year over year revenue below:

2010 $820 Million
2011 $1.12 Billion
2012 $1.46 Billion
2013 $1.81 Billion
2014 $2.45 Billion
2015 $3 Billion

We currently employ close to 500 employees.

To support you to determine that we have the financial resource to perform the contract we provide you the following information:

We maintain a $25M line of credit available (currently 100% available) with Xenith Bank. I have included a recent banking clarification letter from Xenith.

Mr. Joe Humphries is the Regional President and can be reached at 703-869-3610 if you need any information from him.

We have received numerous accolades including:

- For the 6th consecutive year CRN's 2012 Fast Growth List
- Washington Business Journal's 2012 List of Largest Government Contractors in Metro DC
- Third consecutive year Washington SmartCEO magazine's 2012 Future 50 list which recognizes the metro areas fastest growing companies.

Should you require additional details please call me and I can discuss our confidential financial information with you or provide you trade references that can further assist you.

Sincerely,

Jillian Dewey Szczepanek
Controller

dun & bradstreet

Carahsoft Technology Corp. DUNS: 08-836-5767

Credit Information

Risk Summary

Risk of Late Payment



Risk of late payment is based on the following prioritized factors in addition to other information in D&B's files:

- Proportion of slow payments in recent months
- Higher risk industry based on delinquency rates for this industry
- Increase in proportion of delinquent payments in recent payment experiences
- Proportion of past due balances to total amount owing
- Evidence of open liens

Indications of slowness can be the result of disputes over merchandise, skipped invoices, etc.

Payment Performance Trend



The payment performance trend for this company is Increased . Payment Trend currently is Increased compared to payments three months ago. The most recent payment information in D&B's files is:

- Payments currently: 11 days beyond terms
- Payments 3 months ago: 19 DAYS BEYOND terms
- Industry average: 5 DAYS BEYOND terms

*Note: Payments to suppliers are averaged weighted by dollar amounts.

Credit Limit Recommendation

Recommendation Date: 11/18/2015

Risk Category
High

Conservative Credit Limit
$0

Aggressive Credit Limit
$0



Company Profile

Chief Executive:
DIRECTOR(S): THE OFFICER(S)

Type of Business: NA

Years in Business: NA

Annual Sales:

Line of Business:
Whol computers/peripherals

1000000000	
Employees Total:	500

Legal Filings and Other Important Information

Bankruptcies:	None	**Negative Payment Experience:**	None
Judgements:	0	**Negative Payment Experience Amount:**	None
Liens:	3		
Suits:	None	**Payments Placed for Collection:**	0
Suits/Judgments/Liens Amounts:	None		

The public record items reported may have been paid, terminated, vacated or released prior to the date this data is transmitted. Accounts are sometimes placed for collection even though the existence or amount of the debt is disputed.

Special Events

We currently do have any information to be displayed for this business.

This report is prepared and provided under contract for the exclusive use of

This report may not be reproduced in whole or in part by any means of reproduction.

Payment Trends

Summary

Address:
1860 Michael Faraday Dr, Suite 100
Reston, VA 20190

Primary Industry SIC:
5045

D-U-N-S Number:
08-836-5767

Description:
Whol computers/peripherals

This is a single location.

Payment Activity

Total payment Experiences in D&Bs File:	48
Payments Within Terms: (not dollar weighted)	72%
Total Placed For Collection:	NA
Average Highest Credit:	$2,379,615
Largest High Credit:	$20,000,000
Highest Now Owing:	$20,000,000
Highest Past Due:	$4,000,000

Indications of slowness can be the result of dispute over merchandise, skipped invoices, etc. Accounts are sometimes placed for collection even though the existence or amount of the debt is disputed.

PAYDEX®®

3 Month PAYDEX®

75

When weighted by dollar amount, payments to suppliers average 8 days beyond terms terms.



Based on payments collected over the last 3 months

24 Month PAYDEX®

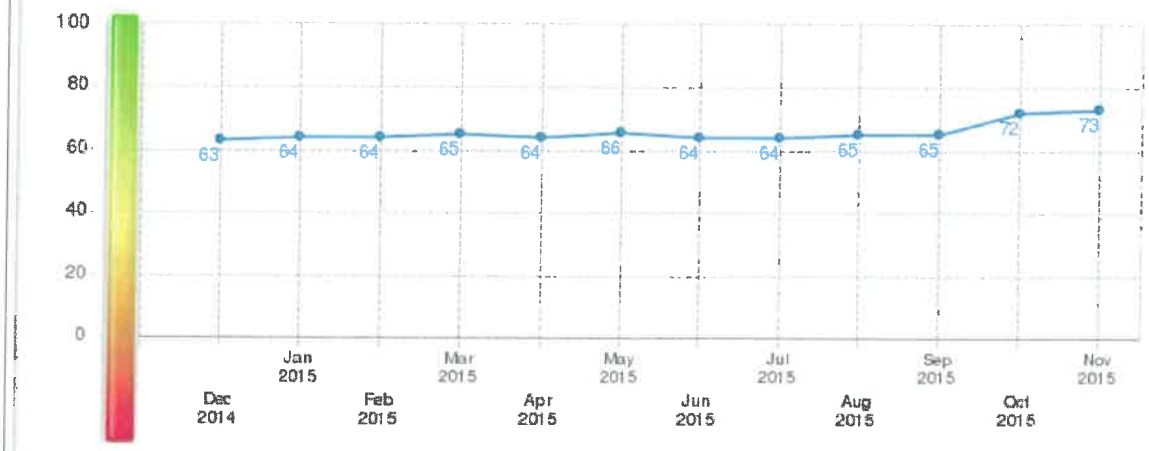
73 ▲

When weighted by dollar amount, payments to suppliers average 11 days beyond terms terms.



Based on payments collected over the last 24 months

PAYDEX ® Trends - This Company, 12 Months

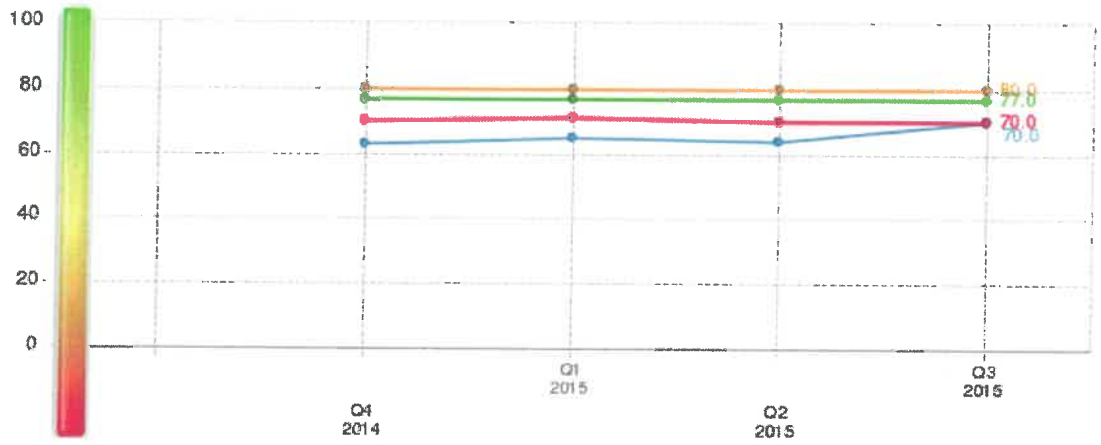


This Company (73)

Based on payments collected over the last 12 months.

- Current PAYDEX® for this Business is 73 , or equal to 11 days beyond terms terms
- The 12-month high is 73 , or equal to 11 DAYS BEYOND terms
- The 12-month low is 63 , or equal to 11 DAYS BEYOND terms

PAYDEX ® Score Comparison - This Company to Primary Industry Comparison, 4 Quarters



- My Company (73)
- Industry Upper Quartile (80)
- Industry Median (77)
- Industry Median (70)

Based on payments collected over the last 4 quarters.

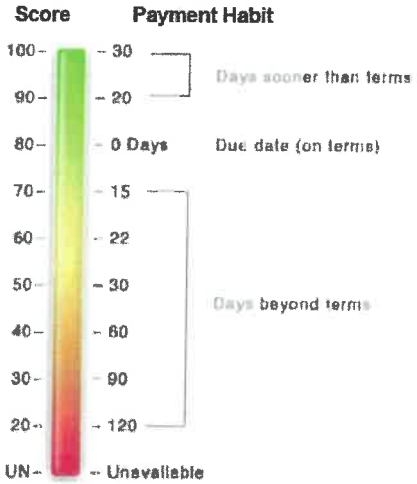
- Current PAYDEX® for this Business is 73 , or equal to 11 days beyond terms
- Current PAYDEX® for this Business is 77 , or equal to 5 DAYS BEYOND terms

- Industry upper quartile represents the performance of the payers in the 75th percentile
- Industry lower quartile represents the performance of the payers in the 25th percentile

Business Payment Habit by Amount of Credit Extended, 24 Months

$ Credit Extended	% of Payments Within Terms	# Payment Experiences	Total $ Dollar Amount
Over 100,000	73%	24	$90,200,000
50,000-100,000	100%	1	$85,000
15,000-49,999	27%	5	$110,000
5,000-14,999	73%	4	$27,500
1,000-4,999	100%	1	$2,500
under 1,000	100%	3	$400

How to Read the D&B PAYDEX ® Score



Risk Interpretation

	80 - 100	LOW risk of late payment (averages prompt to 30 days within terms)
	50 - 79	MEDIUM risk of late payment (averages 30 or less beyond terms)
	0 - 49	HIGH risk of late payment (averages 30 to 120 days beyond terms)

©Dun & Bradstreet, Inc. 2015. All rights reserved.

AODocs Terms of Service - Version published on the Web Site

TERMS OF SERVICE

These Terms of Service **("Terms")** are a legal agreement between Altirnao, Inc., herein **"Altirnao",** having an office and place of business at 221 Kearny Street, Suite 300, San Francisco, CA 94108, USA, and the person or entity agreeing to the terms herein **("Customer", "You" or "you").** By using or accessing any part of A0Docs (the **"Service"),** You agree that You have read, understand, and agree to be bound by all of the terms and conditions contained herein. If You do not agree to these Terms, You must not use or access the Service. If You are entering into this Terms on behalf of a company, You represent that You have the authority to bind that company to these Terms. If You have purchased a license to use A0Docs through an Altirnao reseller, You also agrees to comply with the terms of any agreement between You and such reseller. In the event of an inconsistency between these Terms and any such reseller agreements, these Terms shall control.

Description of Service

AODocs is an online document management solution for Google Apps. The Service is offered and provided subject to these Terms and solely for Your business purposes. You may connect to the Service using any Internet browser supported by the Service.

The Service requires one or more Google Apps for Business account that will be the owner(s) of all files stored and managed by the Service. The Service stores all the files that it stores and manages for You in the Google Drive account(s) that You will assign to AODocs when You deploy AODocs. You understand and acknowledge that You are solely responsible for obtaining the Internet access and all equipment necessary to use the Service, for appropriately configuring Your Google Apps account(s) and for allocating a sufficient number of accounts and sufficient Google Drive storage space to allow proper operation of the Service, as per the recommendation of Altirnao's technical support or product documentation. You also understand and agree that content you store through your use of the Service will be made available to Google as part of Google providing the Google Apps service. All fees associated with the foregoing shall be paid by You.

Modifications

To these Terms: Altirnao reserves the right to update and change the Terms of Service upon notice from time to time. You will be provided notice of any such modification by electronic mail or by the publishing of such on the website http://www.aodocs.com/terms-of-service. You may terminate your use of the Service if the Terms are modified in a manner that substantially affects your rights in connection with use of the Service. Your continued use of the Service after any such changes shall constitute your consent to such changes. You can review the most current version of the Terms of Service at any time at http://www.aodocs.com/terms-of-service.

To the Service: Altirnao may make changes to the Service from time to time. Altirnao will notify you of any material changes or modifications. Any updates, upgrades, additions or new features to the Service, including the release of new tools and resources, shall be subject to these Terms and may require you to agree to additional terms and conditions.

Use of the Service

Access to Service: Access to the Service is only available to the Customer and the end users **("Users")** to whom Customer has purchased individual user licenses and granted access. Upon registration with Altirnao, Customer will specify the email address of a Google Apps account (the **"Account"),** which will be granted access to the Service. Customer is solely responsible for granting the Service access to Customer's Google Apps files and revoking such access when Customer ceases use of the Service. Customer is responsible for maintaining the confidentiality of Customer's password. Customer agrees not to share its password with anyone other than Users, let anyone else access its password or do anything else that might jeopardize the security of its password. Customer agrees to notify Altirnao if Customer's password is lost, stolen or disclosed to an unauthorized third party, if there is any unauthorized use of its password or Account, or if Customer learns of any other breach of security in relation to the Service. Customer is solely responsible for any and all activities that occur through the use of Customer's Account.

License to Customer: Subject to Customer's compliance with these Terms and the Google Acceptable Use Policy (available at https ://cloud.google .com/terms/aup), including, without limitation, Customer's payment of all applicable fees, Altirnao hereby grants Customer a limited, revocable, non-transferable non-exclusive, non-sublicensable license to access and use the Service, solely for Customer's own internal use, and not for timesharing, application service provider or service bureau use.

Customer is at all times fully responsible and liable for all acts and omissions by Users to whom Customer has granted access to the Service and Customer agrees to indemnify Altirnao for all claims and losses related to any such acts and/or omissions.

Each user license ordered by Customer is specific to the email address of only one User and, once granted to that User, may not be transferred or reassigned to any other user unless the User originally granted the license will no longer use the Service. Any such transfer or reassignment is permanent and Licensee shall not permit the original User to use the Service after such User's license has been used by a different User.

Altirnao reserves the right to terminate unpaid Accounts and Accounts that are inactive for a continuous period of ninety (90) days. In the event of any termination, all data associated with such Account will be deleted and Customer shall be responsible for revoking the Service's access to Customer's Google Apps domain data and files. Altirnao will provide Customer with prior notice of such termination and will send a data backup to Customer by email. In case of Accounts with more than one User, if at least one of the Users is active, the Account will not be considered inactive.

Restrictions on Use

Restrictions on Use of AODocs: In addition to all other terms and conditions contained herein, you shall not and shall not permit others to:

1. copy, modify, adapt, translate or otherwise create derivative works of the Service;
2. reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Service;
3. rent, lease, sell, assign or otherwise transfer rights in or to the Service;
4. remove any proprietary notices or labels from the Service;
5. use, post, transmit or introduce any device, software or routine which interferes or

attempts to interfere with the operation of the Service.

6. use the Service for spamming or any other illegal or unauthorized purpose or engage in illegal or deceptive trade practices; or

7. otherwise use of the Service in violation of any laws in your jurisdiction (including but not limited to copyright laws).

8. use the Service for High Risk Activities;

9. process or store any content on or through the Service that is subject to the International Traffic in Arms Regulations maintained by the Department of State.

10. if you are (or become) a Covered Entity or Business Associate, as defined in the Health Insurance Portability and Accountability Act **("HIPAA"),** use the Service for any purpose or in any manner involving Protected Health Information (as defined in HIPAA) unless you have received prior written consent to such use from both Google and Altirnao.

11. use the Service as a way to circumvent your obligation to provision one Google Apps End User Account for each User.

This list of prohibitions provides examples and is not complete or exclusive.

Restrictions on Use of Google Apps: You understand and agree that your use of the Service requires the use of Google Apps. You agree that you shall not and shall not permit others to:

copy, modify, create a derivative work of, reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract the source code of Google Apps or any component thereof;

use the Google Apps or any component thereof for uses such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of Google Apps or any component thereof could lead to death, personal injury, or environmental damage;

sublicense, resell, or distribute Google Apps or any component thereof;

use Google Apps or any component thereof to create, train, or improve (directly or indirectly) a substantially similar product or service, including any machine translation engine;

access Google Apps or any component thereof in a manner intended to avoid incurring fees;

use Google Apps or any component thereof to operate or enable any telecommunications service or in connection with any application that allows end users to place calls to or to receive calls from any public switched telephone network; or

process or store any data that is subject to the International Traffic in Arms Regulations maintained by the U.S Department of State or any other applicable law.

Altirnao reserves the right to suspend or terminate your access to Service with or without cause and with or without notice, for any reason or no reason, or for any action that Altirnao determines is inappropriate or disruptive to the Service or to any other user of this Service. Google may suspend your Google Apps account if: (a) your use of Google Apps is in violation of Google's Acceptable Use Policy, which could disrupt: (i) Google Apps; (ii) other users' use of Google Apps; or (iii) the Google network or servers used to provide Google Apps services; or
(b) there is unauthorized third party access to Google Apps.

You acknowledge and agree that Altirnao, in its sole discretion, with or without notice, may establish or revise from time to time general practices and limits concerning your use of the

Service, including without limitation, establishing the maximum number of Google Drive operations that can be done on your behalf in a given period of time. In addition, Altirnao may limit, without notice, the volume of e-mail forwarding or file downloading from the Service in response to unreasonable activity (such as spamming).

Altirnao may report to law enforcement authorities any actions that may be illegal, and any reports it receives of such conduct. When legally required or at Altirnao's discretion, Altirnao will cooperate with law enforcement agencies in any investigation of alleged illegal activity associated with the Service or on the Internet.

Unauthorized use of any trademarked, copyrighted or patented materials contained in the Service may violate certain laws and regulations.

You agree to indemnify and hold Altirnao and its officers, directors, employees, affiliates, agents, licensors, and business partners harmless from and against any and all costs, damages, liabilities, and expenses (including attorneys' fees and costs of defense) Altirnao or any other indemnified party suffers in relation to, arising from, or for the purpose of avoiding, any claim or demand from a third party that your use of this Service or the use of Service by any person using your Account (including without limitation, Your Content (as defined below)) violates any applicable law or regulation, or the copyrights, trademark rights or other rights of any third party.

Suspension

Altirnao reserves the right to suspend or terminate Customer's access to the Service with or without notice if Altirnao reasonably determines that:
(a) there is a threat or attack on the Service (including a denial of service attack) or other event that may create a risk to the Service, Altirnao, Customer, or any user of the Service;
(b) Customer's or its users' use of the Service or Customer Content disrupts or poses a security risk to the Service or any user of the Service, may harm Altirnao's systems, or may subject Altirnao or any third party to liability;
(c) Customer or any User is using the Service for fraudulent or illegal activities;
(d) Customer or any User is causing performance disruptions in the Service or in Google Drive by using the Service in a way that is not recommended in the performance guidelines published in the Service's documentation or by ignoring performance recommendations provided by Altirnao's technical support;
(e) subject to applicable law, Customer has ceased to continue Customer's business in the ordinary course, made an assignment for the benefit of creditors or similar disposition of its assets, or become the subject of any bankruptcy, reorganization, liquidation, dissolution or similar proceeding;
(f) Customer or any User is using the Service or other Altirnao property in breach of this Agreement;
or (g) Customer is in default of its payment obligations hereunder (collectively, "Service Suspensions"). Altirnao will make commercially reasonable efforts, circumstances permitting, to provide written notice of any Service Suspension to Customer, and to provide updates regarding resumption of Customer's access to the Service following any Service Suspension.

Subscription terms

Customer agrees to pay the subscription fee applicable to Customers and its Users use of the Service. Such fees will be paid on a periodic basis as agreed to Altirnao or to your Altirnao reseller as agreed when you registered for the Service.

In case of non-payment for any reason (including, if applicable, Altirnao's inability to charge your credit card or other payment method for any reason) or any violation of these Terms, Altirnao shall be entitled – without liability – to immediately suspend Customer's and Users' access to the Service. If you purchase your license to use the Service from Altirnao, you hereby expressly agree that Altirnao is permitted to bill you for the applicable fees, any applicable tax and any other charges you may incur in connection with your use of the Service, or charge such fees to your credit card or other payment method designated on your initial registration with the Altirnao at regular intervals for the remainder of the term of these Terms. If you cancel your Account at any time, you will not receive any refund.

Customer agrees that Customer's paid use of the Service is neither contingent on the delivery of any future functionality or features nor dependent on any oral or written public or private comments made by Altirnao or any Altirnao reseller regarding future functionality or features.

Intellectual Property

Customer hereby acknowledges and agrees that, subject to the limited rights granted hereunder, Altirnao (or its licensors) own all legal right, title and interest in and to the Service, including, without limitation, any Intellectual Property Rights or other proprietary rights which exist in the Service (whether such rights are registered or unregistered, and wherever in the world those rights may exist) **("Our Technology").** For purposes of these Terms, "Intellectual Property Rights" means, on a worldwide basis, any and all now known or hereafter known (a) rights associated with works of authorship including copyrights and moral rights, (b) trademark and trade name rights and similar rights, (c) trade secret rights, (d) patent rights and other industrial property rights, (e) intellectual and industrial property rights of every other kind and nature and however designated, whether arising by operation of law or otherwise, and (f) all registrations, applications, renewals, extensions, continuations, divisions, or reissues thereof now or hereafter existing, made, or in force (including any rights in any of the foregoing).

Our Technology may not be copied, modified, reproduced, republished, posted, transmitted, sold, offered for sale, or redistributed in any way without our prior written permission and the prior written permission of our applicable licensors. You must abide by all copyright notices, information, or restrictions contained in or attached to any of Our Technology. Nothing in these Terms of Use grants you any right to receive delivery of a copy of Our Technology or to obtain access to Our Technology except as generally and ordinarily permitted through the Service according to these Terms. Furthermore, nothing in these Terms of Use will be deemed to grant, by implication, estoppel or otherwise, a license to Our Technology. Certain of the names, logos, and other materials displayed on the Service constitute trademarks, trade names, service marks or logos **("Marks")** of Altirnao or other entities. You are not authorized to use any such Marks. Ownership of all such Marks and the goodwill associated therewith remains with and will inure to us or those other entities. To the extent indicated, any use of third party software provided in connection with the Service will be governed by such third parties' licenses and not by these Terms of Service. Furthermore, any comments, ideas and/or reports about the Service that you provide to us, whether in written or electronic form **("Feedback"),** shall be considered our proprietary and confidential information, and you hereby irrevocably transfer and assign to us all intellectual property rights embodied in or arising in connection with such Feedback, and any other rights or claims that you may have with respect to any such Feedback.

Ownership & Privacy

As between You and Altirnao, you retain all right, title and interest in any and all data, files, attachments, text, images, personally identifiable information, and other content that You and Your Users upload or submit to the Service (collectively, **"Your Content").** You may not upload, post or otherwise make available through the Service any material protected by copyright,

trademark, or any other proprietary right -without the express permission of the owner of such copyright, trademark or other proprietary right owned by a third party, and the burden of determining whether any material is protected by any such right is on you. You shall have sole responsibility for the accuracy, quality, integrity, legality, reliability, appropriateness, and intellectual property ownership or right to use any and all of Your Content. You represent and warrant that you have all rights, permissions and consents necessary (a) to make Your Content available on or through the Service, and (b) to grant Altirnao the limited rights to use Your Content set forth in these Terms.

You agree that Altirnao may use Your Content to provide the Service and its features, including by making it available for viewing, download and modification by other Users with access rights to Your Content. You hereby grant Altirnao a non-exclusive, perpetual, royalty-free, worldwide license (including the right to sublicense through multiple tiers) to access, use, reproduce, distribute, store, transmit, modify, adapt, reformat, publicly display, publicly perform and create derivative works of Your Content as required for the purpose of providing the Service to you.

You understand and agree that Altirnao does not have the ability to grant or revoke the Service's access to Customer's Google Apps domain data and files or other content and materials stored in Customer's Google Apps account. Therefore, You are solely responsible for granting the Service access to such Google Apps files and revoking such access when You cease use of the Service. Altirnao shall not be responsible and shall have no liability for any damages that result from Your failure to grant or revoke such access.

You understand and agree that Altirnao may, notwithstanding any provision of any separate nondisclosure agreement that may have been executed between You and Altirnao, distribute and disclose Your Content (a) to your Users, and (b) to Altirnao's service providers who act on Altirnao's behalf in providing the Service. Altirnao's use of any personally identifiable information you provide through the Service is governed by our Privacy Policy. Your use of the Service indicates your acceptance of the terms of our Privacy Policy. You can review the most recent version of our Privacy Policy at http://www .altirnao .com/pr ivacy-policy/ .

You hereby consent that, if You choose to become a paying customer of the Service, Altirnao may identify You as a Altirnao customer (using Your name and logo) and generally describe the products or services it provides to You in its promotional materials, presentations, and proposals to other current and prospective customers.

If you cancel your Service subscription, your information is no longer used and Altirnao will delete your Account and data associated with your Account within ninety (90) days of your cancellation. Please note, however, that some information like billing and subscription may remain with us for accounting and legal reasons.

Availability.

Altirnao will make the Service available to You in accordance with the Service Level Agreement available online at https://www.aodocs.com/sla (the **"SLA").** Altirnao does not make any representations or guarantees regarding uptime or availability of the Service unless specifically identified in the SLA. The Service may be unavailable at certain times as specified in the SLA, including during any unanticipated or unscheduled downtime or unavailability of all or any portion of the Service as a result of system failures or force majeure events.

Warranty Disclaimer

THE SERVICE IS PROVIDED ON AN "AS IS" BASIS, WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE

OR NON-INFRINGEMENT. ALTIRNAO MAKES NO WARRANTY THAT (I) THE SERVICE IS FREE OF VIRUSES OR OTHER HARMFUL COMPONENTS; (II) THE SERVICE WILL BE ERROR-FREE OR UNINTERRUPTED (INCLUDING, WITHOUT LIMITATION, INTERRUPTIONS THAT OCCUR IN THE CONTEXT OF REGULARLY SCHEDULED MAINTENANCE); (III) ANY INFORMATION OR ADVICE OBTAINED BY YOU IN CONNECTION WITH THE SERVICE WILL BE ACCURATE OR COMPLETE; OR (IV) THE RESULTS OF USING THE SERVICE WILL MEET YOUR REQUIREMENTS. SOME STATES DO NOT ALLOW EXCLUSION OF AN IMPLIED WARRANTY, SO THIS DISCLAIMER MAY NOT APPLY TO CUSTOMER.

Limitation of Liability

IN NO EVENT SHALL ALTIRNAO BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, OR OTHER LOSS OR DAMAGE WHATSOEVER (INCLUDING BUT NOT LIMITED TO LOSS OF DATA, LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, COMPUTER FAILURE, LOSS OF BUSINESS INFORMATION), ARISING OUT OF OR CAUSED BY YOUR USE OF OR INABILITY TO USE THE SERVICE, EVEN IF ALTIRNAO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. YOUR SOLE AND EXCLUSIVE REMEDY FOR ANY DISPUTE WITH ALTIRNAO RELATED TO ANY OF THE SERVICE SHALL BE TERMINATION OF SUCH SERVICE. IN NO EVENT SHALL ALTIRNAO'S ENTIRE LIABILITY TO YOU IN RESPECT OF ANY SERVICE, WHETHER DIRECT OR INDIRECT, EXCEED THE FEES PAID BY YOU TOWARDS SUCH SERVICE. SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE LIMITATIONS OR EXCLUSIONS IN THIS PARAGRAPH MAY NOT APPLY TO CUSTOMER.

Other Terms

These Terms, their interpretation, performance or any breach thereof, will be construed in accordance with, and all questions with respect thereto will be determined by, the laws of the State of California. Both parties hereby irrevocably submit any disputes under these Terms to the jurisdiction of the courts located in the State of California.

Last Updated: February 11th, 2016

EAST\53456530.2

Published by Google Drive – Report Abuse – Updated automatically every 5 minutes

Channel Foundation Agreement
U.S. Public Sector

1. INTRODUCTION

1.1 This Channel Foundation Agreement ("Foundation Agreement") specifies the terms and conditions agreed between CA and the Ordering Activity, as defined in GSA Order ADM4800.2G and as revised from time to time ("End User" or "Customer") as a foundation for their relationship as further defined in the applicable Modules. Ordering Activity understands and agrees that Ordering Activity's right to use the CA Offerings, ordered by Ordering Activity and submitted to CA by an Authorized CA Partner, is subject to Ordering Activity's compliance with this Foundation Agreement and the relevant Module for such CA Offering. The Foundation Agreement and the Module(s) incorporated into the GSA Schedule contract for the CA Offering(s) purchased by Ordering Activity will govern orders from an Authorized CA Partner for Ordering Activity's acquisition of the CA Offering and such terms shall remain binding upon both Ordering Activity and CA for that CA Offering absent mutual written agreement to the contrary.

1.2 Modules to this Foundation Agreement include the Channel Software Module, , Channel SaaS Module, Channel Hardware Appliance Module, and Channel Education Module.

2. DEFINITION

2.1 "Agreement" means this Foundation Agreement, the applicable Module, and License Metric for the applicable CA Offering, and any document incorporated expressly therein or incorporating the foregoing by reference.

2.2 "Authorized CA Partner" means an entity having a valid, current authorization from CA to market, offer and resell to Ordering Activity the right to use the CA Offering. Ordering Activity may find information regarding authorized CA Partners here: www.ca.com/partners.

2.3 "CA Offering" means the individual offering (such as software, services, software as a service etc.) made available by CA as defined in the Module and/or, License Metric.

2.4 "Confidential Information" means any information, maintained in confidence by the disclosing Party, communicated in written or oral form, marked as proprietary, confidential or otherwise so identified, that is exempt from disclosure under the Freedom of Information Act (FOIA), 5.U.S.C. §552(b) under one or more exemptions to that Act, and/or any information that by its form, nature, content or mode of transmission would to a reasonable recipient be deemed confidential or proprietary, including, without limitation, CA Offerings, Documentation, and any benchmark data and results produced.

2.5 "Documentation" means the documentation, technical product specifications and/or user manuals, published by CA or any entity within CA group of companies (each a CA entity) that is made generally available with CA Offerings.

2.6 "License Metric" means the specific criteria for measuring the usage of the CA Offering (such as MIPS, CPUs, tiers, servers, or users).

2.7 "Module" means the additional terms and conditions applicable to the CA Offering.

2.8 "Parties" means individually and or collectively CA and or the Ordering Activity.

2.9 "Prime Contractor" means the entity contracting directly with the Ordering Activity, if other than an Authorized CA Partner.

2.10 "Term" means the period for which Ordering Activity is authorized to use the CA Offering as specified in CA's order with Ordering Activity's chosen Authorized CA Partner or the Prime Contractor.

3. ORDERING AND DELIVERY

3.1 This Agreement applies to each specific CA Offering purchased by Ordering Activity from an Authorized CA Partner or Prime Contractor. Use of the CA Offerings, or of this Agreement to procure CA Offerings, by Ordering Activity's Affiliates outside of the jurisdiction specified for Ordering Activity in the order between CA and the Authorized CA Partner or Prime Contractor is not permitted unless such Affiliate signs a participation agreement with CA to adopt and adhere to the terms of this Agreement.

3.2 CA will deliver or make available a CA Offering to Ordering Activity only upon, and in accordance with, CA's execution of an order with the Authorized CA Partner. Any terms that may appear on an Ordering Activity's purchase order (including without limitation pre-printed terms), or as part of Ordering Activity's order with an Authorized CA Partner or Prime Contractor, that conflict or vary from the terms and conditions of this Agreement shall not apply to CA and shall be deemed null and void unless otherwise required by law.

3.3 The CA Offering will be delivered by CA to Ordering Activity either by electronic delivery (ESD) or in tangible media in accordance with the terms of the GSA Schedule contract and the relevant purchase order. CA agrees to be responsible for all customs duties and clearances.

4. CONFIDENTIAL INFORMATION

4.1 The Parties agree that when receiving Confidential Information from the disclosing Party, that the receiving Party shall hold it in confidence and shall not disclose or use such information except as permitted under the Agreement. The receiving Party shall treat the disclosing Party's Confidential Information confidentially and in the same manner as it treats its own proprietary and/or confidential information, which shall not be less than a reasonable standard of care, and the receiving Party shall use Confidential Information only for the purposes described in the Agreement. Confidential Information may be disclosed to receiving Party's employees, agents, financial advisors, contractors and attorneys on a need-to know basis and the receiving Party shall ensure that such persons maintain such Confidential Information pursuant to the terms of the Agreement.

4.2 The receiving Party shall be permitted to disclose Confidential Information in connection with a judicial or administrative proceeding to the extent that such disclosure is required under applicable law or court order, provided that the receiving Party shall, where reasonably possible, give the disclosing Party prompt and timely written notice of any such proceeding and shall offer reasonable cooperation in any effort of the disclosing Party to obtain a protective order.

4.3 For the purposes of the Agreement, Confidential Information shall exclude: (i) information which the receiving Party has been authorized in writing by the disclosing Party to disclose without restriction; (ii) information which was rightfully in the receiving Party's possession or rightfully known to it prior to receipt of such information from the disclosing Party; (iii) information which was rightfully disclosed to the receiving Party by a third Party having proper possession of such information, without restriction; (iv) information which is part of or enters the public domain without any breach of the obligations of confidentiality by the receiving Party; and (v) information which is independently developed by the receiving Party without use or reference to the disclosing Party's Confidential Information.

4.4 Nothing in the Agreement will (i) preclude CA from using the ideas, concepts and know-how which are developed in the course of providing any CA Offerings to Ordering Activity or (ii) be deemed to limit CA's rights to provide similar CA Offerings to other customers. Ordering Activity agrees that CA may use any feedback provided by Ordering Activity related to any CA Offering for any CA business purpose, without requiring consent including reproduction and preparation of derivative works based upon such feedback, as well as distribution of such derivative works.

4.5 To the extent permitted by the Federal Records Act, the receiving Party agrees, upon request of the disclosing party, to return to the disclosing Party all Confidential Information in its possession or certify the destruction thereof.

4.6 For CA software (including code) and Documentation, and Ordering Activity's and/or CA's Confidential Information expressly designated in writing as perpetually confidential, the obligations of this section are perpetual and shall survive termination. For all other Confidential Information, the foregoing obligations shall extend for five (5) years from the date of initial disclosure.

5. FEES

5.1 The Parties acknowledge and agree that all terms governing the fees, payments, payment schedules, pricing and discounts for the applicable CA Offering procured by Ordering Activity under this Agreement are and shall be between solely Ordering Activity and their chosen Authorized CA Partner or Prime Contractor.

6. TITLE

6.1 CA retains all right, title, copyright, patent, trademark, trade secret and all other proprietary interests to all CA Offerings and any derivatives thereof. No title, copyright, patent, trademark, trade secret or other right of intellectual property not expressly granted under the Agreement is exchanged between the Parties.

7. WARRANTY

7.1 Each Party represents and warrants that it has the legal power to enter into the Agreement.

7.2 CA represents and warrants that it owns or otherwise has sufficient rights to grant Ordering Activity the rights defined in the Agreement.

8. INDEMNIFICATION

8.1 CA will indemnify any third party claims that Ordering Activity's use of the specific CA Offering licensed or purchased by Ordering Activity under this Agreement infringes any valid US patent or copyright within the jurisdictions where Ordering Activity is authorized to use the CA Offering at the time of delivery. CA may, at its option and expense: (i) procure for Ordering Activity the

right to continue to use the CA Offering; (ii) repair, modify or replace the CA Offering so that it is no longer infringing; or (iii) provide a pro-rated refund to the Authorized CA Partner of the fees paid for the CA Offering which gave rise to the indemnity calculated against the remainder of the Term from the date it is established that CA is notified of the third party claim. If the CA Offering is CA Software, and is licensed on a perpetual basis, an amortization schedule of three (3) years shall be used for the basis of the refund calculation.

8.2 CA shall have no liability: (i) in the event the allegation of infringement is a result of a modification of the CA Offering except a modification by CA, (ii) if the CA Offering is not being used in accordance with CA's specifications, related documentation and guidelines, (iii) if the alleged infringement would be avoided or otherwise eliminated by the use of a CA published update or patch, (iv) if the alleged infringement is a result of use of the CA Offerings in combination with any third party product, or (v) if the applicable fees due for the specific CA Offering have not been paid by Ordering Activity or Prime Contractor to its Authorized CA Partner. The indemnifications contained herein shall not apply and CA shall have no liability in relation to any CA Offering produced by CA at the specific direction of Ordering Activity. THE FOREGOING PROVISIONS STATE THE ENTIRE LIABILITY AND OBLIGATIONS OF CA REGARDING CLAIMS OF INFRINGEMENT, AND THE EXCLUSIVE REMEDY AVAILABLE TO ORDERING ACTIVITY WITH RESPECT TO ANY ACTUAL OR ALLEGED INFRINGEMENT OR MISAPPROPRIATION OF ANY INTELLECTUAL PROPERTY OR OTHER PROPRIETARY RIGHTS.

8.3 CA shall indemnify Ordering Activity against all damages, fees, (including reasonable attorney's fees) fines, judgments, costs and expenses finally awarded as a result of a third party action alleging a bodily injury or death which arises under the Agreement, provided that such liabilities are the proximate result of gross negligence or intentional tortuous conduct on the part ofCA.

8.4 The above indemnities are contingent upon: (i) Ordering Activity providing prompt notice of any claim of infringement and assistance in the defense thereof, (ii) CA's right to consult with Ordering Activity at any time and to intervene in the proceedings through CA's chosen counsel at CA's expense, provided that Ordering Activity shall not have the right to settle any claim requiring CA to make a payment or to admit liability without CA's prior written agreement , and (iii) Ordering Activity not taking any actions or failing to take actions that hinder the defense or settlement process.

9. LIMITATION OF LIABILITY

EXCEPT IN THE CASE OF A BREACH OF TITLE, INFRINGMENT OF CA'S INTELLECTUAL PROPERTY RIGHTS OR CONFIDENTIALITY, OR OF THIRD PARTY CLAIMS ARISING UNDER THE INDEMNIFICATION SECTION, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW NEITHER PARTY (INCLUDING ANY OF CA'S SUPPLIERS) SHALL BE LIABLE FOR A) ANY INDIRECT, SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES OF ANY NATURE, INCLUDING, BUT NOT NECESSARILY LIMITED TO, LOSS OF PROFIT, DAMAGES RELATING TO MONIES SAVED OR FEES GENERATED AND OR ANY LOSS OF DATA BY USE OF ANY CA OFFERING, REGARDLESS OF WHETHER A PARTY WAS APPRISED OF THE POTENTIAL FOR SUCH DAMAGES; AND B) IN NO EVENT WILL A PARTY'S LIABILITY, EXCEED THE FEES PAID AND OR OWED TO CA FOR THE THEN CURRENT INITIAL OR RENEWAL TERM FOR WHICH THE ORDERING ACTIVITY HAS PROCURED THE CA OFFERING OR AS FURTHER DEFINED IN THE MODULE. FURTHERMORE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, CA SHALL NOT INCUR ANY LIABILITY FOR DEATH OR BODILY INJURY TO ANY THIRD PARTY UNLESS THE SAME ARISES FROM THE INTENTIONAL OR GROSSLY NEGLIGENT ACT(S) OF CA. This clause shall not impair the U.S. Government's right to recover for fraud or crimes arising out of or related to this Agreement under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733.

10. TERM & TERMINATION

10.1 This Foundation Agreement shall continue in effect unless otherwise terminated in accordance with this section or as required pursuant to Federal Acquisition Regulation (FAR) 52.212-4 "Contract Terms and Conditions- Commercial Items" sections (l) "Termination for the Government's Convenience" and (m) "Termination for Cause."

10.2 In the event Ordering Activity elects to terminate an order for its convenience prior to the expiration of the then current term, and such order includes licenses for CA Software, Ordering Activity shall also, within a reasonable period of time, delete all copies of such software from its systems, including copies stored for archival purposes and either destroy or return them to CA. The foregoing shall not apply, however, where such licenses were perpetual and Ordering Activity, at the time of such termination, has paid all associated perpetual license fees.

10.3 Termination does not release either Party from any liability which, at the time of such termination, had already accrued to the other Party or which is attributable to a period prior to such termination, nor preclude either Party from pursuing any rights or remedies it may have under law or in equity with respect to any breach of this Foundation Agreement or the Agreement.

11. DISPUTE RESOLUTION

11.1 Prior to the initiation of formal dispute resolution procedures regarding any dispute, controversy, or claim arising out of the Agreement or interpretation thereof (a "Dispute"), the Parties shall first meet as often, and for such duration and as promptly as the Parties reasonably deem necessary to discuss the Dispute and negotiate in good faith in an effort to resolve it.

11.2 The provisions of paragraph 11.1 will not be construed to prevent a Party from instituting formal proceedings to the extent necessary to avoid the expiration of any applicable limitations period or to pursue equitable rights or injunctive remedies deemed reasonable necessary to protect its interests.

11.3 Disputes relating to the payments of fees, any third party products or services or otherwise relating to the terms and conditions of an order between an Authorized CA Partner and Ordering Activity, shall be between Ordering Activity and such Authorized CA Partner, or if applicable, between Ordering Activity and Prime Contractor, and Ordering Activity agrees that it shall have no right of contribution or other claim from or against CA by reason thereof.

12. GENERAL TERMS

12.1 **Amendments**. The terms of the Agreement may only be amended by mutual written agreement of the Parties.

12.2 **Force Majeure**. Except for payment obligations and obligations pertaining to non-disclosure, notwithstanding any contrary provision in the Agreement, neither Party will be liable for any action taken, or any failure to take any action required to be taken, in the event and to the extent that the taking of such action or such failure arises out of causes beyond a Party's control, including, without limitation, war, civil commotion, act of God, strike or other stoppage (whether partial or total) of labor, any law, decree, regulation or order of any government or governmental body (including any court or tribunal).

12.3 **Order of Precedence**. Any conflict or inconsistency among or between the terms and conditions of the documents comprising the Agreement shall be resolved according to the following order of precedence, in the order of the greatest control to the least: (1) U.S. Federal law, (2) the relevant Module and(3) this Channel Foundation Agreement. Notwithstanding this Order of Precedence, unless expressly required by U.S. Federal law in subcontracts for commercial information technology, neither an Ordering Activity issued purchase order, nor the terms of an order between Ordering Activity and the Authorized CA Partner or Prime Contractor, shall modify the terms of the documents indicated herein.

12.4 **Ordering Activity Data**. If Ordering Activity transfers any personal data to CA as a requirement pursuant to any CA Offering, then Ordering Activity represents that (i) it is duly authorized to provide personal data to CA and it does so lawfully in compliance with relevant legislation, (ii) CA and any entity within the CA group of companies (each a "CA entity") or its subcontractors can process such data for the purposes of performing its obligations and (iii) CA may disclose such data to any CA entity and its subcontractors for this purpose and may transfer such data to countries outside of the country of origin. CA, Inc. is Safe Harbour certified and the CA Entities have committed to comply with relevant data protection/privacy legislation.

12.5 **Import Export**. Ordering Activity agrees that CA Offerings, Documentation, and or Confidential Information is subject to export controls of the United States of America and import controls of any other country in which such information may be used. Ordering Activity agrees to export, re-export or import such information only in compliance with such laws and controls.

12.6 **Announcements**. Neither Party may issue press releases relating to the Agreement without approving the content with the other Party. Either Party may include the name and logo of the other Party in lists of customers or vendors in accordance with the other Party's standard guidelines.

12.7 **Counterparts**. This Foundation Agreement and any Module, as applicable, may be signed in any number of counterparts by the Parties and each part shall be considered part of the whole and valid, legally binding document.

12.8 **Notice**. All notices hereunder shall be delivered to the other Party identified in the Agreement either personally, via certified mail, facsimile or overnight courier. If delivered personally, notice shall be deemed effective when delivered; if delivered via facsimile, notice shall be deemed effective upon electronic confirmation; and if delivered via certified mail or overnight courier, notice shall be deemed effective upon confirmation of delivery.

12.9 **Headings**. The section headings used herein are for information purposes only and shall not affect the interpretation of any provision of this Agreement.

12.10 **Validity**. In the event any term or provision of the Agreement shall be held to be invalid, the same shall not affect in any respect whatsoever the validity of the remainder of the Agreement.

12.11 **Third Parties**. This Agreement shall not create any rights in favor of, or any obligations owed by, any third party unless otherwise expressly defined in any Module. The Parties agree that any action arising from this Agreement shall solely be brought by Ordering Activity, the U.S. Government, or CA, unless otherwise permitted by law.

12.12 **Choice of Law**. To the extent that federal law is not dispositive of a dispute hereunder, the laws of the State of New York (excluding its conflict of laws provisions) shall govern the construction and enforceability of the Agreement.

12.13 **Survival**. Sections pertaining to Confidentiality, Title, Limitation of Liability, Termination, and Import Export shall survive termination of this Foundation Agreement.

12.14 **Entire Agreement**. The Agreement and all documents incorporated by reference therein shall comprise the entire agreement as pertaining to the subject matter thereof and all other prior representations, proposals, and other such information exchanged by the Parties concerning the subject matter is superseded in their entirety by the Agreement.

Channel SaaS Module

U.S. Public Sector

1. INTRODUCTION

1.1. This Module for Software as a Service ("SaaS Module") specifies terms and conditions which apply to Software as a Service that CA will provide to Ordering Activity.

1.2. This SaaS Module incorporates by reference the terms of the Foundation Agreement. Any capitalized terms used in this SaaS Module shall have the meanings given in the Foundation Agreement unless otherwise provided herein.

2. DEFINITIONS

2.1. "Ordering Activity Data" means information stored in the SaaS database.

2.2. "Force Majeure Event" means an event of Force Majeure as defined in the Foundation Agreement and/or delays caused by an internet service provider or hosting facility that results in data center outages resulting from causes not within CA'scontrol.

2.3. "ISO 27001" means an Information Security Management System standard published by the International Organization for Standardization (ISO). This particular standard specifies a management system that is intended to bring information security under explicit management control and mandates specific requirements when this standard is met.

2.4. "Production" means the "live" environment of SaaS provided to process data on a real-time basis.

2.5. "Production Availability" means, for purposes of measuring the Service Level, the aggregate number of minutes during the month in which the SaaS is available for Production access and use by Ordering Activity.

2.6. "SaaS" means the online version of the CA Software specified in the Authorized CA Partner's order with CA for access to and usage by its customers via a website(s) environment.

2.7. "SAS 70 Type II" means the standards used by an independent auditor that employs procedures, policies and controls of SAS 70 Type I to verify and validate that the organization is following those procedures regarding control objectives, activities and control over information technology, and related processes.

2.8. "SaaS Support" means support of the underlying CA software so it operates materially in accordance with the Documentation.

2.9. "Sandbox" means a development or test environment that is not Production.

2.10. "Scheduled Downtime" means planned downtime of SaaS availability where CA provides notice to Ordering Activity at least 72 hours in advance.

2.11. "Service Level" means as described in the section entitled: Service Level Commitments.

2.12. "Subscription Term" means the period of the Ordering Activity's subscription to the SaaS as specified in the Authorized CA Partner's order with CA.

2.13. "Users" means the number of individuals authorized to access and use of SaaS by Ordering Activity and who have been provided user identifications and passwords by Ordering Activity (or by CA at Ordering Activity's request), measured by CA on an aggregate monthly basis by the amount of User Logins. Users may include Ordering Activity and Affiliate's employees and independent contractors that agree to be bound by terms and conditions no less restrictive than those contained herein and are acting on behalf of Ordering Activity and not a third party.

2.14. "User Logins" means the initial and standard login screen where a User is required to enter its user ID and the password.

3. SAAS OFFERING

3.1. CA shall provide SaaS to Ordering Activity during the Subscription Term directly or through a third party SaaS provider in accordance with the terms of the Agreement.

3.2. CA hereby provides Ordering Activity a non-transferable and non-exclusive right to access and use SaaS for the sole purpose of supporting its internal business use. A new User may replace a former User who no longer requires access to, or use of, the SaaS. Users may be Ordering Activity employees, Ordering Activity third party consultants, contractors or agents, which third parties may

access and use the SaaS solely for the benefit of Ordering Activity's internal business purposes in accordance with the provisions of this Agreement.

3.3. Ordering Activity acknowledges and agrees that in order for CA to effectively provide SaaS, Ordering Activity may be required to provide necessary information and shall not delay, prevent or interfere with CA's provision of SaaS.

4. FEES & RENEWAL

4.1. Ordering Activity may access SaaS for solely the number and type of Users specified in the Authorized CA Partner's order with CA. Additional Users, or an additional SaaS offering, if available, shall require Ordering Activity to procure with CA or an Authorized CA Partner (whether directly or through a Prime Contractor) for such users or offering. Unless otherwise agreed by CA, (i) additional Users may be purchased only in increments of 50 Users; and (ii) such additional User subscriptions shall be coterminous with the expiration of the Subscription Term.

4.2. CA may with notice prior to any renewal, replace the Ordering Activity ordered SaaS with replacement, underlying software that is generally available to customers with alternative, materially similar, functionality.

4.3. The fees for SaaS subscription are not contingent upon the delivery of any future functionality or features of the CA Software.

5. ORDERING ACTIVITY DATA

5.1. Ordering Activity exclusively owns all rights, title and interest in and to all Ordering Activity Data. Ordering Activity Data shall be considered to be Confidential Information under the Agreement. CA shall not access Ordering Activity's User accounts, or Ordering Activity Data, except (i) in the course of data center business operations if required, (ii) in response to SaaS or technical issues or (iii) at Ordering Activity's specific request as reasonably required in the provision of SaaS. CA will segregate Ordering Activity's Data from other customers' data.

5.2. CA operates and maintains a disaster recovery procedure. In case of a Force Majeure Event, Ordering Activity acknowledges and agrees that Ordering Activity Data may not be recoverable and accepts responsibility for re-entry of such data.

5.3. Ordering Activity Data will be returned to the Ordering Activity at the end of the Subscription Term or at the termination of the SaaS subscription in the manner described in the SaaS Documentation.

6. SECURITY

6.1. CA shall adhere to SAS 70 Type II audit compliance criteria and data security procedures which meet ISO 27001 status during the Subscription Term.

6.2. CA shall comply with CA's security policy and procedures, which policies and procedures are designed to provide and maintain commercially reasonable safeguards against the destruction, loss or alteration of, or unauthorized access to or use of the Ordering Activity Data in CA's possession or control and which safeguards are, at a minimum, no less rigorous than those maintained by CA for its own information of a similar nature.

6.3. Ordering Activity Data shall be stored pursuant to CA's data security procedures, which shall be provided to Ordering Activity upon request. Except as required herein, CA will not be responsible for any unauthorized access to, or alteration, theft or destruction of Ordering Activity Data, unless caused as a result of CA's negligence or intentional misconduct, in which case restoring or recovery of Ordering Activity Data shall be limited to the most recent back-up of Ordering Activity Data. CA is not responsible for loss of Ordering Activity Data arising from Ordering Activity's: (i) transmission of data in contravention of the User Guide; or (ii) failure to act on any CA provided communication.

6.4. CA shall comply with the applicable EU member states' implementation of the Directive 95/46/EC ("Directive") governing the processing of personal data as defined specifically in the Directive and CA, Inc. is Safe Harbour certified.

6.5. Ordering Activity or an independent third party may audit CA's operations within the applicable data center to verify CA's compliance with the security and technical provisions defined in this Module. The audit may take place, no more than once annually, upon thirty (30) days prior written notice subject to Ordering Activity or its independent third party having executed a CA confidentiality agreement and stating the purpose and scope of the request. Such audit shall be conducted during normal business hours in a manner that does not disrupt business operations.

7. INITIATION AND SUPPORT PROCESSES

7.1. The following processes apply to the SaaS:

i. CA will send an email to Ordering Activity's technical contact identified in the Authorized CA Partner's order with CA setting out the SaaS URL(s) and other information necessary for initial use of the SaaS. Ordering Activity shall provide information as requested within 7 days of receiving the email.

ii. Customer will utilize the CA Support website, or other site or notification mechanism as CA may designate from time to time, to notify CA of SaaS availability issues, request other in-scope technical support assistance, or for Customer's to provide feedback or approvals on requests as applicable.

8. SAAS SUPPORT

8.1. The Ordering Activity shall be provided with SaaS Support during the Subscription Term.

8.2. For any SaaS Support requests, Ordering Activity should be prepared to provide to SaaS Support personnel, all pertinent information, in English, including but not limited to, Ordering Activity number or site identification number, incident severity, SaaS/software name, area of SaaS (Production or Sandbox), incident description, and a technical contact familiar with Ordering Activity's environment or the problem to be solved. Ordering Activity must use reasonable efforts to communicate with CA in order to verify the existence of the problem and provide information about the conditions under which the problem could be duplicated.

8.3. Upon receiving Ordering Activity's technical contact information, SaaS Support will be provided in a timely and professional manner by qualified support engineers as defined below:

i. Access to CA help desk and the ability to open and manage support incidents via CA support online or by telephone.

ii. Production environment support: 24x7 for severity 1 incidents; normal business hours for severities 2-4.

iii. Sandbox environment support: Normal business hours for incidents of all severities.

iv. Access to CA support website (currently: http://support.ca.com) for 24x7x365 online support and access to CA software product and documentation, global user communities and regional user groups, FAQs, samples, webcast recordings and demos, usage tips, technical updates and HYPER notifications, as such are made available by CA.

v. Interactive remote diagnostic support allowing CA support engineers to troubleshoot an incident securely through a real-time browser-based remote control feature.

vi. Additional support such as file storage, point in time backup, periodic file refresh and basic reporting may be available at CA's discretion according to the SaaS provided.

Any additional support requirements are only by prior written agreement with CA.

8.4. In order to respond to an issue raised through SaaS Support, CA may request Ordering Activity to upgrade to appropriate operating systems and or third party applications as required in order to properly operate and access the SaaS offering. Any such upgrades or installations shall be at the Ordering Activity's sole option and discretion. The costs associated with any upgrades required and any such installations are not included as SaaS Support and all such costs shall be the responsibility of the Ordering Activity.

9. ORDERING ACTIVITY RESPONSIBILITIES

9.1. Ordering Activity is responsible for all activities that occur in, or are related to, User accounts including the data, information stored or transmitted when accessing SaaS.

9.2. Because Ordering Activity may integrate or utilize third party links to other software, hardware or other service which are associated with, or otherwise available through SaaS, Ordering Activity agrees that it and its Users shall use such third party links in their sole discretion. CA shall have no responsibility or liability with respect to such third party links used by Ordering Activity's or Users' or for any act or omission of any such third party provider.

9.3. Ordering Activity shall not: (i) make SaaS available to any third party not authorized, other than to Users or as otherwise contemplated by this Agreement; (ii) send or store code that can harm or result in damage to the SaaS offering (including but not limited to malicious code and malware); (iii) wilfully interfere with or disrupt the integrity of SaaS or the data contained therein; (iv) attempt to gain unauthorized access to the SaaS or its related system or networks; (v) use SaaS to provide services to external end users and or to process data other than Ordering Activity's as an outsourcer, service bureau or consultant without written permission provided by CA.

10. WARRANTY

10.1. CA warrants that (i) SaaS shall perform materially in accordance with the applicable SaaS Documentation and (ii) that SaaS will be available online according to the performance levels described in the Service Levels defined in this SaaS Module.

10.2. EXCEPT AS EXPRESSLY SET FORTH ABOVE, TO THE EXTENT PERMITTED BY LAW, NO OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THIRD PARTY WARRANTIES, IMPLIED WARRANTIES OF MERCHANTABILITY, SUITABILITY OR SATISFACTORY QUALITY, OR THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE ARE MADE BY CA AND CA MAKES NO WARRANTIES HEREUNDER WITH RESPECT TO ANY HARDWARE EQUIPMENT OR THIRD PARTY SOFTWARE WHICH CA MAY USE TO PROVIDE THE SAAS.

10.3. Ordering Activity warrants that (i) it has the right to transmit any data or information as may be required for the purposes of accessing SaaS (ii) it will ensure compliance to the Agreement by itself and its Users and (iii) it is responsible for all activities that occur in User accounts, (iv) it shall not misuse SaaS through sending spam or otherwise duplicative or unsolicited messages or store infringing, obscene, threatening, or otherwise unlawful material that is harmful to children or violates third party privacy rights.

11. WARRANTY REMEDY

11.1. In the event of a breach of the Warranty by CA, CA may in consultation with Ordering Activity (i) use reasonable efforts consistent with industry standards to cure the defect as defined in CA Support process outlined in this SaaS Module and or (ii) Ordering Activity may exercise its rights to termination as defined under the Service Level Commitment section below and qualify for a refund as defined therein and or (iii) mutually agree with Ordering Activity to terminate the subscription and provide a pro-rata refund to the Authorized CA Partner calculated on the number of months left remaining on the Subscription Term. Warranty remedies are conditioned upon (i) any error or defect complained of is reasonably reproducible by CA, (ii) the breach is not attributable in whole or in part to any non-CA product(s) or service(s).

12. SERVICE LEVEL COMMITTMENT

12.1. Service Levels: The following Service Levels will apply to the applicable SaaS offering during the applicable Subscription Term:

i. Production Availability of SaaS 99.5% on a monthly basis. If Production Availability falls below 99%, it shall be considered a minor failure; and if Production Availability falls below 98%, it shall be considered a major failure.

12.2. Ordering Activity will be provided monthly electronic reports regarding Service Levels and follow the procedure set out below:

i. CA will investigate missed Service Levels through determining the root cause of the issue then using commercially reasonable efforts to correct the issue and advising Ordering Activity as reasonably requested by Ordering Activity of the status of efforts being undertaken with respect to the issue;

ii. Provide Ordering Activity reasonable evidence to Ordering Activity that the cause of the issue is being corrected or will be corrected and

iii. In the event of a minor failure, Ordering Activity is entitled to 2 additional days of the applicable SaaS offering at no additional charge. In the event of a major failure, Ordering Activity is entitled to 5 additional days of the applicable SaaS offering at no additional charge.

12.3. Pursuant to FAR 52.212-4(l), Ordering Activity may terminate for convenience its subscription to SaaS without incurring any additional charges or termination fees. In the event of such termination for convenience CA shall refund to the CA Authorized Partner that portion of the fees paid which have not yet been applied towards SaaS as of the effective date of termination. Any such refund herein shall be Ordering Activity's sole and exclusive remedy under this SaaS Module with respect to CA only and CA shall have no further liability arising out of the applicable SaaS subscription, and shall not impact termination of any other Module or the Foundation Agreement. This section does not limit the rights or remedies of the Ordering Activity under FAR 52.212-4(m), Termination for cause.The following events shall be excluded from the calculation of any Service Level failures: (i) Force Majeure Event; (ii) outages due to Scheduled Downtime such as upgrading data center infrastructure; (iii) outages based on Ordering Activity networks or domain name server issues; (iv) Ordering Activity's configuration, scripting, coding; (v) internet outages; (vi) Ordering Activity outages requested by Ordering Activity (vii) Ordering Activity changes to its environment which hinder SaaS production and (viii) inability for Ordering Activity to log in due to use of Lightweight Directory Access Protocol (LDAP) to control authentication.

13. NIMSOFT SaaS

13.1. The following sections of this Module are not applicable to Nimsoft Saas transactions:

i. 2.2;

ii. 2.3;

iii. 2.7;

iv. 5.2;

v. 6.1;

vi. 6.5 and

vii. 12.2;

13.2. The following sections of this Module are modified or added as follows for Nimsoft SaaS (On-Demand) transactions to the extent consistent with U.S. Federal law:

i. Section 7.1 ii: "Ordering Activity will utilize the **Nimsoft** CA Support website, or other site or notification mechanism as CA may designate from time to time, to notify CA of SaaS availability issues, request other in-scope technical support assistance, or for Ordering Activity to provide feedback or approvals on requests as applicable."

ii. Section 8.1: "The Ordering Activity shall be provided with SaaS Support pursuant ot the terms of http://www.nimsoft.com/content/dam/nimsoft/documents/un-secure/agreements/nimsoft-us-support-agreement.pdf during the Subscription term."

iii. Section 10.1: "CA warrants that (i) SaaS shall perform materially in accordance with the applicable SaaS Documentation for a period of 60 days from the commencement of the Term and (ii) that SaaS will be available online according to the performance levels described in the Service Levels defined in this SaaS Module.

iv. Add the following as Section 15:

"15. **REPORTING AND AUDIT**

Reports. Ordering Activity agrees to prepare and submit monthly reports to the Authorized CA Partner and CA that shall include, without limitation, information detailing the use of SaaS pursuant to the license metrics applicable to SaaS ("Report"). Ordering Activity shall submit each Report to the Authorized CA Partner and CA on the fifteenth day of each calendar month.

Overage. If the Report shows the Ordering Activity has exceeded the Authorized Use Limitation at any time during a month, such Report shall constitute a basis for a claim to the relevant Contracting Officer pursuant to the Contract Disputes Act and FAR 52.233-1. In no event may the SaaS quantity be lowered below the original numberordered.

14. **GENERAL TERMS.**

14.1. Any conflict or inconsistency among or between the terms and conditions of the documents comprising the Agreement shall be resolved according to the following order of precedence, in the order of the greatest control to the least: (1) U.S. Federal law, (2) this Channel SaaS Module and (3) the Channel Foundation Agreement. Notwithstanding the foregoing, unless expressly required by U.S. Federal law in subcontracts for commercial information technology, neither an Ordering Activity issued purchase order, nor the terms of an order between Ordering Activity and the Authorized CA Partner or Prime Contractor, shall modify the terms of the documents indicated herein.

Channel Hardware Appliance Module
U.S. Public Sector

1. INTRODUCTION

1.1. This Module for the Hardware Appliance ("Hardware Appliance Module") specifies terms and conditions which apply to the Hardware Appliance which CA will provide to Ordering Activity.

1.2. This Hardware Appliance Module incorporates by reference the terms of the Foundation Agreement. Any capitalized terms used in this Hardware Appliance Module shall have the meanings given in the Foundation Agreement unless otherwise provided herein.

2. DEFINITIONS

2.1. "Hardware" means a single CA-supplied third party physical server or device.

2.2. "Hardware Appliance" means Hardware that is bundled with and operates the CA Software licensed by Ordering Activity and pre-installed on the Hardware.

3. APPLIANCE OFFERING

3.1. CA shall provide the Hardware Appliance specified in the Authorized CA Partner's order with CA.

3.2. The terms for license and support for the underlying CA Software is covered separately under the Software Module.

4. FEES

4.1. Ordering Activity may order Hardware Appliance with, and pay the associated fees and other charges to an Authorized CA Partner or Prime Contractor. CA will deliver to Ordering Activity the Hardware Appliance specified in the Authorized CA Partner's order with CA.

4.2. Upon CA's receipt of payment from the Authorized CA Partner, Ordering Activity will own the Hardware free of any liens or encumbrances.

5. WARRANTY

5.1. Upon the purchase of a Hardware Appliance, CA will pass through to the Ordering Activity the applicable Hardware warranty. Such warranty will be provided for a period of twelve (12) months or more depending on the type of Hardware Appliance purchased. A copy of the applicable third party support warranty coverage is available under the "Get Support" section of CA's Support website located at https://support.ca.com.

6. WARRANTY REMEDY

6.1. To address a warranty issue on the Hardware, CA will provide Ordering Activity telephone assistance to access the third party Hardware support to address support issues with the Hardware.

6.2. Except for procuring third party warranty coverage for the Hardware as described above, the Hardware is provided on an "AS IS" basis and CA makes no warranties, and disclaims any and all express or implied warranties (including but not limited to warranties of merchantability or satisfactory quality or fitness for a particular purpose), with respect to the Hardware. None of the warranties specified in the Foundation Agreement or any other agreement shall apply to the Hardware.

7. ORDERING ACTIVITY REQUIREMENTS

7.1. Ordering Activity is solely responsible for use of the Hardware, including assuring proper supported environment configuration, CA software installation, and operating methods in accordance with the Hardware specifications and Documentation.

7.2. CA will not support modifications to the Hardware nor will it support the Hardware if Ordering Activity fails to comply with the terms of the Agreement to the extent such failure causes the Hardware's failure to perform in substantial accordance with the applicable Hardware documentation.

7.3. CA shall have no obligation to replace the Hardware, or provide additional hardware, in cases where future Versions or Releases (as such terms are defined in the Software Module) of the CA Software require an upgrade of or addition to such Hardware.

8. GENERAL TERMS

8.1. Any conflict or inconsistency among or between the terms and conditions of the documents comprising the Agreement shall be resolved according to the following order of precedence, in the order of the greatest control to the least: (1) U.S. Federal law, (2) this Channel Hardware Appliance Module and (3) the Channel Foundation Agreement. Notwithstanding the foregoing, unless expressly required by U.S. Federal law in subcontracts for commercial information technology, neither an Ordering Activity issued purchase

order, nor the terms of an order between Ordering Activity and the Authorized CA Partner or Prime Contractor, shall modify the terms of the documents indicated herein.

1. INTRODUCTION

1.1. This Module for Education ("Education Module") specifies terms and conditions which apply to Education that CA will provide to Ordering Activity.

1.2. This Education Module incorporates by reference the terms of the Foundation Agreement. Any capitalized terms used in this Education Module shall have the meanings given in the Foundation Agreement unless otherwise provided herein.

2. DEFINITIONS

2.1. "Attendees" mean the participants authorized by Ordering Activity to attend or participate in the Education offerings as indicated in the Transaction Document.

2.2. "Course Materials" means any Education content provided to Ordering Activity in any media form pursuant to a Transaction Document, including without limitation, all publications, courseware, training manuals and materials, user guides, web portals, or virtual labs provided by CA or a CA subcontractor.

2.3. "Education" means any standard or customized education offerings, training or instruction, or related services, provided by CA or a CA subcontractor in any format or location, including without limitation, (i) instructor led training, including at CA or Ordering Activity site(s), (ii) virtual training, including online classes, courses, or course catalogues and/or (iii) class room training or testing, at a CA or third party training facility.

3. EDUCATION OFFERING

3.1. CA shall provide the Education as specified in the Authorized CA Partner's order with CA.

3.2. CA may require the registration or pre-registration of Attendees in order to attend or access the applicable Education. Ordering Activity acknowledges that CA reserves the right to refuse entry or access to any individual that cannot authenticate their registration or authorization for such Education.

4. FEES AND CANCELLATION

4.1. The Parties acknowlede and agree that all terms governing the fees, payments, payment schedules, pricing and discounts for the applicable CA Offering procured by Ordering Activity under this Agreement are and shall be between solely Ordering Activity and their chosen Authorized CA Partner or Prime Contractor.

4.2. If CA cancels a class due to unforeseen circumstances, or low enrollment, CA will provide as much advance notice as possible but no less than ten (10) business days prior to the class in which case Ordering Activity may reschedule the class to an alternative time.

4.3. Cancellation in writing by Ordering Activity must be provided at least ten (10) business days prior to the class. If such notice is not given CA may charge Authorized CA Partner up to 100% of the fees for the class. If fees are pre-paid, no refund will be provided to the Authorized CA Partner

4.4. Neither party shall be liable for any travel related fees or expenses incurred by the other party in relation to Education which such party has properly cancelled in compliance with this section.

5. INTELLECTUAL PROPERTY RIGHTS

5.1. CA grants to Ordering Activity, a non-exclusive, non-transferable license to use the Course Materials for the internal use of the Ordering Activity, but limited to the specific Attendees and subject to terms of the Agreement. Ordering Activity shall be responsible for all use of the Education and Course Materials by its Attendees.

6. WARRANTY

6.1. If CA provides an instructor, the delivery of the Course Offering shall be provided in a professional, workman-like manner.

6.2. EXCEPT AS SET FORTH IN THIS SECTION, NO OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THIRD PARTY WARRANTIES, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR SUITABILITY AND/OR THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE ARE MADE BY CA.

7. WARRANTY REMEDY

7.1. In the event of a breach of the Warranty section, Ordering Activity's remedy shall be, at CA's discretion and in consultation with Ordering Activity, to re-perform the Education at no additional charge to the Ordering Activity. These remedies are contingent upon the alleged breach not resulting from Ordering Activity's failure to abide by its obligations or to conform to the Course Materials.

8. GENERAL TERMS

Any conflict or inconsistency among or between the terms and conditions of the documents comprising the Agreement shall be resolved according to the following order of precedence, in the order of the greatest control to the least: (1) U.S. Federal law, (2) this Channel Education Module and (3) the Channel Foundation Agreement. Notwithstanding the foregoing, unless expressly required by U.S. Federal law in subcontracts for commercial information technology, neither an Ordering Activity issued purchase order, nor the terms of an order between Ordering Activity and the Authorized CA Partner or Prime Contractor, shall modify the terms of the documents indicated herein.

1. INTRODUCTION

1.1. This Module for CA Software ("Software Module") specifies terms and conditions which apply to CA Software that CA will license to Ordering Activity and the Support that applies.

1.2. This Software Module incorporates by reference the terms of the Foundation Agreement. Any capitalized terms used in this Software Module shall have the meanings given in the Foundation Agreement unless otherwise provided herein.

2. DEFINITION

2.1. "Access" means use of CA Software remotely by an Authorized End User.

2.2. "Authorized End Users" means Ordering Activity as well as its employees and support contractors (but excluding any outsourcer, facilities management providers, managed service provider, or application service provider) that are bound by terms and conditions no less restrictive than those contained herein and are acting on behalf of Ordering Activity and not a third party.

2.3. "Authorized Use Limitation" means the quantity of the CA Software authorized by CA in accordance with the License Metric specified in the order between CA and the Authorized CA Partner.

2.4. "CA Software" means the computer software programs, either provided individually or packaged as a software appliance, made generally available and licensed to a Ordering Activity under this Module, including all Versions, Releases, provided as part of Support if applicable.

2.5. "Distributed" means the CA Software designated as distributed that is generally used for indepedent usage across individuals systems or hardware based on the Licensed Metric in a decentralized form of computing.

2.6. "Mainframe" means CA Software designated as mainframe that is generally used for a large capacity processor that provides links to users through less powerful devices such as workstations or terminals based on the Licensed Metric in a centralized form of computing.

2.7. "Maintenance" means the provision of new Releases made available while on active Support or new Versions if applicable to the generally available CA Software licensed by Ordering Activity.

2.8. "Perpetual License" means a license to use CA Software for an indefinite period subject to compliance with the Agreement.

2.9. "Release" means a general available release of a CA software product, which may contain minor new software product functionality, code, or compatibility and incorporates all previous fixes (if any exist) since the last Version. Typically, a Release requires a new installation, rather than an overlay to the already installed software. Unless otherwise specified by CA for a particular product, a Release is tied to the preceding Version and is typically designated by a number to the right of the decimal point such as 1.1, 1.2, 1.3, etc.

2.10. "Subscription" or "UMF" (Usage and Maintenance Fee) license means a license to use CA Software for a specific period of time which shall include Support unless otherwise specified by CA in its order with the Authorized CA Partner.

2.11. "Support" means the provision of technical support and Maintenance provided for a particular CA Software as specified in the Authorized CA Partner's order with CA.

2.12. "Territory" is the location where Ordering Activity is authorized to install the CA Software as specified in the Authorized CA Partner's order with CA or the Prime Contractor.

2.13. "Version" means a release of a CA Software Product that contains major changes in software product functionality, code, or compatibility and incorporates the previous release (if one has occurred), fixes and service Packs (if they have occurred). Typically, a Version requires a new installation, rather than an overlay to the already installed software. Unless otherwise specified by CA for a particular product, a Version is designated by the number to the left of the decimal point such as 1.0, 2.0, 3.0, etc.

3. SOFTWARE OFFERING & OBLIGATIONS

3.1. CA grants the Ordering Activity a limited, non-exclusive, non-transferable license, for the Term:

3.1.1. install and deploy the CA Software in the Territory up to the Authorised Use Limitation.

3.1.2. permit its Authorized End Users Access to the CA Software for Ordering Activity's and Affiliates' internal business wherever located. Ordering Activity hereby expressly agrees that a breach by an Authorized End User of the Agreement shall be considered to be a breach by and the responsibility of the Ordering Activity.

3.1.3. make a reasonable number of copies of the CA Software for disaster recovery "cold standby", backup and archival purposes. Use of such copies is limited to testing Ordering Activity's disaster recovery procedures and effectiveness and as is necessary during any reasonable period subsequent to the occurrence of an actual disaster during which Ordering Activity cannot operate the CA Software.

3.1.4. relocate CA Software to a new Ordering Activity location within the Territory upon prior written notice.

3.2. The specifications and specified operating environment information of the CA Software may be found in the Documentation accompanying the CA Software, if available (e.g., a user manual, user guide, or readme.txt or notice.txt file).

3.3. Upon request by CA, Ordering Activity agrees to provide records reasonably requested by CA to verify its compliance with the Authorized Use Limitation during the period in which Ordering Activity is licensed to use the CA Software and for a period of twelve (12) months after expiration including certified copies of statements or records as applicable. Such reports will be based on the License Metric for the CA Software ordered for Customer by CA.

3.4. The grant of license is contingent upon Ordering Activity's compliance with the following obligations set out under this provision: Ordering Activity agrees, that it shall not: (i) access or use any portion of the CA Software not expressly authorized by CA or the Documentation of the CA Software; (ii) cause or permit de-compilation, reverse engineering, or otherwise translate all or any portion of the CA Software; (iii) modify, unbundle, or create derivative works of the CA Software and/or Documentation; (iv) rent, sell, lease, assign, transfer or sublicense the CA Software or use the CA Software to provide hosting, service bureau, on demand or outsourcing services for the benefit of a third party; (v) remove any proprietary notices, labels, or marks on or in any copy of the CA Software or Documentation; (vi) use the CA Software beyond the Authorized Use Limitation.

3.5. CA reserves the right, on reasonable notice to the Ordering Activity and subject to any security measures the Ordering Activity deems appropriate, to conduct an audit remotely or onsite of Ordering Activity and/or its Affiliates facilities to verify Ordering Activity's compliance with the terms of the Agreement. CA agrees that such audit shall be conducted during regular business hours at Ordering Activity's offices and CA shall endeavor to conduct such audit so as not to interfere unreasonably with Ordering Activity's activities and/or use an independent third party to conduct the audit subject to terms of non-disclosure if required.

3.6. All rights not specifically granted hereunder are expressly reserved.

4. SUPPORT OFFERING

4.1. If Support is purchased by Ordering Activity, CA will provide Ordering Activity with technical support for the CA Software, according to the Support specified in the Authorized CA Partner's order with CA, to operate according to the Documentation, help desk support and Maintenance for the CA Software based on Support guidelines as described on http://www.support.ca.com.

4.2. In order to initiate an issue, Ordering Activity will provide CA sufficient information so that CA can provide assistance to Ordering Activity in a timely manner.

4.3. CA will provide a minimum of twelve months prior written notice to Ordering Activity if CA ceases to provide new Versions or Releases for a CA Software product.

4.4. CA will renew Support for Ordering Activity's use of the CA Software upon its acceptance of an order with an Authorized CA Partner for such Support.

5. THIRD PARTY TERMS

The CA Software may contain third-party software components. Ordering Activities are advised to review any additional terms, notices, and/or information applicable to third-party software components, which are available at https://support.ca.com/prodinfo/tpterms.

6. PERFORMANCE WARRANTY

6.1. For Distributed Software. CA warrants that the CA Software will operate materially in accordance with the applicable specifications set forth within the Documentation for a period of ninety (90) days after delivery of the CA Software to Ordering Activity subject to Ordering Activity's compliance with the Agreement.

6.2. For Mainframe Software. CA warrants that the Mainframe Software will operate materially in accordance with the applicable specifications set forth within the Documentation for the Term, subject to Ordering Activity's compliance with the Agreement.

7. PERFORMANCE WARRANTY REMEDY

7.1. If CA has breached either warranty set forth in the section entitled: Performance Warranty, Ordering Activity's remedy is for CA to, in consultation with Ordering Activity, to either (i) use reasonable efforts consistent with industry standards to cure the defect, or (ii) replace the CA Software(s) with one that materially complies with the Documentation, or (iii) mutually agree to terminate the license

and provide a pro-rata refund to the Authorized CA Partner of the license fees paid and or Support fees. If option (iii) applies, the pro-rata refund shall be calculated on the number of months left remaining on the Term of the applicable Transaction Document or if the CA Software is licensed under a Perpetual License, using (only for purposes of a refund calculation) an amortization schedule of three (3) years.

7.2. Warranty remedies are conditioned upon (i) any error or defect complained of is reasonably reproducible by CA, (ii) the CA Software is not modified and is being used in accordance with CA Documentation, and (iii) the breach is not attributable in whole or in part to any non-CA product(s) or service(s).

7.3. **THE ABOVE WARRANTIES ARE THE SOLE WARRANTIES PROVIDED BY CA. NO OTHER WARRANTIES, INCLUDING THAT THE CA SOFTWARE IS ERROR FREE, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NONINFRINGEMENT, OR SUITABILITY AND/OR THE WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE ARE MADE BY CA.**

8. ACCEPTANCE

8.1 All CA Software is deemed accepted upon issuance of an order to CA from CA Authorized Partner.

9. VIRTUALIZATION

When CA Software is used on multiple machines (physical and "virtual"), each such use of the CA Software shall be counted for the purposes of determining the Authorized Use Limitation for that CA Software. A "virtual" PC or server environment is created where Virtual Machine Technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously.

10. NEW PRODUCT LANGUAGE AND DISTRIBUTED CA SOFTWARE EXCLUSION

10.1 In addition to and separate from unspecified upgrades and enhancements to be provided as maintenance under the initial Term specified in the order with Authorized CA Partner (together with any extension(s) or renewal(s) thereof, the "Term" for purposes of this section), in the event CA develops a new release of a mainframe CA Software that it designates and makes generally available as a new product (typically containing new functions in addition to or different from existing functionality (a "New Product"), then upon CA's receipt of Ordering Activity's written request and without additional charge, such currently unspecified mainframe New Product shall be made available for use by the Ordering Activity during the Term, on the same basis as applies to such mainframe CA Software, even if CA then determines to charge a separate license fee for the mainframe New Product to CA's other licensees.

10.2 Such rights shall not extend to any Hardware provided under this Agreement. Notwithstanding anything to the contrary in the Agreement by and between the parties hereto (i) the Distributed CA Software herein shall not be construed as a "New Product" for the purposes of any prior agreement between the parties; and (ii) the provisions of any "New Product" provision in any prior agreement shall not apply to the distributed CA Software herein or any subsequent license for CA Software.

11. NIMSOFT ON PREMISE

11.1. **The following terms are modified or added for all Nimsoft transactions to the extent consistent with U.S. Federal law:**

11.1.1. **Section 2.4**: "Nimsoft Software" means the computer software programs, made generally available and licensed to a Ordering Activity under this Module, including all Versions, Releases, provided as part of Support if applicable."

11.1.2. **Section 4.1: "**If Support is purchased by Ordering Activity, CA will provide Ordering Activity with technical support for the Nimsoft Software, according to the Support specified in the Authorized CA Partner's order with CA, to operate according to the Documentation, help desk support and Maintenance for the Nimsoft Software pursuant to the following: http://www.nimsoft.com/content/dam/nimsoft/documents/un-secure/agreements/nimsoft-us-support-agreement.pdf."

11.1.3. **Add as Section 15: "15. REPORTS.** Ordering Activity agrees to prepare and submit monthly reports to the CA Authorized Reseller and CA that shall include, without limitation, information detailing the use of the Nimsoft Software pursuant to the license metrics applicable to the Software ("Report"). Ordering Activity shall submit each Report to CA Authorized Reseller and CA on the fifteenth day of each calendar month."

11.1.4. **Add as Section 16: "16. OVERAGE**. If the Report shows the Ordering Activity has exceeded the Authorized Use Limitation at any time during a month, such Report shall constitute the basis for a claim to the relevant Contracting Officer pursuant to the Contract Disputes Act and FAR 52.233-1. In no event may the Perpetual License or Subscription License quantity be lowered below the original number ordered."

12. GENERAL TERMS

12.1. Any conflict or inconsistency among or between the terms and conditions of the documents comprising the Agreement shall be resolved according to the following order of precedence, in the order of the greatest control to the least: (1) U.S. Federal law, (2) this

Channel Software Module and (3) the Channel Foundation Agreement. Notwithstanding the foregoing, unless expressly required by U.S. Federal law in subcontracts for commercial information technology, neither an Ordering Activity issued purchase order, nor the terms of an order between Ordering Activity and the Authorized CA Partner or Prime Contractor, shall modify the terms of the documents indicated herein.

Attachment A to Channel Software Module
Definitions and License Metrics

APPLICABILITY

The following definitions and License Metrics shall apply to the CA Software licensed by Ordering Activity to the extent such terms and/or CA Software are included in Ordering Activity's agreement with Authorized CA Partner or Prime Contractor:

Arcot

"Tier Servers" means single server of any tier up to and including Tier 9 Server. "Server" shall designate a specialized computer or a serial of processors assigned to store and to distribute information to and from Customer's personal computer (workstations). Linked to a company network, it enables a shared access to the files and a printing service support. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis.

CA Access Control Premium Edition

"Managed Device" means a virtual or physical machine to which the CA Software controls access.

CA Access Control Privileged User Password Management (PUPM)

"Managed Device" means a virtual or physical system or application whose privileged account passwords are being managed by the CA Software, including but not limited to operating system instances, databases, applications, Command Line Interface Software Development Kits, Open Database Connectivity/Java Database Connectivity applications, Windows services and managed tasks, and managed configuration files. When CA Software is used (i) in connection with a Managed Device or (ii) in connection with a virtual or physical system or application that leverages or interoperates with a Managed Device (a "Password Consumer System or Application"), each such use of the CA Software shall be counted for the purposes of determining the Authorized Use Limitation.

CA Automation Suite for Data Centers

A "Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores. CA Configuration Automation program is included in the delivery of CA Automation Suite for Data Centers for use in server environments managed under CA Automation Suite for Data Centers license. Use of this program with server environments not managed by CA Automation Suite for Data Centers requires a separate license for additional fees. Systems Performance for Infrastructure Manager (SystemEDGE) and Virtual Assurance for Infrastructure Manager AIMS components are included in the delivery of the CA Automation Suite for Data Centers for use only with this product. Use of these components with other CA products requires a separate license for additional fees.CA IT Client Management solution consists of CA Software Delivery, CA Asset Management, CA Remote Control programs and is included in the delivery of the CA Automation Suite for Data Centers. Customer may only use these components to manage server class machines, including virtual machines. Use of these programs for managing desktops, laptops and other client devices requires separate licenses for additional fees.CA Asset Intelligence and CA Patch Manager programs are included in the delivery of the CA Automation Suite for Data Centers. Customer may only use these components to manage server class machines, including virtual machines. Use of these programs for managing desktops, laptops and other client devices requires separate licenses for additional fees.CA Process Automation program is included in the delivery of CA Automation Suite for Data Centers. CA Process Automation includes two Orchestrators, all non-Premium Connectors, unlimited Agents and 75 Concurrent Processes per Orchestrator. Additional Orchestrators and Premium Connectors are available as an add-on option at additional cost. "Agent" means a single installation of the agent software component of the CA Process Automation program on a specific operating system which can be identified as unique host identification on a physical or virtual hardware server. "Orchestrator" means a single installation of the Orchestrator software component of the CA Process Automation program on a specific operating system which can be identified as unique host identification on a physical or virtual hardware server. This installation can be a stand-alone Orchestrator or as a node of a new or existing clustered Orchestrator. "Connector" is the software program connecting the CA Process Automation program with specific named third party software or other CA software. For example, CA Process Automation Connector For CA Service Desk connects CA Process Automation with CA Service Desk. Each Connector may only be used to connect the CA Software with the specific named third party software or CA software program. "Premium Connector" means a Connector identified by CA in the Order Form. "Process instance" means a single copy of a Process definition that has been scheduled to run (Queued state), is running (Running state), or has completed running (Failed or Completed state) on a particular "Orchestrator".



"Concurrent Processes" means the number of CA Process Automation Process instances that are marked in the Running state within an Orchestrator at any given time.

CA AutoSys Workload Automation

"Instance" means the number of copies of CA AutoSys Workload Automation installed in your physical and/or virtual environment.

CA Clarity Project & Portfolio Manager

"CA Software" means the CA Clarity Project and Portfolio Manager (also known as CA Clarity PPM). CA Clarity PPM is licensed by Environment and the number of Users (Manager, Team Member or Viewer). Customer is granted the right to install and use CA Clarity PPM in not more than three (3) Environments, of which only one (1) may be a production Environment. An "Environment" can consist of any or all of the following, provided that all of the servers in the Environment function as one logical Environment: one or more application servers, search servers, report servers, background servers, and/or database servers. Typical examples of Environments include production Environments, development Environments and test Environments. A production Environment is a computer system used to process an organization's daily work on a real-time operation, not systems used only for development and testing. "Manager User" means Customer's designated users who have full use of and access to the functions within CA Clarity PPM. "Team Member User" means Customer's designated users who have limited rights to the functions within CA Clarity PPM, and may only (i) view data and run reports in all licensed products; (ii) collaboratively participate in processes, discussions and document sharing and receive notifications in all licensed products; (iii) view project tasks and calendars, and report and approve time and project status; and (iv) enter and view status of ideas. "View Only User" means Customer's designated users who have limited rights to the functions within CA Clarity PPM and may only (i) view data and run reports; (ii) originate idea workflows, and participate in the continuation of those workflows.

CA Client Automation

A "Managed System" is any physical or virtual computer system that can host an operating system, including, but not limited to, a desktop computer or laptop computer, used by an end-user as part of their job function to access data, applications and resources, that is administered or managed by CA Client Automation by way of a management infrastructure, whether a CA management agent resides on the system or not. This includes laptops, desktops and virtual desktops running Windows, Macintosh and Linux operating systems, and it excludes Windows Servers, Linux Servers and UNIX systems. The management infrastructure components, such as Domain Manager, Scalability Server, and System Engine, that run on server platforms do not require a separate license, except if these systems themselves are being managed by an active agent for purposes other than serving as the CA Client Automation management infrastructure.

CA Client Automation consists of:
CA IT Client Manager
CA Patch Manager
CA Desktop Migration Manager
CA Asset Intelligence
CA Workflow for CA IT Client Manager (it is included in the delivery of CA Client Automation for use only for automating workflows inside CA Client Automation and between CA Client Automation and other software programs)

CA Configuration Automation:

The CA Software is licensed by the number of Physical Sockets. A "Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

CA Database Performance

CA Database Performance is licensed by the number of CPUs when used as a distributed product. "CPU" means a central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A dual-core central processing unit is considered a single CPU. Note that because of the use of multi-core CPUs and virtual server environments, the calculation of CPUs for licensing purposes described below will not always equate to the number of physical CPUs in the environment. A virtual server environment is created where virtual machine technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously. With the Authorized Use Limitation as "CPU" or "Processor", the calculation with respect to the number of CPUs on an individual server is determined as follows:

1. For non-virtual server environments, for any server with databases monitored by the CA Software with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with databases monitored by the CA Software with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number.

2. For virtual server environments, for any server with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number. Determine the maximum percentage of the server CPU capacity that is allocated by the Virtual Machine Technology to any operating system instance containing databases(s) monitored by the CA Software, and multiply this percentage by the number of CPUs. Multiply the resulting number by one and a half (1.5X) and round up to the next whole number.

3. For mixed server environments, for each server perform the calculations for CPUs as set forth above in subparagraphs (1) and (2) and add these amounts together to determine the aggregate number of CPUs.

CA Systems Performance for Infrastructure Managers (formerly known as "CA SystemEdge") is a separate program included in the delivery of CA Database Performance. Customers can use this program only for communication with other CA Technologies tools and/or monitoring CA Technologies software systems only. Full functionality of the program to monitor and manage servers requires a separate license with additional fees.

CA DLP

CA DLP includes CA DLP Enterprise Suite, CA DLP Platform & Surveillance, CA DLP Endpoint, CA DLP Stored Data, CA DLP Message Server and CA DLP Network. CA DLP Network and CA DLP Enterprise Suite (which includes CA DLP Network) require and may only be used on a licensed CA DLP Network Appliance.

"CA DLP Network Appliance" means the hardware that operates the CA DLP Network. "User" means a single person, or identity, listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless specified on the Order Form, a User shall not be counted more than once or a concurrent basis. If an Appliance is included with the CA Software, Support for an Appliance is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com.

CA Enterprise Log Manager

"Agent" means a single installation of the agent software on a specific operating system instance which can be identified as a unique host identification on a hardware server. A hardware server may have multiple operating system instances installed on it (through partitioning or virtualization). Each instance of the operating system on a partitioned/virtualized server must license an agent if required for job scheduling purposes. "Node" means, in a communications system, a network junction or connection point. Any system or device connected to a network is also called a node or cluster. "Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA ESP Workload Automation
(MIPS Based license. Operating System is IBM z/OS)

CA ESP Workload Automation is licensed by the specified number of MIPS (the "Authorized Use Limitation in MIPS"). "MIPS" means millions of instructions per second. The MIPS capacity of a computer shall be calculated by reference to CA's published schedules of the MIPS capacity and if a computer isn't listed then the manufacturer's published specifications should apply. In the event that any particular computer is not accounted for on CA's schedule, the manufacturer's published specification of MIPS capacity shall control. Further, in the event a special purpose processor, designed to perform one or more dedicated functions, is being used as a general purpose processor, CA shall treat such processor as a general purpose processor for purposes of calculating Authorized Use Limitation in MIPS. "Customer Site" means the site(s) specified at the time of licensing the CA Software or the Customer Address if no Customer Site has been indicated. Customer may use the CA Software only on the specific computers upon which the CA Software is installed to run at the Customer Site or on computers which are linked, connected to and/or which can remotely access such computers, irrespective of the platform designations of the hardware or operating systems, provided that such computer is capable of accessing, using, executing or benefiting from the CA Software, subject to the aggregate MIPS capacity not exceeding the Authorized Use Limitation in MIPS.

CA Fast Unload for Distributed Databases:

The CA Software is licensed by the number of servers. "Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA Federation Manager:

(a) "Federate" means to link or bind two or more entities together, enabling identity, account, attribute, authentication, and authorization federation across different trust realms.
(b) "Federation" means a relationship or an association between a specific system entity's identified users, partners or accounts.
(c) "Federation Partner" means an internal or external entity (i) for which a unique federation configuration is required in order to join a Federation, and (ii) with whom Customer interoperates using Federation Manager, with or without SAML AA.
(d) "Federation Partnership Licensee" means the Federation Partner designated by Customer as licensed to use SAML AA or Federation Manager in accordance with the provisions of the Agreement and who has agreed in writing to Customer terms and conditions substantially similar to the Federation Manager and SAML AA license provisions contained herein, as well as the confidentiality provisions contained in the Agreement. Such Federation Partnership Licensee shall not have any right to further copy, distribute, or otherwise transfer such software or any rights therein, notwithstanding any provision of the Agreement to the contrary. With regard solely to such Federation Partner's use of the Licensed Programs in accordance herewith, the term "Customer" in the Agreement includes such Federation Partner.
(e) "Federation User" means any user who is allowed to use a Federation via the specific configuration of Federation Manager that Customer deploys. A Federation User shall not be counted more than once or on a concurrent basis.

CA GEN ENC Cross-Gen Opt Linux

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. "Non Tier Servers" means single server of any tier up to and including Tier 9 Server.

CA GEN Implementation Toolset

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. "Non Tier Servers" means single server of any tier up to and including Tier 9 Server.

CA GEN TRANSACTION Enabler

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. "Non Tier Servers" means single server of any tier up to and including Tier 9 Server.

CA GEN TRANSACTION Enabler User Fnl

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. "Non Tier Servers" means single server of any tier up to and including Tier 9 Server.

CA GEN WRKSTN Cross-Gen Linux

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and whichis owned, leased or otherwise controlled by Customer. "User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. "Non Tier Servers" means single server of any tier up to and including Tier 9 Server.

CA Identity Manager

"User" means a single person listed in any Customer directory or network storage location whose access and use rights canbe authenticated, authorized, or administered by CA Identity Manager. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. "Internal User" is an intranet User defined as an employee or contractor of the Customer. CAIdentity Manager may be used for Customer's internal use only, by the Internal Users on Customer's local area network and client/server system or a HTTP-based Web server infrastructure. Internal Users licensed hereunder may not be aggregated by a Customer contractor withany users of CA Identity Manager separately licensed by such contractor. "External User" is either an extranet or internet User defined as an employee of Customer's authorized third parties, which may be Customer's customers, clients, or consumers, on internet website(s) owned by, or under the control of, Customer. External Users licensed hereunder may not be aggregated by a Customer's vendor or business partner with any Users of CA Identity Manager separately licensed by such vendor orpartner.

CA Infrastructure Insight

"Device" means a network-connected device that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, physical servers, single-flow interfaces, andphysical machines, but excluding endpoint devices such as IP telephones. When the Authorized Use Limitation is "Device", the calculation with respect to the number of Licenses is determined asfollows:

a. For network-connected devices, for any device with up to five (5) IPflow interfaces, count the number of devices. For any device with greater than five (5) IPflow interfaces, count the total number of IPflow interfaces. Divide the number of IPflow interfaces by five (5) and round up to the next whole number.

b. For network-connected devices, for any device with up to two hundred (200) ports, count the number of devices. For any device with greater than two hundred (200) ports, count the total number of ports. Divide the number of ports by two hundred (200) and round up to the next whole number.

For avoidance of doubt, when a single network-connected device, has greater than five (5) IPflow interfaces and greater than two hundred (200) ports, the device is included in the license count that results in the highest number of licenses. For example, a device with fifty (50) IPflow interfaces and six hundred (600) ports would be included in the license count based upon the number of IPflow interfaces (50/5 = 10 licenses while 600/200 = 3 licenses).

CA Infrastructure Insight consists of CA Spectrum Infrastructure Manager and CA NetQoS ReporterAnalyzer.

CA Database Performance is included in the delivery of CA Infrastructure Insight for use only for monitoring the databases included in CA Infrastructure Insight. Full functionality of CA Database Performance to monitor other databases requires a separate license for additional fees.

CA Systems Performance for Infrastructure Managers is included in the delivery of CA Infrastructure Insight for use only for provisioning and performance monitoring of the systems that are running CA Infrastructure Insight. Full functionality of CA Systems Performance for Infrastructure Managers requires a separate license for additionalfees.

If an Appliance is included with the CA Software, Support for a CA-provided physical server platform hardware appliance which is bundled with and used to operate one or more pre-installed licensed CA software products is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com.

CA Infrastructure Management

"Device" means a network-connected device that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, physical servers, single-flow interfaces, andphysical machines, but excluding endpoint devices such as IP telephones. When the Authorized Use Limitation is "Device", the calculation with respect to the number of Licenses is determined asfollows:

a. For network-connected devices, for any device with up to five (5) IPflow interfaces, count the number of devices. For any device with greater than five (5) IPflow interfaces, count the total number of IPflow interfaces. Divide the number of IPflow interfaces by five (5) and round up to the next whole number.

b. For network-connected devices, for any device with up to two hundred (200) ports, count the number of devices. For any device with greater than two hundred (200) ports, count the total number of ports. Divide the number of ports by two hundred (200) and round up to the next whole number.

For avoidance of doubt, when a single network-connected device, has greater than five (5) IPflow interfaces and greater than two hundred (200) ports, the device is included in the license count that results in the highest number of licenses. For example, a device with fifty (50) IPflow interfaces and six hundred (600) ports would be included in the license count based upon the number of IPflow interfaces (50/5 = 10 licenses while 600/200 = 3 licenses).

CA Infrastructure Management consists of CA Spectrum Infrastructure Manager, CA eHealth Performance Manager and CA NetQoS ReporterAnalyzer.

CA Database Performance is included in the delivery of CA Infrastructure Management for use only for monitoring the databases included in CA Infrastructure Management. Full functionality of CA Database Performance to monitor other databases requires a separate license for additional fees.

CA Systems Performance for Infrastructure Managers is included in the delivery of CA Infrastructure Management for use only for provisioning and performance monitoring of the systems that are running CA Infrastructure Management. Full functionality of CA Systems Performance for Infrastructure Managers requires a separate license for additional fees.

If an Appliance is included with the CA Software, Support for a CA-provided physical server platform hardware appliance which is bundled with and used to operate one or more pre-installed licensed CA software products is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com.

CA Infrastructure Performance

"Device" means a network-connected device that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, physical servers, single-flow interfaces, and physical machines, but excluding endpoint devices such as IP telephones. When the Authorized Use Limitation is "Device", the calculation with respect to the number of Licenses is determined as follows:

a. For network-connected devices, for any device with up to five (5) IPflow interfaces, count the number of devices. For any device with greater than five (5) IPflow interfaces, count the total number of IPflow interfaces. Divide the number of IPflow interfaces by five (5) and round up to the next whole number.

b. For network-connected devices, for any device with up to two hundred (200) ports, count the number of devices. For any device with greater than two hundred (200) ports, count the total number of ports. Divide the number of ports by two hundred (200) and round up to the next whole number.

For avoidance of doubt, when a single network-connected device, has greater than five (5) IPflow interfaces and greater than two hundred (200) ports, the device is included in the license count that results in the highest number of licenses. For example, a device with fifty (50) IPflow interfaces and six hundred (600) ports would be included in the license count based upon the number of IPflow interfaces (50/5 = 10 licenses while 600/200 = 3 licenses).

CA Infrastructure Performance consists of CA eHealth Performance Manager and CA NetQoS ReporterAnalyzer.

CA Database Performance is included in the delivery of CA Infrastructure Performance for use only for monitoring the databases included in CA Infrastructure Performance. Full functionality of CA Database Performance to monitor other databases requires a separate license for additional fees.

CA Systems Performance for Infrastructure Managers is included in the delivery of CA Infrastructure Performance for use only for provisioning and performance monitoring of the systems that are running CA Infrastructure Performance. Full functionality of CA Systems Performance for Infrastructure Managers requires a separate license for additional fees.

If an Appliance is included with the CA Software, Support for a CA-provided physical server platform hardware appliance which is bundled with and used to operate one or more pre-installed licensed CA software products is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com.

CA Insight Database Performance Manager

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.CA Systems Performance for Infrastructure Managers (formerly known as "CA System Edge") Limited Use, is a separate program included in the delivery of CA Insight Database Performance Manager. The customers can use this program only for communication with other CA Technologies tools and/or monitoring CA Technologies Software systems only. Full functionality of the program to monitor and manage servers requires a separate license with additional fees.

CA IT Asset Manager

"CA Software" means the CA IT Asset Manager and CA Software Compliance Manager. A "Managed System" is any physical or virtual desktop, laptop, server, and tablet computer that may be tracked and/or managed by the CA Software, based upon user-supplied unique designations to identify such computers, regardless of use purpose including non-production, spares, or disaster recovery. If the optional component CA Software Compliance Content Subscription is listed on the applicable Order Form, Customer is granted a term license to use such content with CA Software Compliance Manager or CA IT Asset Manager beginning on the Term Start Date and ending on the Term End Date. The subscription fees for CA Software Compliance Content Subscription include the right to receive content updates during the Term of the content subscription. Such license for CA Software Compliance Content Subscription shall renew at the option of the Ordering Activity and be extended for successive periods equivalent to the original subscription Term, subject to the parties' agreement concerning fees to be paid during each such extended term. Use of the CA Software is limited as to several components included unless separately licensed. Software technology for Software Distribution, Remote Control and Asset Discovery and Inventory (CA IT Client Management) are included with CA Software Compliance Manager and CA IT Asset Manager, however the only authorized use is the ability to import Microsoft SMS 2003 or Microsoft SystemCenter Configuration Manager 2007 through the CA Asset Converter for Microsoft SMS, importing inventory from other third party discovery tools using the Asset Collector technology and CA IT Client Manager technology. Explicitly, Customer is not licensed to use the software distribution, remote control technologies as well as the full asset inventory and discovery agents. Use of the CA Software or CA Software Compliance Content Subscription is not a substitute for Customer's compliance with any laws (including but not limited to any act, statute, regulation, requirement, rule, standard, directive, administrative order, executive order, etc. (collectively, "Laws")). Customer should consult with competent legal counsel regarding any such Laws. Use of the CA Software or CA Software Compliance Content Subscription is not a substitute for Customer's compliance with its contractual obligations. The CA Software and CA Software Compliance Content Subscription require Customer to (i) manually or electronically enter or (ii) make decisions regarding software license data and other information for purposes of tracking authorized use, compliance with its software license contractual obligations and other information ("Data Entry"). Notwithstanding the provisions of any warranty to the contrary, CA makes no warranty with respect to the CA Software or CA Software Compliance Content Subscription failure, error, omission or inaccuracy to the extent that any such failure, error, omission or inaccuracy relates, in whole or in part, to Data Entry errors, omissions, decisions, inaccuracies, misinterpretations or otherwise.

CA IT Client Manager

"Managed System" is any physical or virtual computer system that can host an operating system, including, but not limited to, a desktop computer, server, or laptop computer, that is administered or managed by the CA Software (IT Client Manager / IT Inventory Manager) by way of a CA management agent, whether it resides on the asset or not. A "Non-CA managed system" has their inventory gathered by a non-CA management agent; however, the information about that asset is still stored in the Management Database (MDB). This asset information may have been obtained using the SMS Connector or Asset Collector. If Customer is licensed for CA IT Client Manager Patch Subscription, Customer is granted a term license to use such program with CA IT Client Manager beginning on the Term Start Date and ending on the End Date for the subscription term. The term license for the CA IT Client Manager Patch Subscription shall renew at the Ordering Activity's option and be extended for successive periods equivalent to the original term, subject to the parties' agreement concerning fees to be paid during each extended term.

CA Mainframe for IBM Rational Developer for System z Unit Test (CA Mainframe Suite for RDz UT):

a) Additional license rights to the CA software program(s) referenced below ("CA Software") are provided under the following terms and conditions in addition to any terms and conditions referenced (i) on the Order Form entered into by you and the CA entity ("CA") through which you obtained a license for the CA Software and (ii) in the software license agreement between you and CA for the CA Software. These terms shall be effective from the effective date of the Order Form.

b) **Program Name:** CA Mainframe Suite for IBM Rational Developer for System z Unit Test ("RDz UT")

c) **Specified Operating Environment**

The license rights set forth herein apply only to CA Software separately licensed from CA for the z/OS environment and for use hereunder only in the IBM RDz UT environment.

d) **CA Software**

CA Software for IBM RDz UT Environment:

CA 1™ Tape Management, CA TLMS® Tape Management
CA ACF2™, CA ACF2™ Option for DB2
CA Aion® Business Rules Expert
CA Auditor for z/OS, CA Cleanup
CA Bundl®
CA Cleanup
CA Compliance Manager for z/OS
CA Database Management for DB2 for z/OS
CA Database Management for IMS for z/OS
CA Datacom®
CA Deliver™
CA Disk™ Backup and Restore
CA Dispatch™
CA Easytrieve®
CA Endevor® Software Change Manager
CA FileMaster™ Plus, CA FileMaster™ Plus IMS
CA Gen
CA Gener/OL
CA IDMS™
CA InterTest™ for CICS, CA InterTest™ Batch
CA JCLCheck™ Workload Automation
CA JobTrac™ Job Management
CA Librarian®
CA Mainframe Application Tuner
CA Mainframe Software Manager™
CA NetMaster® File Transfer Management, CA NetMaster® Network Automation, CA NetMaster® Network Management for SNA, CA NetMaster® Network Management for TCP IP
CA Optimizer®/II
CA Panvalet®
CA Roscoe®

CA Scheduler® Job Management
CA Spool™
CA SymDump® Batch, CA SymDump® for CICS
CA Telon®
CA Top Secret®, CA Top Secret® Option for DB2
CA UFO™
CA View®
CA Workload Automation CA 7® Edition, CA Workload Automation ESP Edition, CA Workload Automation Restart Option EE, CA Workload Automation Restart Option for z/OS Schedulers
CA XCOM™ Data Transport®

e) Licensing Model and Terms

The license rights set forth herein authorize you to use CA Software for which you are separately licensed only in the IBM RDz UT environment for non-production purposes. During the term of this license, you must also be licensed to use the IBM RDz UT environment. Use of the CA Software in any other environment or in the RDz UT environment for production purposes is expressly prohibited. This restriction does not change your existing license rights to use the CA Software in a production environment. A production environment is a computer system used to process an organization's daily work on a real-time operation and is not a system used only for development and testing. During the term of this license, if you license additional CA Software, the license rights granted herein apply to such subsequently licensed CA Software.

The license rights are provided on a "per Seat" basis. "Seat" means a single person or identity whose access and use rights can be authenticated, authorized, or administered, or who has the ability to view content aggregated or managed by the CA Software. In general, a Seat shall not be counted more than once or on a concurrent (logged-in) basis. One Seat license shall authorize you to use any of the CA Software for which you are separately licensed in the RDz UT environment. The term of this license (the "Term") is the lesser of: (i) one (1) year; (ii) the term end date for the applicable separately licensed CA Software; or (iii) the term end date for your use of the IBM RDz UT environment. Any termination under clauses (ii) or (iii) immediately above shall not result in refund of any license fees paid hereunder. Subject to the limitations set forth in clauses (i) (ii) and (iii) immediately above, any renewal or extension of the license term for the separately licensed CA Software or the IBM RDz UT environment, as the case may be, shall continue the Term of this agreement for the period identified above. If you have multiple CA Software products with different term end dates, the license rights granted herein terminate as to each specific CA Software product in the lesser of one (1) year or when the applicable term license for such CA Software ends. Termination of license rights hereunder shall not terminate your license to any CA Software product.

CA does not provide support for the CA Software in the RDz UT environment. Any issues with the CA Software in the RDz UT environment must be reproduced by you in the z/OS environment and reported as such through CA Technologies normal support process for the CA Software.

CA NetQoS NetVoyant

"Device" means a network-connected device that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, physical servers, single-flow interfaces, and physical machines. Endpoint devices used solely as IP telephones are not considered to be Devices, unless the CA Software is specifically licensed by the number of phones. For the purposes of CA NetQoS Unified Communication Monitor only, endpoint devices used solely as IP telephones are considered to be Devices. When the Authorized Use Limitation is "Device", the calculation with respect to the number of Licenses is determined as follows:

1. For network-connected devices, in non-virtual server environments, for any device with up to five (5) IPflow interfaces, count the number of devices. For any device with greater than five (5) IPflow interfaces, count the total number of IPflow interfaces. Divide the number of IPflow interfaces by five (5) and round up to the next whole number.

2. For network-connected devices, in non-virtual server environments, for any device with up to two hundred (200) ports, count the number of devices. For any device with greater than two hundred (200) ports, count the total number of ports. Divide the number of ports by two hundred (200) and round up to the next whole number.

For avoidance of doubt, when a single network-connected device, in non-virtual environments, has greater than five (5) IPflow interfaces and greater than two hundred (200) ports, the device is included in the license count that results in the highest number of licenses. For example, a device with fifty (50) IPflow interfaces and six hundred (600) ports would be included in the license count based upon the number of IPflow interfaces (50/5 = 10 licenses while 600/200 = 3 licenses).

CA NetQoS Reporter Analyzer

"Device" means a network-connected device that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, physical servers, single-flow interfaces, and physical machines. Endpoint devices used solely as IP telephones are not considered to be Devices, unless the CA Software is specifically licensed by the number of phones. For the purposes of CA NetQoS Unified Communication Monitor only, endpoint devices used solely as IP telephones are considered to be Devices. When the Authorized Use Limitation is "Device", the calculation with respect to the number of Licenses is determined as follows:

1. For network-connected devices, in non-virtual server environments, for any device with up to five (5) IPflow interfaces, count the number of devices. For any device with greater than five (5) IPflow interfaces, count the total number of IPflow interfaces. Divide the number of IPflow interfaces by five (5) and round up to the next whole number.

2. For network-connected devices, in non-virtual server environments, for any device with up to two hundred (200) ports, count the number of devices. For any device with greater than two hundred (200) ports, count the total number of ports. Divide the number of ports by two hundred (200) and round up to the next whole number.

For avoidance of doubt, when a single network-connected device, in non-virtual environments, has greater than five (5) IPflow interfaces and greater than two hundred (200) ports, the device is included in the license count that results in the highest number of licenses. For example, a device with fifty (50) IPflow interfaces and six hundred (600) ports would be included in the license count based upon the number of IPflow interfaces (50/5 = 10 licenses while 600/200 = 3 licenses).

CA RegFort:

CA RegFort is licensed by the number of Users or Issuance.

"User" means a single person, or identity, listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by CA RegFort or who has the ability to view content aggregated or managed by CA RegFort. In general, a user shall not be counted more than once or on a concurrent (logged-in) basis.

"Issuance" means any activity in the life cycle of a Public Key Infrastructure credential that is managed by CA RegFort, including, but not limited to, creation of a new credential, revocation, renewal, re-issue or update of the credential.

"RegFort Client" means a portion of CA RegFort which enables end-users to interface with smartcards and tokens.

Limited License Grant. In addition to the rights granted in the applicable license agreement, CA grants Customer and its affiliates a nonexclusive license to distribute RegFort Client to end-users. Customer may use Customer's logo and name with the RegFort Client. No title to or ownership of the RegFort Client is transferred to Customer.

CA RiskFort:

CA RiskFort is licensed by the number of Users.

"User" means a single person, or identity, listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by CA RiskFort or who has the ability to view content aggregated or managed by CA RiskFort. In general, a user shall not be counted more than once or on a concurrent (logged-in) basis.

CA Role and Compliance Manager

"User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. An "Internal User" is an intranet User defined as an employee or contractor of the Customer. CA Role and Compliance Manager may be used for Customer's internal use only, by the Internal Users on Customer's local area network and client/server system or a HTTP-based Web server infrastructure. Internal Users licensed hereunder may not be aggregated by a Customer contractor with any users of CA Role and Compliance Manager separately licensed by such contractor. An "External User" is either an extranet or internet User defined as an employee of Customer's authorized third parties, which may be Customer's customers, clients, or consumers, on internet website(s) owned by, or under the control of, Customer. External Users licensed hereunder may not be aggregated by a Customer's vendor or business partner with any Users of CA Role and Compliance Manager separately licensed by such vendor or partner.

CA Server Automation

"Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

CA Systems Performance for Infrastructure Manager (SystemEDGE) and CA Virtual Assurance for Infrastructure Manager AIMS components are included in the delivery of the CA Server Automation for use only with this product. Use of these components with other CA products requires a separate license for additional fees.

CA IT Client Management solution consists of CA Software Delivery, CA Asset Management, CA Remote Control programs and is included in the delivery of the CA Server Automation. Customer may only use these components to manage server class machines, including virtual machines. Use of these programs for managing desktops, laptops and other client devices requires separate licenses for additional fees.

CA Asset Intelligence and CA Patch Manager programs are included in the delivery of the CA Server Automation. Customer may only use these components to manage server class machines, including virtual machines. Use of these programs for managing desktops, laptops and other client devices requires separate licenses for additional fees.

CA Service Desk Manager

"CA Software" and "SDM" mean the CA Service Desk Manager – Analyst License, CA Service Desk Manager - Full License, or CA CMDB Manager Servers described herein in object code form. CA Service Desk Manager-Full License and CA Service Desk Manager-Analyst License are licensed on a Concurrent Analyst basis. In CA Service Desk Manager-Full License, CA Service Desk Manager-Analyst License, the authorized users are assigned various roles based upon the functions needed to accomplish designated tasks. "Concurrent Analyst", in the context of CA Service Desk Manager, means a software license that is based on the number of simultaneous (concurrent) users accessing the program. For the purpose of SDM, all roles (for example: Analyst, Manager, Administrator), and programmatic API and/or web services calls require a license. The Software does not prohibit additional users from access, but does log a license exception for auditing purposes. Customer is entitled to have the specified number of Concurrent Analysts access CA Service Desk Manager simultaneously. For CA Service Desk Manager-Full License, CA Service Desk Manager-Analyst License, You are also licensed for End-User Self-Service, which is granted to the employee and customer roles to allow for the creation, modification, and closure of a ticket on their own behalf, but not on behalf of someone else. CA Service Desk Manager-Full License includes a limited entitlement to CA Cohesion, and use of CA Cohesion is restricted to a maximum of one hundred (100) Managed Servers. Use for additional Servers requires additional licenses for CA CMDB Managed Server. CA Service Desk Manager-Analyst License does not include the CA Cohesion entitlement. CA CMDB Managed Servers is licensed by the number of Servers. "Managed Servers" means a virtual or physical Server managed by CA Software. "Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA Service Desk Manager includes a limited entitlement to CA Business Intelligence. This entitlement is restricted to use within the context of reporting for SDM only. Specifically, SDM reports created using CA Business Intelligence may access and incorporate data created by, derived from, or used by SDM or third party data sources, provided that such data facilitates or augments data for Customer's use of SDM.

CA Service Desk Manager includes a limited entitlement to CA Process Management for Workflows. This entitlement is restricted to use within the context of Workflows associated with SDM only. This entitlement includes: the Service Desk Manager connector; three (3) Custom Operators; and five (5) Agents. This entitlement does not include any Premium Connectors. Multiple Orchestrators can be deployed with the constraints specified herein. There are no license limitations on the number of concurrent processes per Orchestrator.

For the purpose of CA Process Management for Workflows, "Agent" means a single installation of the agent software component of the CA Process Management for Workflows on a specific operating system which can be identified as a unique host identification on a physical or virtual hardware server.

For the purpose of CA Process Management for Workflows, "Connector" is the software program connecting CA Process Management for Workflows with specifically named third-party software or other CA software. For example, "CA Process Management for Workflows Connector for CA Service Desk Manager" connects CA Process Management for Workflows with CA Service Desk Manager. Each Connector may only be used to connect the CA Software with the specific named third-party software or CA software program.

For the purpose of CA Process Management for Workflows, "Custom Operator" means a type of automation object within the CA Process Management for Workflows that can be created to enhance, modify, or restrict the capabilities of an existing "Connector".

For the purpose of CA Process Management for Workflows, "Orchestrator" means a single installation of the Orchestrator software component of CA Process Management for Workflows on a specific operating system which can be identified as a unique host identification on a physical or virtual hardware server. This installation can be a stand-alone Orchestrator or as a node of a new or existing clustered Orchestrator.

CA SiteMinder

"User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis. An "Internal User" is an intranet User defined as an employee or contractor of the Customer. CA SiteMinder may be used for Customer's internal use only, by the Internal Users on Customer's local area network and client/server system or a HTTP-based Web server infrastructure. Internal Users licensed hereunder may not be aggregated by a Customer contractor with any users of CA SiteMinder separately licensed by such contractor. An "External User" is either an extranet or internet User defined as an employee of Customer's authorized third parties, which may be Customer's customers, clients, or consumers, on internet website(s) owned by, or under the control of, Customer. External Users licensed hereunder may not be aggregated by a Customer's vendor or business partner with any Users of CA SiteMinder separately licensed by such vendor or partner.

CA SOA Security Manager

"Secured Web Service" means a software system designed to support interoperable machine-to-machine interaction over a network which needs to be secured from unauthorized access, software routines or components that is or are intended to disable, erase, or otherwise harm software, equipment, or data, or cause other similar damage. This web service can be a URI or web services End point defined in a WSDL file. "URI" (Uniform Resource Identifier) means a compact string of characters for identifying an abstract or physical resource. "End point" means a specific location for accessing a web service using a specific protocol and data format. "WSDL" (Web Service Definition Language) means an XML (Extensible Markup Language) format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. "User" means a single person, application or identity listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the CA Software or who has the ability to view content aggregated or managed by CA SOA Security Manager. In general, a user shall not be counted more than once or on a concurrent (logged-in) basis.

CA SOA Security Manager with Gateway

CA SOA Security Manager is licensed in number of Secured Web Services and Users. CA SOA Security Gateway is licensed in number of Instances. "Secured Web Service" means a software system designed to support interoperable machine-to-machine interaction over a network which needs to be secured from unauthorized access, software routines or components that is or are intended to disable, erase,

or otherwise harm software, equipment, or data, or cause other similar damage. This web service can be a URI or web services End point defined in a WSDL file. "URI" (Uniform Resource Identifier) means a compact string of characters for identifying an abstract or physical resource. "End point" means a specific location for accessing a web service using a specific protocol and data format. "WSDL" (Web Service Definition Language) means an XML (Extensible Markup Language) format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. "User" means a single person, application or identity listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by CA SOA Security Manager or who has the ability to view content aggregated or managed by CA SOA Security Manager. In general, a user shall not be counted more than once or on a concurrent (logged-in) basis. "Installation" means the number of copies of CA SOA Security Manager installed in the Customer's physical and/or virtual environment.

CA Spectrum Infrastructure Manager

"Managed Network Device" means a virtual or physical network-connected device with less than 200 ports that is managed by CA Spectrum Infrastructure Manager and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, virtual or physical servers, and virtual or physical machines, but excluding endpoint devices such as IP telephones.

CA Spectrum Service Assurance

"Site" or "Installation" means use of CA Spectrum Service Assurance in a data center comprised of one or more CPUs conforming to the following conditions: Two or more CPUs will be considered part of the same site if (i) the CPUs are located in a single building, (ii) each CPU shares access to data storage and peripheral devices with one or more of the other CPUs without requiring any programming interface to another CPU, and (iii) the CPUs function as a data processing facility under common data processing operations supervision. Use of CA Spectrum Service Assurance on two or more CPUs will be considered multiple and separate sites if all of the foregoing conditions of a single site are not satisfied, regardless of (i) whether they occupy different floors or locations in the same building or share the same mailing location address, or (ii) the extent to which the CPUs are integrated within a network or serve a functional role as part of a larger data processing organization. Customer is granted the right to deploy CA Spectrum Service Assurance at the Sites with the addresses listed in the Order Form. Customer may change and amend the addresses of the Sites by notice to CA providing that the total number of Sites listed does not exceed the number listed in the Order Form. "Connection" means a data source indicated by CA Spectrum Service Assurance to have a connector status of "Online". A Connection may consist of a connection to a CA Software product (i.e. CA Wily, CA Spectrum), a third party product (i.e. HPOV), or a custom application. "Data source" means any software application that provides data to CA Spectrum Service Assurance.

CA SYSVIEW for CA Wily APM

Customer is granted a limited license to use CA SYSVIEW for CA Wily APM solely for the integration with CA Wily APM or CA Wily Introscope 8.2 or above ("CA Wily"). With this license, Customer is only authorized to install, configure and use CA SYSVIEW for CA Wily APM components to support its authorized use with CA Wily to provide mainframe performance metrics to CA Wily and trace transactions tagged by CA Wily that perform activity on the mainframe. Customer may not use CA SYSVIEW for CA Wily APM for other purposes. Any additional use requires a separate non-restricted license. In the event Customer chooses to increase its Authorized Use for CA Wily, Customer must also increase its Authorized Use for CA SYSVIEW for CA Wily APM and pay all applicable additional license and maintenance fees related thereto in order to use CA SYSVIEW for CA Wily APM with such increased CA Wily capacity. Additional use of CA Wily without obtaining a separate non-restricted license may be the basis for filing a claim with the relevant Contracting Officer under the Contract Disputes Act and FAR 52.233-1.

CA TSreorg for Distributed Databases

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA Virtual Assurance

"Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

If an Appliance is included with the CA Software, Support for an Appliance is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com.

CA Virtual Automation

"Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

CA Virtual Configuration

"Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

CA Virtual Performance Management (CA VPM)

"CPU" or "Processor" means central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A Processor may not exceed a maximum of 12 processing cores.

CA WebFort:

CA WebFort is licensed by the number of User Credentials and Users.

"Credential" means an attestation of qualification, competence, or authority issued to a User by the CA Software.

"User" means a single person, or identity, listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by CA WebFort or who has the ability to view content aggregated or managed by CA WebFort. In general, a user shall not be counted more than once or on a concurrent (logged-in) basis.

"User Credentials" means the number of Credentials set forth on the Order Form to be issued to the Users who are authorized to access and use CA WebFort. Each User may have more than one credential for different verification methods.

"ArcotID Client" or "ArcotOTP Client" means portions of CA WebFort which enable end-users to use the ArcotID and ArcotOTP credentials.

Limited License Grant. In addition to the rights granted in the applicable license agreement, CA grants Customer and its affiliates a nonexclusive license to distribute the ArcotID Client or ArcotOTP Client to end users. Customer may use Customer's logo and name with the ArcotID Client or ArcotOTP Client. No title to or ownership of the ArcotID Client or ArcotOTP Client is transferred to Customer.

CA Wily Application Performance Management v9 (CA Wily APMv9)

CA Wily APMv9 is licensed by (1) the number of CPUs when used as a distributed product or by (2)(a) millions of service units ("MSUs") and number of System z Application Assist Processors ("zAAPs") and number of System z Integrated Information Processors ("zIIPs") or (b) number of integrated facilities for Linux ("IFLs"), when used in the mainframe environment. "CPU" means a central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A dual-core central processing unit is considered a single CPU. Note that because of the use of multi-core CPUs and virtual server environments, the calculation of CPUs for licensing purposes described below will not always equate to the number of physical CPUs in the environment. A virtual server environment is created where virtual machine technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously ("Virtual Machine Technology"). When the

Authorized Use Limitation is "CPU" or "Processor", the calculation with respect to the number of CPUs on an individual server is determined as follows:

1. For non-virtual server environments, for any server with applications monitored by the CA Software with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with applications monitored by the CA Software with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number.

2. For virtual server environments, for any server with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number. Determine the maximum percentage of the server CPU capacity that is allocated by the Virtual Machine Technology to any operating system instance containing application(s) monitored by the CA Software, and multiply this percentage by the number of CPUs. Multiply the resulting number by one and a half (1.5X) and round up to the next whole number.

3. For mixed server environments, for each server perform the calculations for CPUs as set forth above in subparagraphs (1) and (2) and add these amounts together to determine the aggregate number of CPUs.

When the Authorized Use Limitation is "MSUs", "zAAPs", or "zIIPs" (i) the MSUs shall be calculated by totaling the MSU capacity for all logical partitions, or LPARs, that run an application monitored by the CA Software, (ii) the zAAPs shall be calculated by totaling the number of zAAP engines attached to such LPARs, and (iii) the zIIPs shall be calculated by totaling the number of zIIP engines attached to such LPARs. An "LPAR" means the division of a computer's processors, memory, and storage into multiple sets of resources so that each set of resources is operated independently with its own physical or virtual operating system instance and applications.

When the Authorized Use Limitation is "IFLs", the IFLs shall be calculated by totaling the number of IFL engines that run an application monitored by the CA Software.

CA Wily Transaction Impact Monitor ("TIM") "Software Appliance" means the software running TIM on Customer's network feed to capture http/https transactions necessary for the Customer Experience analysis portion of CA Wily APMv9. Customer is responsible for providing hardware on which to run the TIM Software Appliance that meets CA's specifications. Customer must license a copy of the TIM Software Appliance for each physical server (regardless of the number of CPUs) on which a TIM Software Appliance will be installed and configured.

CA Wily Application Performance Management (CA Wily APM)

CA Wily APM is licensed by (1) the number of CPUs when used as a distributed product or by (2)(a) millions of service units ("MSUs") and number of System z Application Assist Processors ("zAAPs") and number of System z Integrated Information Processors ("zIIPs") or (b) number of integrated facilities for Linux ("IFLs"), when used in the mainframe environment. "CPU" means a central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A dual-core central processing unit is considered a single CPU. Note that because of the use of multi-core CPUs and virtual server environments, the calculation of CPUs for licensing purposes described below will not always equate to the number of physical CPUs in the environment. A virtual server environment is created where virtual machine technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously. When the Authorized Use Limitation is "CPU" or "Processor", the calculation with respect to the number of CPUs on an individual server is determined as follows:

1. For non-virtual server environments, for any server with applications monitored by the CA Software with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with applications monitored by the CA Software with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number.

2. For virtual server environments, for any server with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number. Determine the maximum percentage of the server CPU capacity that is allocated by the Virtual Machine Technology to any operating system instance containing application(s) monitored by the CA Software, and multiply this percentage by the number of CPUs. Multiply the resulting number by one and a half (1.5X) and round up to the next whole number.

3. For mixed server environments, for each server perform the calculations for CPUs as set forth above in subparagraphs (1) and (2) and add these amounts together to determine the aggregate number of CPUs.

When the Authorized Use Limitation is "MSUs", "zAAPs", or "zIIPs" (i) the MSUs shall be calculated by totaling the MSU capacity for all logical partitions, or LPARs, that run an application monitored by the CA Software, (ii) the zAAPs shall be calculated by totaling the number of zAAP engines attached to such LPARs, and (iii) the zIIPs shall be calculated by totaling the number of zIIP engines attached to such LPARs. An "LPAR" means the division of a computer's processors, memory, and storage into multiple sets of resources so that each set of resources is operated independently with its own physical or virtual operating system instance and applications.

When the Authorized Use Limitation is "IFLs", the IFLs shall be calculated by totaling the number of IFL engines that run an application monitored by CA Wily APM.

An Appliance is a CA-supplied physical server ("Hardware") that is bundled with and used to operate the CA Software licensed by Customer which is pre-installed on the Hardware. Support is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com. Customer must acquire at least one license (per CPU, MSU or IFL) in order to purchase a CA Wily Transaction Impact Monitor ("TIM") or CA Wily Transaction Event & Statistics Server ("TESS"). Both a TIM and a TESS are required for any production installation. CA Wily Solutions for Lab Environments ("Wily LAB") is a single Appliance that contains TIM and TESS capabilities but is not supported for a production environment. The Wily LAB system includes one CPU license for CA Wily APM at no additional charge.

CA Wily Customer Experience Manager (CA Wily CEM)

CA Wily CEM is licensed by (1) the number of CPUs when used as a distributed product or by (2)(a) millions of service units ("MSUs") and number of System z Application Assist Processors ("zAAPs") and number of System z Integrated Information Processors ("zIIPs") or (b) number of integrated facilities for Linux ("IFLs"), when used in the mainframe environment. "CPU" means a central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A dual-core central processing unit is considered a single CPU. Note that because of the use of multi-core CPUs and virtual server environments, the calculation of CPUs for licensing purposes described below will not always equate to the number of physical CPUs in the environment. A virtual server environment is created where virtual machine technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously ("Virtual Machine Technology"). When the Authorized Use Limitation is "CPU" or "Processor", the calculation with respect to the number of CPUs on an individual server is determined as follows:

1. For non-virtual server environments, for any server with applications monitored by the CA Software with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with applications monitored by the CA Software with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number.

2. For virtual server environments, for any server with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number. Determine the maximum percentage of the server CPU capacity that is allocated by the Virtual Machine Technology to any operating system instance containing application(s) monitored by the CA Software, and multiply this percentage by the number of CPUs. Multiply the resulting number by one and a half (1.5X) and round up to the next whole number.

3. For mixed server environments, for each server perform the calculations for CPUs as set forth above in subparagraphs (1) and (2) and add these amounts together to determine the aggregate number of CPUs.

When the Authorized Use Limitation is "MSUs", "zAAPs", or "zIIPs" (i) the MSUs shall be calculated by totaling the MSU capacity for all logical partitions, or LPARs, that run an application monitored by the CA Software, (ii) the zAAPs shall be calculated by totaling the number of zAAP engines attached to such LPARs, and (iii) the zIIPs shall be calculated by totaling the number of zIIP engines attached to such LPARs. An "LPAR" means the division of a computer's processors, memory, and storage into multiple sets of resources so that each set of resources is operated independently with its own physical or virtual operating system instance and applications.

When the Authorized Use Limitation is "IFLs", the IFLs shall be calculated by totaling the number of IFL engines that run an application monitored by the CA Software.

An Appliance is a CA-supplied physical server ("Hardware") that is bundled with and used to operate the CA Software licensed by Customer which is pre-installed on the Hardware. Support is provided in accordance with the CA Appliance Hardware Policy published on CA Support Online located at http://support.ca.com. Customer must acquire at least one license (per CPU, MSU or IFL) in order to purchase a CA Wily Transaction Impact Monitor ("TIM") or CA Wily Transaction Event & Statistics Server ("TESS"). Both a TIM and a TESS are required for any production installation. CA Wily Solutions for Lab Environments ("Wily LAB") is a single appliance that contains TIM and TESS capabilities but is not supported for a production environment. The Wily LAB system includes one CPU license for CA Wily CEM at no additional charge.

CA Wily Introscope

CA Wily Introscope is licensed by (1) the number of CPUs when used as a distributed product or by (2)(a) millions of service units ("MSUs") and number of System z Application Assist Processors ("zAAPs") and number of System z Integrated Information Processors ("zIIPs") or (b) number of integrated facilities for Linux ("IFLs"), when used in the mainframe environment. "CPU" means a central processing unit which is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. A dual-core central processing unit is considered a single CPU. Note that because of the use of multi-core CPUs and virtual server environments, the calculation of CPUs for licensing purposes described below will not always equate to the number of physical CPUs in the environment. A virtual server environment is created where virtual machine technology (which applies to both client and server hardware) is used to enable multiple instances of an operating system(s) to run on a single computer simultaneously ("Virtual Machine Technology"). When the Authorized Use Limitation is "CPU" or "Processor", the calculation with respect to the number of CPUs on an individual server is determined as follows:

1. For non-virtual server environments, for any server with applications monitored by the CA Software with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with applications monitored by the CA Software with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number.

2. For virtual server environments, for any server with single CPUs (including, for the avoidance of doubt, dual-core CPUs), count the number of CPUs. For any server with greater than dual-core CPUs, count all cores of the CPUs. Divide the number of cores by two (2) and round up to the next whole number. Determine the maximum percentage of the server CPU capacity that is allocated by the Virtual Machine Technology to any operating system instance containing application(s) monitored by the CA Software, and multiply this percentage by the number of CPUs. Multiply the resulting number by one and a half (1.5X) and round up to the next whole number.

3. For mixed server environments, for each server perform the calculations for CPUs as set forth above in subparagraphs (1) and (2) and add these amounts together to determine the aggregate number of CPUs.

When the Authorized Use Limitation is "MSUs", "zAAPs", or "zIIPs" (i) the MSUs shall be calculated by totaling the MSU capacity for all logical partitions, or LPARs, that run an application monitored by the CA Software, (ii) the zAAPs shall be calculated by totaling the number of zAAP engines attached to such LPARs, and (iii) the zIIPs shall be calculated by totaling the number of zIIP engines attached to such LPARs. An "LPAR" means the division of a computer's processors, memory, and storage into multiple sets of resources so that each set of resources is operated independently with its own physical or virtual operating system instance and applications. When the Authorized Use Limitation is "IFLs", the IFLs shall be calculated by totaling the number of IFL engines that run an application monitored by the CA Software.

CA Workload Automation

"Instance" means the number of copies of the CA Software installed in the Customer physical and/or virtual environment.

CA XCOM Data Transport for Windows Family Server

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA eHealth Performance Manager

"Managed Network Device" means a virtual or physical network-connected device with less than 200 ports that is managed by the CA Software and uses an Internet Protocol ("IP") address, including but not limited to IP and hybrid telephony devices, routers, appliances, hubs, virtual or physical servers, and virtual or physical machines, but excluding endpoint devices such as IP telephones.

Mainframe CPU CA Software only

The CA Software is licensed by the specified number and model of CPU (the "Authorized Use Limitation"). "CPU" shall mean the central processing unit(s) capable of running the CA Software. Customer may only use CPUs specified when licensing the licenses herein and upon which the CA Software is installed and runs ("Designated CPUs"). Customer may change the Designated CPU on providing written notice to CA provided that such replacement CPU is of the same or lower CPU tier/power rating to the Designated CPU (save that Customer may

require an authorization key from CA in order to commence use of such CPU). Should Customer wish to add to the number of Designated CPUs or upgrade the then current Designated CPU(s) to a CPU with greater tier/power rating, Customer may elect to do so by providing CA with prior written notice of such additional CPU and/or upgrade to the Designated CPU(s) and by executing an order form to effect such addition/change and purchasing the applicable license.

Mainframe MIPS CA Software only

The CA Software is licensed by the specified number of MIPS (the "Authorized Use Limitation in MIPS"). "MIPS" means millions of instructions per second. The MIPS capacity of a computer shall be calculated by reference to CA's published schedules of the MIPS capacity and if a computer isn't listed then the manufacturer's published specifications should apply. Further, in the event a special purpose processor, designed to perform one or more dedicated functions, is being used as a general purpose processor, CA shall treat such processor as a general purpose processor for purposes of calculating Authorized Use Limitation in MIPS. "Customer Site" means the site(s) specified at the time of licensing the CA Software or the Customer Address if no Customer Site has been indicated. Customer may use the CA Software only on the specific computers upon which the CA Software is installed to run at the Customer Site or on computers which are linked, connected to and/or which can remotely access such computers, irrespective of the platform designations of the hardware or operating systems, provided that such computer is capable of accessing, using, executing or benefiting from the CA Software, subject to the aggregate MIPS capacity not exceeding the Authorized Use Limitation in MIPS.

Mainframe MSU CA Software only

The CA Software is licensed by the specified number of MSU (the "Authorized Use Limitation in MSU"). "MSU" means millions of service units. The MSU capacity shall be calculated with the aggregate computing power (expressed in millions of service units) by reference to CA's published schedules of the MSU capacity and if a computer isn't listed then the manufacturer's published specifications shall apply of all computers upon which the CA Software is installed to run at the Customer Site ("Customer Site" means the site(s) specified at the time of licensing the CA Software or the Customer Address if no Customer Site has been indicated) or computers which are linked, connected to and/or which can remotely access such computers, irrespective of the platform designations of the hardware or operating systems, provided that such computer is capable of accessing, using, executing or benefiting from the CA Software. Customer may use the CA Software subject to the aggregate MSU Capacity not exceeding the Authorized Use Limitation in MSU.

Pervasive Software:

The Pervasive Software is licensed by either by the number of Server or Users. Pervasive Software may be used to build integrations that connect to any authorized CA Clarity environment.

Pervasive Data Integrator Engine/Agent **for CA** Clarity PPM* is licensed by the number of Servers.
* includes one User license of Pervasive Data Integrator Analyst **Studio for C**A Clarity PPM

Pervasive Data Integrator Analyst **Studio for C**A Clarity PPM is licensed by the number of Users.

Pervasive Data Profiler Engine for CA Clarity PPM is licensed by the number of Servers.

Pervasive Data Profiler Analyst Studio for CA Clarity PPM is licensed by the number of Users.

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

"User" means a single person listed in any Customer directory or network storage location whose access and use rights can be authenticated, authorized, or administered by the Pervasive Software. Unless otherwise specified, a User shall not be counted more than once or on a concurrent basis.

CA Process Automation:

CA Software means the CA Process Automation software described herein in object code form only.

"Agent" means a single installation of the agent software component of the CA Software on a specific operating system which can be identified as a unique host identification on a physical or virtual hardware server.

"Orchestrator" means a single installation of the Orchestrator software component of the CA Software on a specific operating system which can be identified as a unique host identification on a physical or virtual hardware server. This installation can be a stand-alone Orchestrator or as a node of a new or existing clustered Orchestrator.

"Connector" is the software program connecting the CA Software with specific named third party software or other CA software. For example, CA Process Automation Connector For CA Service Desk connects CA Process Automation with CA Service Desk. Each Connector may only be used to connect the CA Software with the specific named third party software or CA software program.

"Premium Connector" means a Connector identified as "Premium" by CA.

"Custom Operator" means a type of automation object within the CA Process Automation Orchestrator that can be created to enhance, modify, or restrict the capabilities of an existing "Connector".

"Process" means a type of automation object within CA Process Automation Orchestrator that contains connectors and other logical constructs that define a set of actions that will take place when the "Process" is executed by the Orchestrator.

"Process instance" means a single copy of a Process definition that has been scheduled to run (Queued state), is running (Running state), or has completed running (Failed or Completed state) on a particular "Orchestrator".

"Concurrent Processes" means the number of CA Process Automation Process instances that are marked in the Running state within an Orchestrator at any given time.

"Power Pack" means a combination of Process definitions, Premium Connectors, Custom Operators and other automation objects that are packaged together to implement a specific solution.

The CA Software is licensed in different editions, as set forth in this Order Form, which authorizes the use of the specified number of Orchestrators, Agents, Connectors, and Concurrent processes (the "Authorized Use Limitation"). The various editions are:

CA Process Automation Player License includes: one Orchestrator, forty Agents, all non-Premium Connectors, and two hundred Concurrent Processes per Orchestrator. This license requires the purchase of either a "Power Pack" or a Services contract for the implementation of a solution that will be executed by the Player. No new automation objects may be created with the Player License. Only modifications of the purchased Power Packs and any Services delivered content is allowed.

CA Process Automation Express License includes: two Orchestrators, forty Agents, all non-Premium Connectors, and seventy-five Concurrent Processes per Orchestrator.

CA Process Automation Standard License includes: two Orchestrators, unlimited Agents, three Premium Connectors, all non-Premium Connectors, and two hundred Concurrent Processes per Orchestrator.

CA Process Automation Enterprise License includes: unlimited Orchestrators, unlimited Agents, twenty Premium Connectors, all non-Premium Connectors, and four hundred and seventy-five Concurrent Processes per Orchestrator.

CA Process Automation Level 1 Orchestrator includes: one Orchestrator and seventy-five Concurrent Processes per Orchestrator.

CA Process Automation Level 2 Orchestrator includes: two Orchestrators and two hundred Concurrent Processes per Orchestrator.

CA Process Automation Level 3 Orchestrator includes: three Orchestrators and four hundred and seventy-five Concurrent Processes per Orchestrator.

CA Process Automation Premium Connector License includes the right to use a Premium Connector to connect to a single instance of the target application or system.

CA Process Management for Workflows License includes: unlimited Orchestrators, five Agents, and three Custom Operators. No Premium connectors are available for purchase with this license. The only CA product connectors that are available are those associated with the product(s) providing the entitlement. This is a limited use entitlement and its use is restricted to the context of Workflows associated with the CA product(s) providing the entitlement. The component limits are not cumulative across multiple instances of the license at any individual customer.

The number of concurrent processes executing on any licensed Orchestrator may be exceeded as long as the total number of concurrent processes executing on all licensed Orchestrators is not exceeded. For example, if the license is for two Orchestrators with seventy-five Concurrent Processes per Orchestrator, one hundred Concurrent Processes could be utilized on one Orchestrator so long as only fifty Concurrent Processes are utilized on the second Orchestrator.

Server:

"Server" means a single physical or virtual computer which processes data using one or more central processing units, and which is owned, leased or otherwise controlled by Customer.

CA Virtual Assurance for Infrastructure Managers and CA System Performance for Infrastructure Managers

"Physical Socket" means an electrical component attached to a printed circuit board ("PCB") and electrically interconnects a central processing unit ("CPU") and PCB. A CPU is the specialized integrated circuit that executes binary programs and performs most logical functions or calculations. One physical CPU may have up to twelve (12) processing cores.

DOCUSIGN, INC.
CORPORATE SUBSCRIBER TERMS AND CONDITIONS
v121008

These Terms and Conditions are incorporated by this reference into the Order Form (collectively referred to as the "Agreement") entered into by DocuSign, Inc. ("DocuSign") and the customer identified in the Order Form ("Subscriber").

1. DEFINITIONS

"**Account**" means a unique account established by Subscriber to enable its Authorized Users to access and use the Subscription Service and, where applicable, other DocuSign Products.

"**Authorized User**" means any employee of Subscriber, identified by a unique email address and user name, who is registered under the Account; provided that no two persons may register or use the Subscription Service as the same Authorized User.

"**Consulting Services**" means any additional professional services to be delivered by DocuSign, such as integration consulting or assistance, custom development, training, and transition services, that are set forth in an Order Form or Work Order as described in Section 15.

"**DocuSign API**" means the application programming interface that supports interoperation of applications with the Subscription Service.

"**DocuSign Products**" means the products and services identified on an Order Form, which may include the Subscription Service, the Repository Services, the Consulting Services and any other DocuSign offerings.

"**eContract**" refers to a contract, notice, disclosure, or other record or document deposited into the System by Subscriber for Processing using the Subscription Service.

"**Envelope**" means an electronic record containing one or more eContracts consisting of a single page or a group of pages of data uploaded to the System.

"**Order Form**" means a standard DocuSign order form or any other document separately and specifically approved by DocuSign that describes the DocuSign Products to be purchased by Subscriber and is signed by both parties.

"**Personal Data**" means any of the following: (a) nonpublic personally identifiable information, including driver's license numbers, national identification numbers such as social security account numbers, credit card numbers, digital identity certificates; (b) personally identifiable financial information regarding a consumer (i) provided by a consumer to a financial institution, (ii) resulting from any transaction with the consumer or any service performed for the consumer by a financial institution, or (iii) otherwise obtained by the financial institution, including any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information; (c) personally identifiable medical or health-related information.

"**Process**" means any operation or set of operations performed upon Subscriber's data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, accessing, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"**Repository Services**" means the Contract Repository or eVaulting Services, each as defined in the Terms and Conditions for Repository Services (available at http://www.docusign.com/company/terms-and-conditions/eoriginal/v121005), that are made the subject of an Order Form.

"**Specifications**" means the technical specifications set forth in the "Subscription Service Specifications" available at http://docusign.com/company/specifications.

"**Subscription Service**" means DocuSign's on-demand electronic signature service, which provides online display, certified delivery, acknowledgement, electronic signature, and storage services for eContracts via the Internet.

"**System**" refers to the software systems and programs, communication and network facilities, and hardware and equipment used by DocuSign or its agents to provide the Subscription Service.

"**Term**" means the period of effectiveness of this Agreement, as described in more detail in Section 9 below.

"**Transaction Data**" means the metadata associated with an Envelope and maintained by DocuSign for the purpose of establishing a digital audit trail, such as transaction history, image hash value, method and time of Envelope deletion, sender and recipient names, email addresses and signature IDs.

2. THE SUBSCRIPTION SERVICE

2.1 During the Term and subject to these Terms and Conditions, DocuSign will provide the Subscription Service in accordance with the Specifications, and Subscriber will have the right to obtain an Account and register its Authorized Users, who may access and use the Subscription Service. The right to use the Subscription Service is: (a) limited to its Authorized Users (accordingly, Subscriber may not resell or otherwise provide or assist with the provision of the Subscription Service to any third party); and (b) conditioned on Subscriber's acknowledgement and agreement with the following:

i) Nothing in this Agreement will be construed to make DocuSign a party to any eContract, and DocuSign makes no representation or warranty regarding the transactions sought to be effected by any eContract;

ii) DocuSign maintains no control of or access to the contents of any eContract, and so the content, quality, and format of any eContract is at all times in the exclusive control and responsibility of Subscriber;

iii) If Subscriber elects to use optional features designed to verify the identity of the intended recipient of an eContract ("Authentication Measures"), DocuSign will apply only those Authentication Measures (if any) selected by the Subscriber, but makes no representations or warranties about the appropriateness of any Authentication Measure and further, assumes no liability for the inability or failure by the intended recipient or other party to satisfy the Authentication Measure or to circumvent it;

iv) Certain types of agreements and documents are excepted from electronic signature laws, such that they cannot be legally formed by electronic signatures, and additionally, various agencies may have promulgated specific regulations that apply to electronic signatures and electronic records. DocuSign assumes no responsibility to determine whether any particular eContract is an exception to applicable electronic signature laws, or whether it is subject to any particular agency promulgations, or whether it can be legally formed by electronic signatures;

v) Subscriber is solely responsible for making available to third parties (including all parties to its eContracts) all contracts, documents, and other records required by applicable law, including, without limitation, electronic signature laws and other laws that may require records relating to a transaction to be retained or made accessible for a certain period of time;

vi) Certain laws or regulations impose special requirements with respect to electronic transactions involving one or more "consumers," such as (among others) requirements that the consumer consent to the method of contracting and/or that the consumer be provided with a copy, or access to a copy, of a paper or other non-electronic, written record of the transaction. DocuSign assumes no responsibility to: (A) determine whether any particular transaction involves a consumer; (B) furnish or obtain any such consents or to determine if any such consents have been withdrawn; (C) provide any information or disclosures in connection with any attempt to obtain any such consents; (D) provide legal review of, or to update or correct any information or disclosures currently or previously given; (E) provide any such copies or access except as expressly provided in the Specifications for all transactions, consumer or otherwise; or (F) otherwise to comply with any such special requirements; and

vii) Subscriber expressly undertakes to determine whether any consumer is involved in any eContract presented by its Authorized Users for Processing, and, if so, to comply with all requirements imposed by law on such eContracts or their formation.

3. SUBSCRIPTION PLANS AND USAGE PRICING

3.1 The pricing, features and options of the DocuSign Products selected by Subscriber are set forth in the Order Form. The Subscription Service is sold on a subscription basis and may be limited by usage ("Envelope Allowance"), or by the number of Authorized Users ("Seats"), or both. Optional features, such as Authentication Measures or fax-back services, may be purchased on a periodic or per-use basis.

3.2 If Subscriber selects an **Envelope Allowance Subscription,** then Subscriber is allowed to send the number of Envelopes in the Envelope Allowance specified in the Order Form during the Term. All Envelopes sent in excess of the Envelope Allowance will incur a per-Envelope charge that will be invoiced within 30 days of the date first incurred. The total number of Envelopes used is based on the sum of all Envelopes that have been sent for signature or for certified delivery from the Account. An Envelope will be deemed consumed at the time it is sent by an Authorized User, whether or not it has been received by the recipients or the recipients have performed any actions upon any eContract in the Envelope.

3.3 If Subscriber selects a **Seat Subscription,** then Subscriber is allowed to manually send Envelopes from the number of Seats specified in the Order Form during the Term. A Seat is defined as a natural person manually preparing and sending Envelopes, and excludes the Processing of Envelopes using automated batch or bulk sending operations, or the use of the

DocuSign API for sending Envelopes. If the number of Envelopes sent from a particular Seat or a group of Seats is abusive and/or unduly burdensome (indicating automated Processing), DocuSign will promptly notify Subscriber and the parties will review the use-case scenario as well as any continued monitoring and additional Seats that may be required to be purchased. The number of Seats is determined by the total number of active Authorized Users listed in the membership of an Account at any one time. No two individuals may log onto or use the Subscription Service as the same Authorized User, but Subscriber may unregister or deactivate Authorized Users and replace them with other Authorized Users without penalty, so long as the number of active Authorized Users registered at any one time is equal to or less than the number of Seats purchased. The addition by Subscriber of more Authorized Users than the number of Seats purchased in an Order Form will result in an additional charge for one Seat per additional Authorized User for the remainder of the Term, to be invoiced immediately.

4. ADDITIONAL SUBSCRIBER RESPONSIBILITIES

4.1 Subscriber agrees that it will not use or permit the use of the Subscription Service to send unsolicited mass mailings outside its organization, it being understood that the term "unsolicited mass mailings" includes all statutory and other common definitions, including all Commercial Electronic Marketing Messages as defined in the U.S. CAN SPAM Act.

4.2 Subscriber agrees that it is solely responsible for the nature and content of all materials, works, data, statements, and other visual, graphical, video, written or audible communications of any nature submitted by any Authorized User or otherwise Processed through its Account.

4.3 Subscriber further agrees not to use or permit the use of the Subscription Service: (a) to communicate any message or material that is defamatory, harassing, libelous, threatening, or obscene; (b) in a way that violates or infringes upon the intellectual property rights or the privacy or publicity rights of any person or entity or that may otherwise be unlawful or give rise to civil or criminal liability (other than contractual liability of the parties under eContracts Processed through the Subscription Service); (c) in any manner that is likely to damage, disable, overburden, or impair the System or the Subscription Service or interfere in any way with the use or enjoyment of the Subscription Service by others; or (d) in any way that constitutes or encourages conduct that could constitute a criminal offense.

4.4 Although DocuSign does not monitor the content Processed through the Subscription Service, DocuSign may at any time suspend any use of the Subscription Service and/or remove or disable any content as to which DocuSign reasonably and in good faith believes is in violation of this Agreement. DocuSign agrees to provide Subscriber with notice of any such suspension or disablement before its implementation unless such suspension or disablement is necessary to comply with legal process or prevent imminent harm to DocuSign's System, the Subscription Service or any third party, in which case DocuSign will notify Subscriber of such suspension or disablement as soon as reasonably practicable thereafter.

5. INTELLECTUAL PROPERTY AND TRADEMARK LICENSE

5.1 DocuSign is the owner of various intellectual property and technology rights associated with the Subscription Service, its document management, digital signature, and notary system, including patent, copyright, trade secret, and trademark and service mark rights. Except for the rights expressly granted in this Agreement, DocuSign does not license or transfer to Subscriber or any Authorized User or other third party any of DocuSign's technology or other intellectual property or technology rights. All right, title, and interest in and to DocuSign's technology and intellectual property will remain solely with DocuSign. Subscriber agrees that it will not, directly or indirectly, reverse engineer, decompile, disassemble, or otherwise attempt to derive source code or other trade secrets from or about any of the DocuSign Products or DocuSign's technology. DocuSign agrees that data and information provided by Subscriber under this Agreement shall remain, as between Subscriber and DocuSign, owned by Subscriber.

5.2 DocuSign hereby grants to users and licensees of its products and services a limited, revocable, nonexclusive and nontransferable right to use DocuSign's regular trade names, trademarks, titles and logos ("Licensed Marks") solely for purposes of identifying DocuSign's products and services. Details of this trademark license are available at: http://www.docusign.com/trademark-license.

6. CUSTOMER SUPPORT

DocuSign will provide customer support to Subscriber in accordance with the package that is identified on the Order Form, as further detailed at http://www.docusign.com/products/support-plans.

7. eCONTRACT STORAGE AND DELETION

7.1 DocuSign will store in accordance with the Specifications all completed eContracts sent by Subscriber until the termination or expiration of the Agreement, unless otherwise directed by Subscriber. Copies of stored eContracts may be retrieved by Subscriber at any time during that period, provided that following the expiration or termination of the Agreement, Subscriber may

request DocuSign's assistance in retrieving completed eContracts still remaining on the System pursuant to the transition services terms described in Section 9.4.

7.2 Prior to the expiration or termination of this Agreement, Subscriber may elect to purchase post-expiration or post-termination storage services for their completed eContracts. Where Subscriber opts not to purchase storage services, all copies of eContracts may be deleted by DocuSign without prior notice after the period available for transition services has expired pursuant to the terms described in Section 9.4. Subscriber may, at its option and wholly at Subscriber's risk, direct that any eContract be deleted at a time stated by Subscriber and prior to the end of the Term.

7.3 DocuSign may at its sole discretion delete an uncompleted eContract from the System immediately and without notice upon earlier of: a) expiration of the Envelope (where Subscriber has established an expiration for such Envelope, not to exceed 365 days); or b) expiration of the Term.

7.4 DocuSign will retain the Transaction Data permanently, provided that any Transaction Data that constitutes Confidential Information of Subscriber will at all times maintain that status and DocuSign will comply with its obligations in Section 13.

8. FEES AND PAYMENT TERMS

8.1 Subscriber will pay DocuSign the amounts set forth in each Order Form. An Order Form is not binding until it is executed by both DocuSign and Subscriber, at which point it will be deemed to be incorporated into this Agreement. Unless otherwise specified in an applicable Order Form, the first invoice will be submitted to Subscriber within 30 days after the Order Start Date, and Subscriber will pay all amounts due within 30 days of the date of the applicable invoice.

8.2 If Subscriber's usage under an Envelope Allowance Subscription exceeds the Envelope Allowance prior to the end of the Term, the unpaid balance of the Order Form for such Envelope Allowance Subscription shall become immediately due and payable.

8.3 Any undisputed amount not paid when due will be subject to finance charges equal to 1.5% of the unpaid balance per month or the highest rate permitted by applicable usury law, whichever is less, determined and compounded daily from the date due until the date paid. Subscriber will reimburse any costs or expenses (including reasonable attorneys' fees) incurred by DocuSign to collect any undisputed amount that is not paid when due. DocuSign may accept any check or payment in any amount without prejudice to DocuSign's right to recover the balance of the amount due or to pursue any other right or remedy. Amounts due to DocuSign under this Agreement may not be withheld or offset by Subscriber for any reason against amounts due or asserted to be due to Subscriber from DocuSign. All amounts payable under this Agreement are denominated in United States dollars, and Subscriber will pay all such amounts in United States dollars.

8.4 **Taxes**. Other than federal and state net income taxes imposed on DocuSign by the United States, Subscriber will bear all taxes, duties, and other governmental charges (collectively, "taxes") resulting from this Agreement or transactions conducted in relation to this Agreement or the DocuSign Products. If a tax is imposed on DocuSign by a jurisdiction outside the United States, Subscriber will not be obligated to bear that tax to the extent: (a) the tax is allowable as a credit against the United States federal income taxes of DocuSign; (b) Subscriber reduces such tax to the extent possible, giving effect to the applicable Income Tax Convention between the United States and other jurisdictions; and (c) Subscriber furnishes DocuSign with such evidence as the United States taxing authorities may require to claim the credit. Subscriber will pay any additional taxes as are necessary to ensure that the net amounts received and retained by DocuSign after all such taxes are paid are equal to the amounts that DocuSign would have been entitled to in accordance with this Agreement as if the taxes did not exist.

9. TERM AND TERMINATION

9.1 **Term**. Unless sooner terminated as stated below, and subject to Section 17 with respect to Work Orders (as defined below), the effectiveness of this Agreement will commence upon the Order Start Date and will continue for the term specified on the Order Form (the "Term").

9.2 **Termination for Cause.** If either party commits a material breach or default in the performance of any of its obligations under this Agreement, then the other party may terminate this Agreement by giving the defaulting party written notice of termination if the material breach or default in performance is not cured within 30 days after the defaulting party receives notice thereof. Without limiting the foregoing, any failure by Subscriber to timely pay to DocuSign any amounts owing under this Agreement will constitute a material breach of this Agreement. If Subscriber fails to timely pay any amounts due for services to be performed by DocuSign, then without limitation to any of its other rights or remedies, DocuSign may suspend performance of such services until it receives all amounts due.

9.3 **Post-Termination Obligations.** If this Agreement expires or is terminated for any reason: (a) Subscriber will pay to DocuSign any amounts required to be paid under this Agreement that have accrued prior to, and remain unpaid as of, the date of

termination or expiration (including Subscription fees, which become due upon termination of this Agreement as set forth in an Order Form, and any one-time or recurring fees through the end of the billing cycle in which termination occurs); (b) any and all liabilities accrued prior to the effective date of the termination will survive; (c) Subscriber will destroy all copies of DocuSign software, documentation, and materials within five business days of such termination, and immediately thereafter, if requested by DocuSign, provide DocuSign with a written certification signed by an authorized Subscriber representative certifying that all copies of software, documentation, and materials have been destroyed; (d) licenses to use DocuSign software and the provision of DocuSign services will immediately end; and (e) the parties' rights and obligations under Sections 1, 7.4, 9.3, 9.4, 10.3, and 11 through 14 will survive.

9.4 **Transition Services**. Upon expiration or termination of this Agreement for any reason, at Subscriber's request and at DocuSign's then-current standard professional services rates plus expenses, DocuSign shall provide reasonable transition services for a period not to exceed 90 days to assist Subscriber in moving Subscriber's data to another provider or exporting eContracts to external media. As part of such transition services, DocuSign shall at a minimum transfer, and cause any of its independent contractors to transfer, all data and electronic files associated with the Subscription Service. At its then-current standard professional services rates, DocuSign shall at Subscriber's request further cooperate with Subscriber in the development of a transition plan and shall use reasonable efforts to assist Subscriber and/or another service provider in the transition. DocuSign may at its discretion require advance payment or other adequate security for payment as DocuSign may consider appropriate in connection with or as a condition to the provision of services described in this section.

10. WARRANTIES AND DISCLAIMERS

10.1 **DocuSign Warranties**. DocuSign represents and warrants that: (a) the Subscription Service as delivered to Subscriber and used in accordance with the Specifications will not infringe on any United States patent, copyright or trade secret; (b) the Subscription Service shall be performed in accordance with the Specifications in their then-current form at the time of the provision of such Subscription Service; (c) any DocuSign Products that are software shall be free of harmful or illicit code, trapdoors, viruses, or other harmful features; (d) the proper use of the Subscription Service by Subscriber in accordance with the Specifications and applicable law in the formation of an eContract not involving any consumer will be sufficient under the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq. (the "ESIGN Act") to support the validity of such formation, to the extent provided in the ESIGN Act; (e) the proper use of the Subscription Service by Subscriber in accordance with the Specifications and applicable law in the formation of an eContract involving a consumer will be sufficient under the ESIGN Act to support the validity of such formation, to the extent provided in the ESIGN Act, so long as and provided that Subscriber complies with all special requirements for consumer eContracts, including and subject to those referenced in Section 2.1(vi) and (vii) above; and (f) DocuSign has implemented information security policies and safeguards to preserve the security, integrity, and confidentiality of Personal Data and to protect against unauthorized access and anticipated threats or hazards thereto, that meet the objectives of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information as set forth in Section 501 (b) of the Gramm-Leach-Bliley Act.

10.2 **Mutual Warranties**. Each party represents and warrants to the other that: (a) this Agreement has been duly executed and delivered and constitutes a valid and binding agreement enforceable against such party in accordance with its terms; (b) no authorization or approval from any third party is required in connection with such party's execution, delivery, or performance of this Agreement; and (c) the execution, delivery, and performance of this Agreement does not violate the laws of any jurisdiction or the terms or conditions of any other agreement to which it is a party or by which it is otherwise bound.

10.3 **Disclaimer**. EXCEPT FOR THE EXPRESS REPRESENTATIONS AND WARRANTIES STATED IN SECTIONS 10.1 AND 10.2 ABOVE (WHICH ARE NOT APPLICABLE TO CONSULTING SERVICES), DOCUSIGN MAKES NO ADDITIONAL REPRESENTATION OR WARRANTY OF ANY KIND -- WHETHER EXPRESS, IMPLIED IN FACT OR BY OPERATION OF LAW, OR STATUTORY -- AS TO ANY MATTER WHATSOEVER. DOCUSIGN EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. DOCUSIGN DOES NOT WARRANT THAT THE DOCUSIGN PRODUCTS (INCLUDING CONSULTING SERVICES OR RELATED DELIVERABLES, IF ANY), ARE OR WILL BE ERROR-FREE, WILL MEET SUBSCRIBER'S REQUIREMENTS, OR BE TIMELY OR SECURE. SUBSCRIBER WILL NOT HAVE THE RIGHT TO MAKE OR PASS ON ANY REPRESENTATION OR WARRANTY ON BEHALF OF DOCUSIGN TO ANY THIRD PARTY.

11. INDEMNIFICATION

11.1 **By DocuSign**. DocuSign will defend Subscriber, and its employees, directors, agents, and representatives ("Indemnified Party") from any actual or threatened third party claim arising from: (a) any breach by DocuSign of its confidentiality obligations in Section 13, and/or (b) alleged infringement by DocuSign of any third party intellectual property rights (each a "Subscriber Claim").

11.2 **By Subscriber**. Subscriber will defend DocuSign, and its employees, directors, agents, and representatives ("Indemnified Party") from any actual or threatened third party claim arising from: (a) any breach by Subscriber of its confidentiality obligations in Section 13, and/or (b) alleged infringement by Subscriber of any third party intellectual property rights, and/or (c) the content submitted by any Authorized User or otherwise Processed through Subscriber's Account (each a "DocuSign Claim").

11.3 **Procedures.** The parties' respective indemnification obligations above are conditioned on: (a) the Indemnified Party gives the Indemnifying Party prompt written notice of the Subscriber Claim or DocuSign Claim (as the case may be, a "Claim"); (b) the Indemnifying Party has full and complete control over the defense and settlement of the Claim; (c) the Indemnified Party provides assistance in connection with the defense and settlement of the Claim as the Indemnifying Party may reasonably request; and (d) the Indemnified Party complies with any settlement or court order made in connection with the Claim. The Indemnifying Party will indemnify the Indemnified Party against: (i) all damages, costs, and attorneys' fees finally awarded against any of them in any Claim under this Section 11; (ii) all out-of-pocket costs (including reasonable attorneys' fees) reasonably incurred by any of them in connection with the defense of the Claim (other than attorneys' fees and costs incurred without the Indemnifying Party's consent after it has accepted defense of such Claim); and (iii) if any Claim arising under this Section 11 is settled by the Indemnifying Party or with its approval, then the Indemnifying Party will pay any amounts to any third party agreed to by the Indemnifying Party in settlement of any such Claims.

12. LIMITATIONS OF LIABILITY

12.1 **Disclaimer of Consequential Damages.** EXCEPT WITH RESPECT TO INDEMNIFICATION OBLIGATIONS OF SECTION 11, NOTWITHSTANDING ANYTHING TO THE CONTRARY CONTAINED IN THIS AGREEMENT, NEITHER PARTY WILL, UNDER ANY CIRCUMSTANCES, BE LIABLE TO THE OTHER PARTY FOR CONSEQUENTIAL, INCIDENTAL, SPECIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR RELATED TO THE TRANSACTIONS CONTEMPLATED UNDER THIS AGREEMENT (INCLUDING WITH RESPECT TO CONSULTING SERVICES, IF ANY), INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OF BUSINESS, EVEN IF APPRISED OF THE LIKELIHOOD OF SUCH DAMAGES OCCURRING.

12.2 **Cap on Liability.** EXCEPT WITH RESPECT TO INDEMNIFICATION OBLIGATIONS OF SECTION 11, UNDER NO CIRCUMSTANCES WILL EITHER PARTY'S TOTAL LIABILITY OF ALL KINDS ARISING OUT OF OR RELATED TO THIS AGREEMENT (INCLUDING, BUT NOT LIMITED TO, WARRANTY CLAIMS AND WITH RESPECT TO CONSULTING SERVICES, IF ANY), REGARDLESS OF THE FORUM AND REGARDLESS OF WHETHER ANY ACTION OR CLAIM IS BASED ON CONTRACT, TORT, OR OTHERWISE, EXCEED THE TOTAL AMOUNT PAID BY SUBSCRIBER TO DOCUSIGN UNDER THIS AGREEMENT DURING THE 12 MONTHS PRECEDING THE DATE OF THE ACTION OR CLAIM.

12.3 **Independent Allocations of Risk.** EACH PROVISION OF THIS AGREEMENT THAT PROVIDES FOR A LIMITATION OF LIABILITY, DISCLAIMER OF WARRANTIES, OR EXCLUSION OF DAMAGES REPRESENTS AN AGREED ALLOCATION OF THE RISKS OF THIS AGREEMENT BETWEEN THE PARTIES. THIS ALLOCATION IS REFLECTED IN THE PRICING OFFERED BY DOCUSIGN TO SUBSCRIBER AND IS AN ESSENTIAL ELEMENT OF THE BASIS OF THE BARGAIN BETWEEN THE PARTIES. EACH OF THESE PROVISIONS IS SEVERABLE AND INDEPENDENT OF ALL OTHER PROVISIONS OF THIS AGREEMENT, AND EACH OF THESE PROVISIONS WILL APPLY EVEN IF THE WARRANTIES IN THIS AGREEMENT HAVE FAILED OF THEIR ESSENTIAL PURPOSE.

13. CONFIDENTIALITY

13.1 "**Confidential Information**" means any trade secrets or other information of DocuSign or Subscriber, whether of a technical, business, or other nature (including, without limitation, in the case of DocuSign, DocuSign software and related information, and in the case of Subscriber, Personal Data and eContracts), that is disclosed to the other party (the "Recipient"). Confidential Information does not include any information that: (a) was known to Recipient prior to receiving it from the disclosing party; (b) is independently developed by Recipient without use of or reference to any Confidential Information of the other party; (c) is acquired by Recipient from another source that did not receive it in confidence from the other party to this Agreement; or (d) is or becomes part of the public domain through no fault or action of Recipient.

13.2 **Restricted Use and Nondisclosure.** During and after the Term, Recipient will: (a) use the Confidential Information of the other party solely for the purpose for which it is provided; (b) not disclose such Confidential Information to a third party; and (c) protect such Confidential Information from unauthorized use and disclosure to the same extent (but using no less than a reasonable degree of care) that it protects its own Confidential Information of a similar nature.

13.3 **Required Disclosure**. If Recipient is required by law to disclose Confidential Information of the other party or the terms of this Agreement, Recipient must give prompt written notice of such requirement before such disclosure and assist the disclosing party to obtain where reasonably available an order protecting the Confidential Information from public disclosure.

13.4 **Return of Materials.** Except for as provided in Section 7.4, upon written request by the disclosing party, Recipient will destroy or deliver to the disclosing party all of the disclosing party's Confidential Information that Recipient may have in its possession or control.

13.5 **Ownership**. Recipient acknowledges that, as between the parties, all Confidential Information it receives from the disclosing party, including all copies thereof in Recipient's possession or control, in any media, is proprietary to and exclusively owned by the disclosing party. Nothing in this Agreement grants Recipient any right, title or interest in or to any of the disclosing party's Confidential Information. Recipient's incorporation of the disclosing party's Confidential Information into any of its own materials shall not render Confidential Information non-confidential.

13.6 **Remedies**. Recipient acknowledges that any actual or threatened violation of this confidentiality provision may cause irreparable, non-monetary injury to the disclosing party, the extent of which may be difficult to ascertain, and therefore agrees that the disclosing party shall be entitled to seek injunctive relief in addition to all remedies available to the disclosing party at law and/or in equity. Absent written consent of the disclosing party, the burden of proving that the disclosing party's Confidential Information is not, or is no longer, confidential or a trade secret shall be on the Recipient.

13.7 **Existing Obligations.** The obligations in this Section 13 are in addition to, and supplement, each party's obligations of confidentiality under applicable law and/or under any nondisclosure or other agreement between the parties.

14. GENERAL

14.1 **Relationship**. At all times, the parties are independent actors, and are not the agent or representative of the other. This Agreement is not intended to create a joint venture, partnership, or franchise relationship, or give rise to any third party beneficiary. Subscriber must not represent to anyone that Subscriber is an agent of DocuSign or is otherwise authorized to bind or commit DocuSign in any way without DocuSign's prior authorization.

14.2 **Assignability**. Subscriber may not assign its rights, duties, or obligations under this Agreement without DocuSign's prior written consent. If consent is given, this Agreement will bind Subscriber's successors and assigns. Any attempt by Subscriber to transfer its rights, duties, or obligations under this Agreement except as expressly provided in this Agreement is void. Notwithstanding the foregoing, either party may assign this Agreement to a successor of its business without the other party's consent.

14.3 **Nonsolicitation**. During the Term of this Agreement and for a period of one year thereafter, Subscriber will not, directly or indirectly, employ or solicit the employment or services of a DocuSign employee or independent contractor without the prior written consent of DocuSign.

14.4 **Notices**. Any notice required or permitted to be given in accordance with this Agreement will be effective if it is in writing and sent using: (a) the "acknowledge receipt" function of the Subscription Service; (b) by certified or registered mail; or (c) insured courier, to the appropriate party at the address set forth on the Order Form. Either party may change its address for receipt of notice by notice to the other party in accordance with this Section. Notices are deemed given upon receipt if delivered using the Subscription Service, two business days following the date of mailing, or one business day following delivery to a courier.

14.5 **Force Majeure.** Except for any payment obligations, neither party will be liable for, or be considered to be in breach of or default under this Agreement on account of, any delay or failure to perform as required by this Agreement as a result of any cause or condition beyond such party's reasonable control, so long as such party uses all commercially reasonable efforts to avoid or remove such causes of non-performance or delay.

14.6 **Dispute Resolution**. In the event of any dispute regarding any right or obligation under this Agreement, the aggrieved party shall notify the other party in a writing describing the dispute ("Notice of Dispute"). Upon receipt of the Notice of Dispute, the parties shall arrange a meeting between their representatives. Over a period not to exceed 10 business days after receipt of Notice of Dispute ("Period"), the parties shall engage in good faith negotiations to resolve such dispute. If the parties' representatives are unable to resolve the dispute at such meetings during the Period, then each party may seek any remedies available to it in law or equity. Notwithstanding the foregoing, either party may seek injunctive relief at any time. Each party hereby irrevocably waives, to the fullest extent permitted by law, any and all right to trial by jury in any legal proceeding arising out of or relating to this Agreement.

14.7 **Governing Law**. This Agreement will be interpreted, construed, and enforced in all respects in accordance with the local laws of the State of Washington, U.S.A., without reference to its choice of law rules to the contrary. The provisions of the 1980 U.N. Convention on Contracts for the International Sale of Goods are expressly excluded and do not apply to this Agreement. Any legal action by Subscriber arising under this Agreement must be initiated within two years after the cause of action arises.

14.8 **Waiver**. The waiver by either party of any breach of any provision of this Agreement does not waive any other breach. The failure of any party to insist on strict performance of any covenant or obligation in accordance with this Agreement will not be a waiver of such party's right to demand strict compliance in the future, nor will the same be construed as a novation of this Agreement.

14.9 **Severability**. If any part of this Agreement is found to be illegal, unenforceable, or invalid, the remaining portions of this Agreement will remain in full force and effect. If any material limitation or restriction on the grant of any license to Subscriber under this Agreement is found to be illegal, unenforceable, or invalid, the license will immediately terminate.

14.10 **Counterparts**. This Agreement may be executed in any number of identical counterparts, notwithstanding that the parties have not signed the same counterpart, with the same effect as if the parties had signed the same document. All counterparts will be construed as and constitute the same agreement.

14.11 **Entire Agreement**. This Agreement is the final and complete expression of the agreement between these parties regarding the DocuSign Products. This Agreement supersedes, and the terms of this Agreement govern, all previous oral and written communications regarding these matters. This Agreement may be changed only by a written agreement signed by an authorized agent of both parties.

ADDITIONAL TERMS AND CONDITIONS FOR CONSULTING SERVICES

The following additional terms and conditions apply to Consulting Services, if any, that are made the subject of an Order Form.

15. SERVICES, WORK ORDERS, AND CHANGE ORDERS

15.1 **Services**. Subject to the terms and conditions of this Agreement, DocuSign will, if ordered as provided hereunder, perform for Subscriber certain Consulting Services.

15.2 **Work Orders**. The specific details of the Consulting Services to be performed will be determined on a per-project basis, and the details for each project will be described in a Work Order that is executed by both parties (called the "Work Order" for purposes of the Consulting Services). An Order Form that lists a DocuSign standard training or consulting package as a DocuSign Product constitutes a Work Order. Once executed by both parties, each Work Order will be a unique agreement that incorporates the terms of this Agreement and stands alone with respect to all other Order Forms. If there is a conflict between the terms of this Agreement and the terms of a Work Order, the terms of this Agreement will control unless the Work Order states that a specific provision of this Agreement will be superseded by a specific provision of the Work Order.

15.3 **Change Orders**. Unless otherwise specified in a Work Order, Subscriber may reasonably request in writing that revisions be made with respect to the Consulting Services or deliverables set forth in that Work Order ("Change Order"). If a Change Order recites revisions that materially increase the scope of the Consulting Services or the effort required to deliver deliverables under the applicable Work Order, then within 10 business days after DocuSign's receipt of the Change Order, DocuSign will deliver to Subscriber a written, revised Work Order reflecting DocuSign's reasonable determination of the revised Consulting Services, deliverables, delivery schedule, payment schedule, and adjusted fees or fee estimates, if any, that will apply to the implementation of the revisions. If Subscriber approves the revised Work Order, then the parties will execute it, and upon execution, the revised Work Order will supersede the then-existing Work Order. If Subscriber does not approve the revised Work Order within 10 business days after its receipt by Subscriber, the then-existing Work Order will remain in full force and effect, and DocuSign will have no further obligation with respect to the applicable Change Order.

16. PERFORMANCE OF CONSULTING SERVICES

16.1 **Project Management**. For each project described in a Work Order, each party will designate a single point of contact within its organization to manage the project ("Project Leader"). The Project Leaders will meet as necessary to manage the Consulting Services to be performed under a Work Order. Disputes will be escalated to more senior executives if the Project Leaders are unable to resolve a problem. DocuSign's Project Leader will provide Subscriber's Project Leader with regular reports on the status of the Consulting Services at least once per month.

16.2 **Performance Standard**. DocuSign warrants to Subscriber that the Consulting Services will be performed in a good and workmanlike manner in accordance with standard industry practice and the applicable Work Order, including any specifications

in such Work Order. DocuSign will complete the Consulting Services, including the delivery of any deliverables, in accordance with the schedule of times and milestones specified in the Work Order.

16.3 **Fees**. Unless otherwise specified in a Work Order, Subscriber will pay DocuSign for Consulting Services on a time-and-materials basis at DocuSign's then-current rates and under payment terms described in this Agreement ("Consulting Fees").

16.4 **Disclaimer**. EXCEPT FOR WARRANTIES PROVIDED HEREIN OR EXPRESSLY IDENTIFIED AS SUCH IN A WORK ORDER, THE CONSULTING SERVICES AND ANY RELATED DELIVERABLES WILL BE PROVIDED AS-IS AND WITHOUT WARRANTY OF ANY KIND. DOCUSIGN EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT AS TO ANY AND ALL CONSULTING SERVICES AND RELATED DELIVERABLES.

17. TERM AND TERMINATION OF WORK ORDERS

17.1 **Term**. Each Work Order is non-cancellable except pursuant to a Change Order, and will commence on the specified effective date and will continue until each party's obligations under the Work Order have been fulfilled or the Work Order is terminated as provided in the Work Order.

17.2 **Effect of Termination**. If any Work Order is terminated in accordance with this Section 17, then Subscriber will pay to DocuSign any Consulting Fees and all other payment obligations accrued and payable for the Consulting Services performed under the terminated Work Order through the effective date of the termination. If a Work Order is terminated for any reason other than for material breach by DocuSign, Subscriber will pay to DocuSign all Consulting Fees due under the Work Order had the Work Order not been terminated and had the Consulting Services been fully performed in accordance with the schedule then in effect, which amount owing will be evidenced in a final termination invoice to be provided by DocuSign to Subscriber. The amount of Consulting Services Fees specified in such termination invoice from DocuSign will be final and binding on the parties, absent manifest error.

18. PROPRIETARY RIGHTS

18.1 **Subscriber Materials**. Any materials provided by Subscriber to DocuSign specifically for use by DocuSign in the course of the Consulting Services ("Subscriber Materials") will be used and disclosed solely as required to perform the Consulting Services. As between the parties, Subscriber will continue to own the Subscriber Materials.

18.2 **Inventions**. Except as expressly set forth to the contrary in a Work Order, all works of authorship, inventions, discoveries, improvements, methods, processes, formulas, designs, techniques, and information: (a) conceived, discovered, developed or otherwise made by DocuSign, solely or in collaboration with others, in the course of performing the Consulting Services; or (b) that form all or part of a deliverable provided as part of the Consulting Services, whether developed as part of the Consulting Services or separately, but excluding Subscriber Materials (as defined in Section 18.1) (collectively, "Inventions"), will be the sole property of DocuSign. Upon and subject to final payment by Subscriber of all amounts owing to DocuSign, DocuSign hereby grants to Subscriber a nonexclusive, perpetual, worldwide, royalty-free license to use, copy, modify, and prepare derivative works of the Inventions solely for purposes of Subscriber's internal business operations only.

MASTER PURCHASE AGREEMENT

This Master Purchase Agreement (this "Agreement") is entered into as of [DATE] (the "Effective Date") by and between FireEye (as defined below) and _____, a _____ corporation, with its principal place of business at _____("Customer"). This Agreement will govern Customer's initial purchase of FireEye Offerings and any future orders by Customer as agreed between the parties in writing. FireEye shall provide its Offerings pursuant to the terms and conditions below. For good and valuable consideration, the parties hereby agree as follows:

Structure and Order of Precedence. This Agreement provides the general terms under which the Customer may use FireEye's various Offerings. The explicit rights for the Customer to use and receive Products, Support Services or Subscriptions or otherwise engage with specific FireEye Offerings are set forth in the applicable Exhibit. In the event of conflict between any of the terms in this Agreement and an Exhibit, the Exhibit shall govern.

GENERAL TERMS APPLICABLE TO ALL FIREEYE OFFERINGS

1. DEFINITIONS.

1.1 "Content Feed" means all intelligence and content feeds associated with Products, which may consist of inbound and outbound feeds that are part of FireEye's Dynamic Threat Intelligence (DTI) Cloud, downloads of Indicators for use with Products, and/or intelligence provided as part of the Advanced Threat Intelligence (ATI) Subscription.

1.2 "Deliverables" means the written reports that are created specifically for Customer as a result of the Professional Services provided hereunder.

1.3 "Documentation" means the user manuals generally provided in writing by FireEye to end users of the Products and Subscriptions in electronic format, as amended from time to time by FireEye.

1.4 "FireEye" means (i) FireEye, Inc., a Delaware corporation with its principal place of business at 1440 McCarthy Blvd., Milpitas, CA, 95035 with respect to Offerings that are shipped to, deployed or rendered inside of North America (including the United States, Mexico, Canada and the Caribbean), Central America and South America (collectively, the "Americas"); or (ii) with respect to all Offerings that are shipped to, deployed or rendered outside of the Americas, FireEye Ireland Limited, a company incorporated under the laws of Ireland with principal place of business at 2 Park Place, City Gate Park, Mahon, Cork, Ireland. FireEye includes the operating divisions Mandiant and iSIGHT.

1.5 "FireEye Materials" means all FireEye proprietary materials, Deliverables, intellectual property related to Products or Subscriptions, (such as all rights in any software incorporated into a Product or Subscription, copyrights, and patent, trade secret and trademark rights related to Products, and screens associated with Products or Subscriptions), Documentation, any hardware and/or software used by FireEye in performing Services or providing Subscriptions, Content Feeds, FireEye's processes and methods (including any forensic investigation processes and methods), Indicators of Compromise, materials distributed by FireEye during Training, and any FireEye templates and/or forms, including report and presentation templates and forms. FireEye Materials does not include Third Party Materials.

1.6 "Indicators of Compromise" or "Indicators" means specifications of anomalies, configurations, or other conditions that FireEye is capable of identifying within an information technology infrastructure, used by FireEye in performing Professional Services and providing Subscriptions.

1.7 "Intellectual Property Rights" means copyrights (including, without limitation, the exclusive right to use, reproduce, modify, distribute, publicly display and publicly perform the copyrighted work), trademark rights (including, without limitation, trade names, trademarks, service marks, and trade dress), patent rights (including, without limitation, the exclusive right to make, use and sell), trade secrets, moral rights, right of publicity, authors' rights, contract and licensing rights, goodwill and all other intellectual property rights as may exist now and/or hereafter come into existence and all renewals and extensions thereof, regardless of whether such rights arise under the law of the United States or any other state, country or jurisdiction.

1.8 "Offerings" means, collectively, Products, Subscriptions, Training, Professional Services and Support Services.

1.9 "Order" means a written purchase order or similar ordering document, signed or submitted to FireEye by Customer and approved by FireEye, under which Customer agrees to purchase Offerings.

1.10 "Products" means the FireEye software and hardware appliances (which may include embedded software or firmware components) as described in Exhibit A to this Agreement.

1.11 "Professional Services" means, collectively, those security consulting services provided by FireEye under a Statement of Work and/or set forth on an Order, which may consist of Product-related services such as deployment, configuration or installation services; proactive security consulting such as penetration testing, vulnerability assessments or compromise assessments; or incident response or other remediative services.

1.12 "Service" or "Services" means the Professional Services, Support Services and Training.

1.13 "Statement of Work" or "SOW" means a mutually agreed-upon document between FireEye and Customer, describing Professional Services, rates and timelines (if applicable) for those Professional Services, and incorporating this Agreement.

1.14 "Subscription" means a service provided by FireEye for a fixed term, under which FireEye provides access to certain features, functionality, and/or information, as described in the applicable Exhibit for each Subscription attached to this Agreement.

1.15 "Support Services" means the Product support and maintenance services provided by FireEye with respect to each Product, and that are described in the applicable Exhibit for each Product attached to this Agreement.

1.16 "Third Party Materials" means software or other components that are licensed to FireEye by third parties for use in FireEye's Offerings.

1.17 "Training" means training in the use of Products, or on security-related topics in general, provided by FireEye.

2. ORDERS AND STATEMENTS OF WORK.

2.1. Orders. Customer may purchase Offerings by submitting an Order. If accepted by FireEye, the "Order Effective Date" will be the date of the Order. All Orders will be governed by this Agreement. For clarity, FireEye will not be obligated to ship any Product, or provide any Services, Training or Subscriptions until Customer has issued a valid Order for those Offerings.

2.2. Statements of Work. Each Statement of Work will incorporate and be governed by this Agreement. The "Statement of Work Effective Date" will be the date both Customer and FireEye have agreed to the Statement of Work, either by executing the Statement of Work or by issuing and accepting an Order for the Professional Services described on the Statement of Work. For clarity, FireEye will not be obligated to perform any Professional Services until a SOW describing those Professional Services has been agreed by both parties or an Order listing those Professional Services has been accepted by FireEye.

3. PAYMENT. Customer agrees to purchase the Offerings for the prices set forth in each Order and/or Statement of Work, as applicable ("Fees"). If Customer purchases through a FireEye partner (such as an authorized reseller or distributor, collectively, "FireEye Partners"), all fees and other procurement and delivery terms shall be agreed between Customer and the applicable partner. If Customer purchases directly from FireEye, Customer will make full payment in the currency specified in FireEye's invoice, without set-off and in immediately available funds, within thirty (30) days of the date of each invoice. All Fees are non-cancelable and non-refundable. All Fees described on an Order will be fully invoiced in advance, unless otherwise agreed by FireEye. Unless otherwise specified in a Statement of Work, all Fees related to Professional Services will be invoiced

fully in advance. Customer shall reimburse FireEye for any and all expenses incurred so long as such expenses are directly attributable to the Services or Subscriptions performed for or provided to Customer. FireEye will provide appropriate vouching documentation for all expenses exceeding $25. If any payment is more than fifteen (15) days late, FireEye may, without limiting any remedies available to FireEye, terminate the applicable Order or Statement of Work or suspend performance until payment is made current. Customer will pay interest on all delinquent amounts at the lesser of 1.5% per month or the maximum rate permitted by applicable law. All Fees are exclusive of all present and future sales, use, excise, value added, goods and services, withholding and other taxes, and all customs duties and tariffs now or hereafter claimed or imposed by any governmental authority upon the Offerings which shall be invoiced to and paid by the Customer. If Customer is required by law to make any deduction or withholding on any payments due to FireEye, Customer will notify FireEye and will pay FireEye any additional amounts necessary to ensure that the net amount FireEye receives, after any deduction or withholding, equals the amount FireEye would have received if no deduction or withholding had been required. Additionally, Customer will provide to FireEye evidence, to the reasonable satisfaction of FireEye, showing that the withheld or deducted amounts have been paid to the relevant governmental authority. For purposes of calculating sales and similar taxes, FireEye will use the address set forth on the Order or Statement of Work, as applicable, as the jurisdiction to which Offerings and shipments are delivered unless Customer has otherwise notified FireEye in writing as of the Order Effective Date or Statement of Work Effective Date, as applicable. Customer will provide tax exemption certificates or direct-pay letters to FireEye on or before the Order Effective Date or Statement of Work Effective Date, as applicable. FireEye reserves the right to increase Fees at any time, although increases in Fees for Subscriptions or Support Services will not go into effect until the next Renewal Subscription Term or Renewal Support Term, as applicable.

4. TITLE AND RISK OF LOSS; INSPECTION. All hardware, including Products and any hardware provided for use with Subscriptions and/or Services, is shipped FOB Origin (FCA) from FireEye's designated manufacturing facility or point of origin, and title to such hardware and the risk of loss of or damage to the hardware shall pass to Customer at time of FireEye's delivery of such hardware to the carrier. FireEye is authorized to designate a carrier pursuant to FireEye's standard shipping practices unless otherwise specified in writing by Customer. Customer must provide written notice to FireEye within five (5) days of delivery of the Products of any non-conformity with the Order, e.g., delivery of the wrong Product or incorrect quantities.

5. TERMS APPLICABLE TO OFFERINGS.

5.1. Products and Support Services. Customer's purchase and use of each Product and Support Services for each Product will be subject to the licenses and terms specific to each Product set forth in Exhibit A.

5.2. Subscriptions. Customer's purchase of and access to each Subscription will be subject to the terms specific to each Subscription set forth in Exhibit B.

5.3. Training. Customer's purchase of Training will be subject to the terms in this Section 5.3. Training delivery dates and location for such Training will be mutually agreed upon by the parties. If an Order does not specify such dates and/or locations, then the parties will mutually agree upon the dates and locations for Training. Customer must request rescheduling of Training no less than two (2) weeks in advance of the scheduled start date. FireEye will use reasonable efforts to reschedule the Training, subject to availability, and Customer will pay any expenses associated with the rescheduling, including any expenses associated with cancelling or changing travel plans. If Customer cancels attendance at a public Training class, Customer must notify FireEye no later than two (2) business days before the date of the Training class. If Customer timely notifies FireEye of the cancellation, FireEye will issue Customer a credit for the amount paid for that public Training class, which Customer may apply toward another public Training class held within one (1) year of the date of the Order on which the cancelled Training class was included. Customer may substitute a named attendee at a public Training class, but Customer will notify FireEye in advance of any such substitution. FireEye reserves the right to refuse admittance to public Training classes to any person, for any reason, and if FireEye refuses admittance, FireEye will refund the amount paid for that person's attendance at the public Training class. FireEye does not refund or credit Fees paid for attendees who do not attend Training classes or who leave before a Training class concludes. If Customer purchases a block of Training hours (for example, 10 hours of Training), then Customer must use those hours within one (1) year of the effective date of the applicable Order. All Training must be scheduled and conducted within one (1) year of the date of the applicable Order for that Training.

5.4. Professional Services.

5.4.1. Deliverables. Subject to Customer's timely payment of applicable fees, and subject to this Agreement and each applicable SOW, Customer shall have a perpetual, non-exclusive, nontransferable, right and license to use, display and reproduce the Deliverables for its internal business purposes. Deliverables may not be shared with any third party other than law enforcement agencies. In no event may Deliverables be used for sales or marketing activities.

5.4.2. Customer-Owned Property. Customer will be and remain, at all times, the sole and exclusive owner of the Customer-Owned Property (including, without limitation, any modification, compilation, derivative work of, and all intellectual property and proprietary rights contained in or pertaining thereto). FireEye will promptly return to Customer all Customer-Owned Property upon the termination or expiration of the applicable Statement of Work or Order, or sooner at Customer's request. "Customer-Owned Property" means any technology, software, algorithms, formulas, techniques or know-how and other tangible and intangible items that were owned by Customer, or developed by or for Customer prior to the SOW Effective Date that are provided by Customer to FireEye for incorporation into or used in connection with the development of the Deliverables or performance of Professional Services.

5.4.3. Customer Responsibilities. If the Services or Subscriptions require the installation and use of FireEye equipment or software, Customer will facilitate the installation and shall provide physical space, electrical power, Internet connectivity and physical access as reasonably determined and communicated by FireEye. Notwithstanding anything to the contrary herein or in any Statement of Work, including confidentiality provisions, if Customer has hired FireEye to perform a PCI DSS Compliance Audit or a PCI investigation, FireEye may provide The Payment Card Industry Security Standards Council, LLC (PCI SSC), card companies and the relevant merchant bank with all Reports of Compliance (ROC) and all related assessment and investigative report documents generated in connection with such work, as required by PCI DSS rules.

5.4.4. Additional Assumptions. (a) estimated Fees for Professional Services do not include any hardware, software, licensing, maintenance or support costs of any FireEye or other third-party product or service suggested by FireEye in the course of performing Professional Services; (b) when FireEye's personnel are performing Professional Services on site at Customer's premises, Customer will allocate appropriate working space and physical access for all FireEye personnel; (c) Customer will make available key individuals within the security program that can best help plan and coordinate activities described in the SOW; (d) either party may elect to submit written change requests to the other party proposing changes to the Statement of Work. All changes to the requirements and Statement of Work will be made using agreed-to project change control procedures.

5.5 Evaluations. If Customer receives a Product or Subscription for evaluation purposes ("Evaluation Offerings") then Customer may use the Evaluation Offerings for its own internal evaluation purposes for a period of up to thirty (30) days from the date of receipt of the Evaluation Offerings (the "Evaluation Period"). Customer and FireEye may, upon mutual written agreement (including via email), extend the Evaluation Period. If the Evaluation Offering includes hardware components, Customer will return the hardware within ten (10) days of the end of the Evaluation Period, and if Customer does not return the hardware within this period, Customer shall be invoiced for the then-current list price for the applicable Evaluation Offering. Customer acknowledges that title to hardware components of Evaluation Offerings remains with FireEye at all times, and that Evaluation Offerings may be used and/or refurbished units. If the Evaluation Offering does not include hardware components, Evaluator must delete all software and other components (including Documentation) related to the Evaluation Offering at the end of the Evaluation Period, and confirm those deletions in writing to FireEye, or the Evaluator shall be invoiced for the then-current list price for the Evaluation Offering. If the Evaluation Offering is a Subscription, Evaluator understands that FireEye may disable access to the Subscription automatically at the end of the Evaluation Period, without notice to Evaluator. EVALUATION OFFERINGS ARE PROVIDED "AS IS", AND TO THE EXTENT PERMITTED BY APPLICABLE LAW, FIREEYE DISCLAIMS ALL WARRANTIES RELATING TO THE EVALUATION OFFERINGS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES AGAINST INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

6. INTELLECTUAL PROPERTY

6.1. Ownership of FireEye Materials; Restrictions. All Intellectual Property Rights in FireEye Materials, Products, Deliverables, Documentation, and Subscriptions belong exclusively to FireEye and its licensors. Customer will not (and will not allow any third party to): (i) disassemble, decompile, reverse compile, reverse engineer or attempt to discover any source code or underlying ideas or algorithms of any FireEye Materials (except to the limited extent that applicable law prohibits reverse engineering restrictions); (ii) sell, resell, distribute, sublicense or otherwise transfer, the FireEye Materials, or make the functionality of the FireEye Materials available to any other party through any means (unless otherwise FireEye has provided prior written consent), (iii) without the express prior written consent of FireEye, conduct any benchmarking or comparative study or analysis involving the FireEye Materials ("Benchmarking") for any reason or purpose except, to the limited extent absolutely necessary, to determine the suitability of Products or Subscriptions to interoperate with Customer's internal computer systems; (iv) disclose or publish to any third party any Benchmarking or any other information related thereto; (v) use the FireEye Materials or any Benchmarking in connection with the development of products, services or subscriptions that compete with the FireEye Materials; or (vi) reproduce, alter, modify or create derivatives of the FireEye Materials. Between Customer and FireEye, FireEye shall retain all rights and title in and to any Indicators of Compromise FireEye developed by or for FireEye in the course of providing Subscriptions or performing Services.

6.2. Third Party Materials. Customer acknowledges that Products and Subscriptions may include Third Party Materials. FireEye represents that these Third Party Materials will not diminish the license rights provided herein or limit Customer's ability to use the Products and Subscriptions in accordance with the applicable Documentation, and neither the inclusion of Third Party Materials in any Product or Subscription or use of Third Party Materials in performance of Services will create any obligation on the part of Customer to license Customer's software or products under any open source or similar license.

7. WARRANTIES.

7.1. Product Warranty. FireEye warrants to Customer that during the one (1) year period following the shipment of the Products, the Products will perform substantially in accordance with the applicable Documentation. The warranty stated in this Section 7.1 shall not apply if the Product has: (i) been subjected to abuse, misuse, neglect, negligence, accident, improper testing, improper installation, improper storage, improper handling or use contrary to any instructions issued by FireEye; (ii) been repaired or altered by persons other than FireEye; (iii) not been installed, operated, repaired and maintained in accordance with the Documentation; or (iv) been used with any third party software or hardware which has not been previously approved in writing by FireEye. If during the one-year Product warranty period: (a) FireEye is notified promptly in writing upon discovery of any error in a Product, including a detailed description of such alleged error; (b) such Product is returned, transportation charges prepaid, to FireEye's designated manufacturing facility in accordance with FireEye's then-current return procedures, as set forth by FireEye from time to time; and (c) FireEye's inspections and tests determine that the Product contains errors and has not been subjected to any of the conditions set forth in 7.1(i)-(iv) above, then, as Customer's sole remedy and FireEye's sole obligation under the foregoing warranty, FireEye shall, at FireEye's option, repair or replace without charge such Product. Any Product that has either been repaired or replaced under this warranty shall have warranty coverage for the remaining warranty period. Replacement parts used in the repair of a Product may be new or equivalent to new.

7.2. Services Warranty. FireEye warrants to Customer that Services will be performed in a professional manner in accordance with industry standards for like services. If Customer believes the warranty stated in this Section has been breached, Customer must notify FireEye of the breach no later than thirty (30) days following the date the Services were performed, and FireEye will promptly correct or re-perform the Services, at FireEye's expense.

7.3. Subscription Warranty. FireEye warrants to Customer the Subscriptions will be provided in a professional manner in accordance with industry standards for similar subscriptions. If Customer believes the warranty stated in this Section has been breached, Customer must notify FireEye of the breach no later than thirty (30) days following the date the warranty was allegedly breached, and FireEye will promptly correct the non-conformity, at FireEye's expense.

7.4. Remedies Exclusive. Except for any Service Level Credits described in Exhibit B, the remedies stated in Sections 7.1-7.3 above are the sole remedies, and FireEye's sole obligation, with respect to Products, Subscriptions and Services that fail to comply with the foregoing warranties.

7.5. Disclaimer of Warranties. EXCEPT FOR THE EXPRESS WARRANTIES SET FORTH HEREIN, ALL PRODUCTS, SUBSCRIPTIONS, FIREEYE MATERIALS, DELIVERABLES AND SERVICES ARE PROVIDED ON AN "AS IS" BASIS WITHOUT ANY WARRANTY WHATSOEVER. FIREEYE AND ITS SUPPLIERS EXPRESSLY DISCLAIM, TO THE MAXIMUM EXTENT PERMISSIBLE UNDER APPLICABLE LAW, ALL WARRANTIES, EXPRESS, IMPLIED AND STATUTORY, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, NONINFRINGEMENT, OR ARISING FROM COURSE OF PERFORMANCE, DEALING, USAGE OR TRADE. FIREEYE ALSO MAKES NO WARRANTY REGARDING NONINTERRUPTION OF USE OR FREEDOM FROM BUGS, AND MAKES NO WARRANTY THAT PRODUCTS, FIREEYE MATERIALS, DELIVERABLES, SERVICES OR SUBSCRIPTIONS WILL BE ERROR-FREE.

8. INFRINGEMENT INDEMNITY.

8.1. FireEye shall defend Customer, and its officers, directors and employees, against any third party action alleging that the FireEye Materials infringes a valid U.S. patent or copyright issued as of the date of delivery or performance, as applicable, and FireEye shall pay all settlements entered into, and all final judgments and costs (including reasonable attorneys' fees) finally awarded against such party in connection with such action. If the FireEye Materials, or parts thereof, become, or in FireEye's opinion may become, the subject of an infringement claim, FireEye may, at its option: (i) procure for Customer the right to continue using the applicable FireEye Materials; (ii) modify or replace such FireEye Materials with a substantially equivalent non-infringing FireEye Materials; or (iii) require the return of such FireEye Materials or cease providing affected Product, Subscriptions, Deliverables or Services, and refund to Customer, with respect to Products, a pro-rata portion of the purchase price of such Products based on a three-year straight line amortization of the purchase price, and with respect to Subscriptions, a portion of any pre-paid Fees for such Subscriptions, pro rated for any unused Subscription Term, and with respect to Services, any pre-paid Fees for Services that have not been delivered. THIS SECTION 8.1 STATES THE ENTIRE LIABILITY OF FIREEYE AND CUSTOMER'S SOLE REMEDY WITH RESPECT TO ANY INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS BY THE OFFERINGS, FIREEYE MATERIALS, OR DELIVERABLES.

8.2. FireEye shall have no indemnification obligations with respect to any action arising out of: (i) the use of any Product, Subscription, Deliverable, or Service, or any part thereof, in combination with software or other products not supplied by FireEye; (ii) any modification of the Products, Subscriptions, Deliverables, or Services not performed or expressly authorized by FireEye; or (iii) the use of any the Products, Subscriptions, Deliverables, or Services other than in accordance with this Agreement and applicable Documentation.

8.3. The indemnification obligations shall be subject to Customer: (i) notifying FireEye within ten (10) days of receiving notice of any threat or claim in writing of such action; (ii) giving FireEye exclusive control and authority over the defense or settlement of such action; (iii) not entering into any settlement or compromise of any such action without FireEye's prior written consent; and (iv) providing reasonable assistance requested by FireEye.

9. LIMITATION OF LIABILITY.

9.1. Consequential Damages Waiver. EXCEPT FOR LIABILITY ARISING UNDER A BREACH OF ANY INTELLECTUAL PROPERTY RIGHT OF FIREEYE, OR THE INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 8 (INFRINGEMENT INDEMNITY), IN NO EVENT WILL FIREEYE BE LIABLE FOR ANY SPECIAL, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES OF ANY KIND, INCLUDING BUT NOT LIMITED TO ANY LOST PROFITS AND LOST SAVINGS, HOWEVER CAUSED, WHETHER FOR BREACH OR REPUDIATION OF CONTRACT, TORT, BREACH OF WARRANTY, NEGLIGENCE, OR OTHERWISE, WHETHER OR NOT FIREEYE WAS ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGES.

9.2. Limitation of Monetary Damages. EXCEPT FOR LIABILITY ARISING UNDER A BREACH OF ANY INTELLECTUAL PROPERTY RIGHT OF FIREEYE, PAYMENT OBLIGATIONS OF CUSTOMER, AND THE INDEMNIFICATION OBLIGATIONS SET FORTH IN SECTION 8 (INFRINGEMENT INDEMNITY), AND NOTWITHSTANDING ANY OTHER PROVISIONS OF THIS AGREEMENT OR ANY ORDER OR STATEMENT OF WORK, FIREEYE'S TOTAL LIABILITY ARISING OUT OF THIS AGREEMENT, THE OFFERINGS, THE FIREEYE IP AND DELIVERABLES SHALL BE LIMITED TO THE TOTAL AMOUNTS

RECEIVED BY FIREEYE FOR THE RELEVANT OFFERINGS DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE FIRST OCCURRENCE OF THE EVENTS GIVING RISE TO SUCH LIABILITY.

9.3. Applicability. THE LIMITATIONS AND EXCLUSIONS CONTAINED HEREIN WILL APPLY ONLY TO THE MAXIMUM EXTENT PERMISSIBLE UNDER APPLICABLE LAW, AND NOTHING HEREIN PURPORTS TO LIMIT EITHER PARTY'S LIABILITY IN A MANNER THAT WOULD BE UNENFORCEABLE OR VOID AS AGAINST PUBLIC POLICY IN THE APPLICABLE JURISDICTION.

9.4 SAFETY Act. FireEye and Customer hereby mutually waive and release each other from any and all liabilities relating to any claims for losses or damages of any kind (including, but not limited to, business interruption losses) arising out of an Act of Terrorism as defined by the Support Anti-Terrorism By Fostering Effective Technologies Act of 2002 ("SAFETY Act")(6 U.S.C. §§ 441-444). FireEye and Customer further agree to be solely responsible to the full extent of any and all losses they may sustain, or for any and all losses their respective employees, officers, or agents may sustain, resulting from an Act of Terrorism as defined by 6 U.S.C. §§ 441-444 when FireEye's Multi-Vector Virtual Execution Engine and any subscriptions, cloud services platform or associated services (the "Qualified Anti-Terrorism Technology") are utilized in defense against, response to, or recovery from an Act of Terrorism.

10. Export Control; Anti-Corruption; U.S. Government Restricted Rights.

10.1. Export Control. Export Control. Each party represents and warrants that it shall comply with all laws and regulations applicable to it with respect to the Offerings. Customer further acknowledges and agrees that the Products and FireEye Materials may be subject to restrictions and controls imposed by the United States Export Administration Act, the regulations thereunder, as well as European Union ("EU") or National export control laws and obligations and similar laws in other jurisdictions. Customer agrees to comply with all applicable export and re-export control laws and regulations, including the Export Administration Regulations ("EAR") maintained by the U.S. Department of Commerce, trade and economic sanctions maintained by the Treasury Department's Office of Foreign Assets Control, and the International Traffic in Arms Regulations ("ITAR") maintained by the Department of State. Specifically, Customer covenants that it shall not, directly or indirectly, sell, export, reexport, transfer, divert, or otherwise dispose of any Products, FireEye Materials, or technology (including products derived from or based on such technology) received from FireEye under this Agreement to any destination, entity, or person prohibited by the laws or regulations of the United States and the EU, without obtaining prior authorization from the competent government authorities as required by those laws and regulations. These prohibitions include, but are not limited to the following: (i) the Products and FireEye Materials cannot be exported or re-exported to any countries embargoed by the United States (currently including Cuba, Iran, North Korea, Sudan or Syria) which includes nationals of these countries employed by Customer; (ii) the Products and FireEye Materials cannot be exported or re-exported for military use in country group 'b' prior to valid 'export license' or valid 'license exception'; and (iii) the Products and FireEye Materials cannot be used for any prohibited end uses including any "nuclear, biological or chemical weapon related activities."; and (iv) the Products and FireEye Materials will not be re-exported or otherwise sold or transferred if it is known or suspected that they are intended or likely to be used for such purposes. Customer agrees to notify FireEye of any suspicious activities by any employee related to the Products. Customer agrees to indemnify, to the fullest extent permitted by law, FireEye from and against any fines or penalties that may arise as a result of Customer's breach of this provision. This export control clause shall survive termination or cancellation of any Orders.

10.2. Anticorruption Laws. Each Party acknowledges that it is familiar with and understands the provisions of the U.S. Foreign Corrupt Practices Act ("the FCPA") and the U.K. Bribery Act of 2010 ("UKBA") and agrees to comply with its terms as well as any provisions of local law related thereto. Each party further understands the provisions relating to the FCPA and UKBA's prohibitions regarding the payment or giving of anything of value, including but not limited to payments, gifts, travel, entertainment and meals, either directly or indirectly, to an official of a foreign government or political party for the purpose of influencing an act or decision in his or her official capacity or inducing the official to use his or her party's influence with that government, to obtain or retain business involving the Offering. Each Party agrees to not violate or knowingly let anyone violate the FCPA or UKBA, and Each Party agrees that no payment it makes will constitute a bribe, influence payment, kickback, rebate, or other payment that violates the FCPA, the UKBA, or any other applicable anticorruption or anti-bribery law.

10.3. U.S. Government Restricted Rights. The Offerings, Deliverables and Documentation are "commercial items", "commercial computer software" and "commercial computer software documentation," pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. All Offerings and FireEye Materials are and were developed solely at private expense. Any use, modification, reproduction, release, performance, display or disclosure of the Offerings, FireEye Materials and Documentation by the United States Government shall be governed solely by the this Agreement and shall be prohibited except to the extent expressly permitted by this Agreement.

11. CONFIDENTIAL INFORMATION.

11.1. Confidential Information. "Confidential Information" means the non-public information that is exchanged between the parties, provided that such information is: (i) identified as confidential at the time of disclosure by the disclosing party ("Discloser"); or (ii) disclosed under circumstances that would indicate to a reasonable person that the information should be treated as confidential by the party receiving such information ("Recipient"). The terms of any commercial transaction between the parties (including pricing related to the Offerings) shall be considered Confidential Information.

11.2. Maintenance of Confidentiality. Each party agrees that it shall: (i) take reasonable measures to protect the Confidential Information by using the same degree of care, but no less than a reasonable degree of care, to prevent the unauthorized use, dissemination or publication of the Confidential Information as the Recipient uses to protect its own confidential information of a like nature; (ii) limit disclosure to those persons within Recipient's organization with a need to know and who have previously agreed in writing, prior to receipt of Confidential Information either as a condition of their employment or in order to obtain the Confidential Information, to obligations similar to the provisions hereof; (iii) not copy, reverse engineer, disassemble, create any works from, or decompile any prototypes, software or other tangible objects which embody the other party's Confidential Information and/or which are provided to the party hereunder; and (iv) comply with, and obtain all required authorizations arising from, all U.S. and other applicable export control laws or regulations.. Confidential Information shall not be used or reproduced in any form except as required to accomplish the purposes and intent of an Order or Statement of Work. Any reproduction of Confidential Information shall be the property of Discloser and shall contain any and all notices of confidentiality contained on the original Confidential Information.

11.3. Exceptions. The parties agree that the foregoing shall not apply to any information that Recipient can evidence: (i) is or becomes publicly known and made generally available through no improper action or inaction of Recipient; (ii) was already in its possession or known by it prior to disclosure by Discloser to Recipient; (iii) is independently developed by Recipient without use of or reference to any Confidential Information; or (iv) was rightfully disclosed to it by, or obtained from, a third party. Recipient may make disclosures required by law or court order provided that Recipient: (a) uses diligent efforts to limit disclosure and to obtain, if possible, confidential treatment or a protective order; (b) has given prompt advance notice to Discloser of such required disclosure; and (c) has allowed Discloser to participate in the proceedings.

11.4. Injunctive Relief. Each party will retain all right, title and interest to such party's Confidential Information. The parties acknowledge that a violation of the Recipient's obligations with respect to Confidential Information may cause irreparable harm to the Discloser for which a remedy at law would be inadequate. Therefore, in addition to any and all remedies available at law, Discloser shall be entitled to seek an injunction or other equitable remedies in all legal proceedings in the event of any threatened or actual violation of any or all of the provisions hereof.

11.5. Return of Confidential Information. Within thirty (30) days after the date when all Orders and SOWs have expired or been terminated, or after any request for return of Confidential Information, each party will return to the other party or destroy all of such other party's Confidential Information, at such other party's discretion, and, upon request, provide such other party with an officer's certificate attesting to such return and/or destruction, as appropriate.

11.6. Privacy. If FireEye is a data processor under this Agreement, further to the provisions of Article 17 and 25 of the EU Data Protection Directive EU (Directive 95/46/EC), FireEye agrees that it will:

11.6.1 only deal with and process personal data controlled by Customer in compliance with, and subject to, the instructions received from Customer and in compliance with this Agreement and will not use or process the personal data for any other purpose whatever;

11.6.2 adopt and maintain appropriate (including organizational and technical) security measures in dealing with Customer's personal data in order to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of such data, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing; and

11.6.3 take all reasonable steps to ensure that (i) persons employed by it, and (ii) other persons engaged at its place of work, are aware of and comply with applicable data privacy laws and regulations.

11.6.4 FireEye may process or otherwise transfer any personal information in or to any country outside the European Economic Area or any country not deemed adequate by the European Commission pursuant to Article 25(6) to the extent necessary for the provision of the Offerings. If required, FireEye will enter into the EU Standard Contractual Clauses as approved by the European Commission for ensuring an adequate level of data protection in respect of the personal information that will be processed or transferred.

12. TERM AND TERMINATION.

12.1. Term.

12.1.1 Products. Products will be licensed according to the applicable terms in Exhibit A, for the period of time stated on the Order (e.g., if the Order lists a Product as being provided for "3Y," the license for that Product is provided for three years from the date of the Order). If no period of time is stated on the Order, then the Product is licensed perpetually, unless otherwise terminated as set forth herein.

12.1.2 Support Services. Support Services will begin ten (10) days from the date of shipment of the associated Product and continue for the period of time stated on the Order("Initial Support Term"). Unless otherwise stated on the Order, the Support Services will automatically renew for additional periods of one (1) year each (each, a "Renewal Support Term" and together with the Initial Support Term, the "Support Term"), unless either party notifies the other of its intention not to renew Support Services at least sixty (60) days prior to the expiration of the then-current Support Term. Customer may terminate Support at any time, for convenience, on thirty (30) days' written notice to FireEye. If Customer terminates Support Services for convenience before the end of the then-current Support Term, Customer will pay any remaining fees owing for the remainder of the then-current Support Term within thirty (30) days of the effective date of termination.

12.1.3 Subscriptions. The term of each Subscription will begin on the Order Effective Date and will continue in effect for the period of time stated in the Order ("Initial Subscription Term"). Unless otherwise stated on the Order, the Subscription will automatically renew after its Initial Subscription Term for additional periods of one (1) year each (each, a "Renewal Subscription Term" and together with the Initial Subscription Term, the "Subscription Term"), unless either party notifies the other of its intention not to renew that Subscription at least sixty (60) days prior to the expiration of the then-current Subscription Term. Customer may terminate a Subscription at any time, for convenience, on thirty (30) days' written notice to FireEye. If Customer terminates a Subscription for convenience before the end of the then-current Subscription Term, Customer will pay any remaining fees owing for the remainder of the then-current Subscription Term within thirty (30) days of the effective date of termination.

12.1.4 Professional Services; Statements of Work. Professional Services described on an Order will be provided at mutually agreed-upon times, and will continue until complete, unless otherwise terminated as set forth herein. The term of each SOW will be as set forth in that SOW. If no term is expressed in an SOW, then the term of that SOW will begin on the SOW Effective Date and continue until the Professional Services described in that SOW are complete or the SOW is earlier terminated as set forth herein. Unless otherwise stated in a SOW, Customer may terminate a SOW at any time for convenience by giving FireEye at least thirty (30) days' written notice of its intent to terminate the SOW. If Customer terminates an SOW for convenience as set forth in this Section, Customer will pay any amounts owing for Professional Services and Deliverables provided under that SOW up to and including the date of termination. Customer may request that FireEye suspend performing Professional Services during the term of a Statement of Work, and FireEye will suspend such Professional Services within 24 hours of Customer's request. Customer acknowledges that any such suspension will not affect Customer's obligation to pay fees for Professional Services rendered through the date of suspension, and that

resumption of Professional Services may be delayed if FireEye redeploys personnel to other engagements during the period of suspension.

12.2. Termination for Material Breach. Either party may terminate any Order or any SOW upon written notice of a material breach of the applicable Order or SOW by the other party as provided below, subject to a thirty (30) day cure period ("Cure Period"). If the breaching party has failed to cure the breach within the Cure Period after the receipt by the breaching party of written notice of such breach, the non-breaching party may give a second notice to the breaching party terminating the applicable Order or SOW. Termination of any particular Order or SOW under this Section will not be deemed a termination of any other Order or SOW, unless the notice of termination states that another Order or SOW is also terminated. Notwithstanding the foregoing, the Cure Period applicable to a breach by Customer of any payment obligations under any Order or any SOW will be fifteen (15) days. Notwithstanding the foregoing, this Agreement shall terminate automatically in the event Customer has breached any license restriction and, in FireEye's determination, that breach cannot be adequately cured within the Cure Period.

12.3. Effect of Termination. Termination or expiration of any Order or SOW will not be deemed a termination or expiration of any other Orders or SOWs in effect as of the date of termination or expiration, and this Agreement will continue to govern and be effective as to those outstanding Orders and SOWs until those Orders and SOWs have expired or terminated by their own terms or as set forth herein. The provisions of Section 3 (Payment), Section 6 (Intellectual Property), Section 7.5 (Disclaimer of Warranties), 9 (Limitation of Liability), 10 (Export Control; Anti-Corruption; U.S. Government Restricted Rights), 12 (Confidential Information), and 13 (Miscellaneous), and all accrued payment obligations, shall survive the termination of all Orders and SOWs and the relationship between FireEye and Customer.

13. MISCELLANEOUS.

13.1. Assignment. Customer may not assign any Order or Statement of Work, or any rights or obligations thereunder, in whole or in part, without FireEye's prior written consent, and any such assignment or transfer shall be null and void. FireEye shall have the right to assign all or part of an Order or Statement of Work without Customer's approval. Subject to the foregoing, each Order and Statement of Work shall be binding on and inure to the benefit of the parties' respective successors and permitted assigns.

13.2. Entire Agreement. This Agreement along with any Order, Statement of Work and the Exhibits attached hereto is the entire agreement of the parties with respect to the Offerings and supersedes all previous or contemporaneous communications, representations, proposals, commitments, understandings and agreements, whether written or oral, between the parties regarding the subject matter thereof. FireEye does not accept, expressly or impliedly and FireEye hereby rejects and deems deleted any additional or different terms or conditions that Customer presents, including, but not limited to, any terms or conditions contained or referenced in any order, acceptance, acknowledgement, or other document, or established by trade usage or prior course of dealing. This Agreement may be amended only in writing signed by authorized representatives of both parties.

13.3. Force Majeure. Neither party will be liable to the other for any delay or failure to perform any obligation under this Agreement (except for a failure to pay fees) if the delay or failure is due to unforeseen events, which occur after the signing of this Agreement and which are beyond the reasonable control of the parties, such as strikes, blockade, war, terrorism, riots, natural disasters, refusal of license by the government or other governmental agencies, in so far as such an event prevents or delays the affected party from fulfilling its obligations and such party is not able to prevent or remove the force majeure at reasonable cost.

13.4. Governing Law. This Agreement shall be deemed to have been made in, and shall be construed pursuant to the laws of the State of California and the United States without regard to conflicts of laws provisions thereof, and without regard to the United Nations Convention on the International Sale of Goods or the Uniform Computer Information Transactions Act. Any legal suit, action or proceeding arising out of or relating to the Offerings, the FireEye Materials, this Agreement, an Order or a Statement of Work will be commenced exclusively in a federal court in the Northern District of California or in state court in Santa Clara County, California, and each party hereto irrevocably submits to the jurisdiction and venue of any such court in any such suit, action or proceeding.

13.5. Independent Contractors. The parties are independent contractors. Nothing in this Agreement, any Order or any Statement of Work shall be construed to create a partnership, joint venture or agency relationship between the parties. Customer shall make no representations or warranties on behalf of FireEye.

13.6. Language. This Agreement and each Order and Statement of Work are in the English language only, which shall be controlling in all respects. All communications, notices, and Documentation to be furnished hereunder shall be in the English language only.

13.7. Notices. All notices required to be sent hereunder shall be in writing, addressed to receiving party's current business contact, if known, with a cc: to the General Counsel/Legal Department of the receiving party, and sent to the party's address as listed in this Agreement, or as updated by either party by written notice. Notices shall be effective upon receipt and shall be deemed to be received as follows: (i) if personally delivered by courier, when delivered; or (ii) if mailed by first class mail, or the local equivalent, on the fifth business day after posting with the proper address.

13.8. Severability. If any provision of this Agreement is held to be illegal, invalid or unenforceable under the laws of any jurisdiction, the provision will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remaining provisions of this Agreement will remain in full force and effect.

13.9. Third Party Rights. Other than as expressly set out in this Agreement, this Agreement does not create any rights for any person who is not a party to it and no person who is not a party to this Agreement may enforce any of its terms or rely on any exclusion or limitation contained in it.

13.10. Waiver. The waiver of a breach of any provision of this Agreement shall not constitute a waiver of any other provision or any subsequent breach.

13.11. Equal Opportunity. FireEye is committed to the provisions outlined in the Equal Opportunity Clauses of Executive Order 11246, the Rehabilitation Act of 1973, the Vietnam Era Veterans Readjustment Act of 1974, the Jobs for Veterans Act of 2003, as well as any other regulations pertaining to these orders.

Wherefore, the parties have caused this Master Purchase Agreement to be executed as of the Effective Date.

FIREEYE, INC.

Signature: _____

Name: _____

Title: _____

Date: _____

CUSTOMER

Signature: _____

Name: _____

Title: _____

Date: _____

FIREEYE IRELAND LIMITED

Signature: _____

Name: _____

Title: _____

Date: _____

EXHIBIT A
PRODUCT LICENSE AND SUPPORT TERMS
(FIREEYE NX, EX, AX, PX, FX, HX, SECURITY ORCHESTRATOR™, MVX SMART GRID, AND CENTRAL MANAGEMENT SERIES (CMS) PRODUCTS)

The following terms apply to the FireEye NX, EX, AX, PX, FX, HX, Security Orchestrator, MVX Smart Grid, and Central Management Series (CMS) Products, including any add-on features such as FireEye Advanced Threat Intelligence (ATI).

1. **Grant of License and Restrictions.** Subject to the terms hereof, payment of all fees, and any applicable user/use limitations, FireEye grants Customer a personal, perpetual, nonsublicensable, nonexclusive, right to use the Product, in accordance with the Agreement and this Exhibit A. Customer will maintain the copyright notice and any other notices that appear on the Product, including any interfaces related to the Product. With respect to the FireEye HX Series Product, Customer may install the "agent" software component of the Product on the number of Nodes stated on the applicable Order. With respect to the FireEye EX Series Product, Customer may use the Product in connection with the number of attached URL engines (i.e., email accounts) ("Attached URL Engines") stated on the applicable Order. FireEye reserves the right to audit Customer's use of the Product to ensure compliance with this Agreement. "Nodes" are endpoint computing devices owned or controlled by Customer (such as laptops, workstations, and servers), on which Customer installs the agent software. Updates, preview features, Content Feeds and/or Support Services are not necessarily provided with the Software, may require additional payment or include additional terms and conditions, and may be provided on a "preview" basis for a limited period at no additional charge but then licensed for an additional fee at a later date. Customer acknowledges that Third Party Software distributed with the Products may be subject to separate license terms, and specifically, if the Oracle™ Java® software is included within the Product, that software is subject to the license found at http://www.oracle.com/technetwork/java/javase/terms/license/index.html.

2. **Content Feeds.** Subject to Customer's payment in full of all associated fees for the applicable FireEye Content Feed, as set forth on the applicable Order, FireEye shall grant a limited, non-exclusive, personal, non-transferable, non-sublicenseable right to use the Content Feed as set forth in the Documentation for the applicable Product, for Customer's internal business purposes during the active Support Term for the applicable Product. FireEye shall not disclose to any third party any personally identifiable data or Customer Confidential Information in connection with the Content Feed unless expressly authorized to do so by Customer. The Content Feeds available to the Customer with respect to the Products may include:

2.1 FireEye Dynamic Threat Intelligence™ (DTI™) – The DTI Content Feed (currently available only for customers who have purchased the FireEye NX, EX, AX, HX or FX Product) provides continual, updated information to the Product about threats.

2.2. FireEye Advanced Threat Intelligence™ (ATI™) – The ATI Content Feed (currently available only for customers who have purchased the FireEye NX Product) provides contextual information about malware detected in Customer's environment, such as information regarding threat groups associated with certain malware, industry verticals in which FireEye has observed certain threat groups operate and in which certain malware is used, and relative frequency of observation of various threats and malware.

3. Support Services. Subject to Customer's payment in full of all associated fees for FireEye Support Services, FireEye shall provide Support Services for the Products as set forth in Exhibit C, as may be updated by FireEye in its discretion.

EXHIBIT B
SUBSCRIPTION TERMS

EXHIBIT B-1
SUBSCRIPTION TERMS FOR FIREEYE AS A SERVICE (FAAS) – CONTINUOUS PROTECTION

The following terms govern the FireEye as a Service (FaaS) – Continuous Protection (CP) Subscription.

1 Definitions.

1.1 "**Alert**" means, individually and collectively, APT Alerts, High Priority Alerts, and Low Priority Alerts.

1.2 "**APT Alert**" means (a) with respect to Products other than HX, an alert generated by a Product, that is identified by the Product as being associated with a "targeted threat," which means advanced persistent threat (APT) actors or APT activity; (b) with respect to the HX Product, an alert designated by HX as XPLT, EXC, or PRE, that is triggered by a FireEye standard Indicator; and (c) with respect to the TAP Subscription, an "APT Alert" means a TAP Alert designated as an "APT Alert" in the table in Section 1.11 below.

1.3 "**APT Only Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of APT Alert. If Customer purchases the APT Only Service, FireEye will provide FaaS Reports and monitoring of only APT Alerts, and not any other Alerts.

1.4 "**Covered System**" means (i) a computing device (to the extent supported by FireEye) that Customer specifies as within the scope of the CP Subscription, and if the Customer has purchased the HX Product, on which a software agent has been installed to support CP Subscription delivery, or (ii) a computing device (to the extent supported by FireEye) whose network traffic is observable to support CP Subscription delivery; (iii) with respect to ETP Subscriptions, mailboxes monitored to support CP Subscription delivery; or (iv) any computing device that both Customer and FireEye agree is within scope of the CP Subscription.

1.5 "**Full Coverage Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of all Alerts, regardless of the severity level of the Alert as classified by the Product.

1.6 "**High Priority Alert Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of High Priority Alerts and APT Alerts.

1.7 "**FaaS Reports**" means the written reports relating to Alerts that FireEye creates and makes available to Customer through the CP Subscription.

1.8 "**High Priority Alert**" means (a) with respect to Products other than HX and FX, an alert generated by that Product that is classified by that Product as severity level "critical" or "major"; (b) with respect to the FX Product, any alert generated by the FX Product, including APT Alerts; and (c) with respect to a TAP subscription, a TAP Alert designated as a "High Priority Alert" in the table in Section 1.11 below.

1.9 "**Low Priority Alert**" means an alert generated by a Product or TAP Subscription (as applicable) that is not an APT Alert or a High Priority Alert.

1.10 "**Nodes**" or "**Node Band**" refers to number of Covered Systems within the Customer environment, which is reflected on the Subscription Order.

1.11 "**TAP Alert**" means an alert generated by the TAP Subscription, with a severity level assigned by the TAP Subscription (e.g., "Critical," "High," "Medium"). TAP Alerts are investigated and reported on as "APT Alerts" and "High Priority Alerts" as shown in the table below, depending on the TAP Rule Pack that invoked the TAP Alert:

FireEye Rule Pack	APT Alerts	High Priority Alerts
Application Detection		
Cloud Infrastructure		
Commodity Malware		All

Current Events	Critical, High	Critical, High
DTI Rules		All
Exploit Kits		All
FTP		
Industrial Control Systems	Critical, High, Medium	Critical, High, Medium
Intel Match	Critical, High, Medium	Critical, High, Medium
Linux		Critical, High
Malware Methodology		Critical, High
Phishing	Critical High	Critical, High
Point of Sale	All	All
Security Tools		Critical, High, Medium
Targeted Malware	All	All
Vendor – FireEye		
Vulnerability		Critical, High, Medium
Web Application Attacks		Critical, High, Medium
Windows		Critical, High

1.13 "**TAP Rule Packs**" means a predefined set of criteria that identifies suspicious events or threats based on the associated rule type within the TAP Subscription.

2 **Scope of FaaS – Continuous Protection (CP) Subscription**. During the Subscription Term, FireEye will provide the CP Subscription as set forth in this Section 2, according to the Subscription level purchased by Customer as set forth in the Subscription Order. If the Subscription Order does not specify the Subscription lvel purchased, then Customer will be deemed to have purchased the APT Only Service. All services Customer requests that are not described in this Section 2 will be performed at mutually agreed upon rates as set forth in Statements of Work. Unless otherwise specified, the CP Subscription is provided by FireEye personnel remotely accessing Customer's environment from FireEye's networks. The CP Subscription is available for the number of Nodes purchased (available for Customers who have purchased the FireEye NX, FX, or EX Product or the ETP or TAP Subscription). If the number of Nodes exceeds the amount reflected in the Subscription Order by more than ten percent (10%), FireEye will notify Customer in writing, and will issue an invoice for the next higher Node Band at FireEye's then-current rates pro-rated for the remaining portion of the then-current Subscription Term.

2.1 Event Analysis.

(a) Time to Begin Analysis. FireEye will begin analysis of an Alert within the times set forth in the table below, calculated from the time the Alert was generated by the Product or TAP Subscription (as applicable).

(b) Alerts Investigated. FireEye will investigate and report on the Alerts that correspond with the Subscription level the Customer purchased. If the Customer purchased the APT Only Service, FireEye will investigate and report on only APT Alerts. If the Customer purchased the High Priority Alerts Service, FireEye will investigate and report on only High Priority Alerts and APT Alerts. If the Customer purchased the All Alerts Service, FireEye will investigate and report on APT Alerts, High Priority Alerts, and Low Priority Alerts. FireEye has no obligation to investigate and report on Alerts that fall outside the purchased Subscription level.

(c) Initial Investigation. FireEye analysts will perform an initial analysis of the Customer's Covered Systems to determine if the Alert is a true or false positive, benign or suspicious activity.

(d) FaaS Reports. If FireEye's investigation determines that the Alert indicates a true compromise, FireEye will publish a FaaS Report to the FaaS Portal within one (1) hour of the time FireEye makes that determination. Regardless of whether FireEye's investigation determines that an Alert indicates a true compromise, FireEye will publish a FaaS Report on the Alert to the FaaS Portal within the times set forth in the table

below, based on the classification of the Alert (APT Alert, High Priority Alert, Low Priority Alert). Customer acknowledges that in some cases, when FireEye's investigation is not complete, a FaaS Report may provide only an update of current status of the Alert investigation.

Alerts Investigated (Level of Service)			FaaS Alert Classification	Time to Begin Investigation (from time Product or TAP Subscription generates Alert)	Time to Publish FaaS Report (from time FireEye validates actual compromise)	Time to Publish FaaS Report (when no validation of actual compromise; from time Product or TAP Subscription generates Alert)
APT Only Service	High Priority Alerts Service	Full Coverage Service				
Yes	Yes	Yes	APT Alert	1 hours	1 hour	24 hours
No	Yes	Yes	High Priority Alert	7 hours	1 hour	24 hours
No	No	Yes	Low Priority Alert	24 hours	1 hour	48 hours

The service levels noted in the table above will become effective thirty (30) days following the Order Effective Date, to allow time for Customer to install Products and for FireEye to determine the level of staffing needed to respond to Alerts in Customer's environment.

(e) Extended Investigations; Multiple Related Alerts. When FireEye has identified a true positive or suspicious activity, FireEye analysts may perform an extended investigation, and/or may aggregate and review multiple Alerts from related Covered Systems to determine the extent of activity related to the Alert. FireEye analysts may append results from the extended investigation or subsequent Alert investigations to the initial FaaS Report if FireEye determines that additional or subsequent Alerts are related, and in such cases, FireEye will not be required to issue a separate FaaS Report for each such related Alert.

(f) Non-Remediable Alerts. FireEye has no obligation to notify the Customer or generate a new FaaS Report on new Alerts that are directly related to previous investigations where a FaaS Report has been published and FireEye has provided recommended remediation steps, when the Customer has acknowledged the FaaS Report but chooses not to or cannot remediate the cause of these Alerts.

(g) Alert Priority. FireEye may re-prioritize Alerts, regardless of their severity classification, to provide focus to Alerts that FireEye determines may have the largest impact to the Customer's environment.

(h) Continuity of Monitoring. All monitoring, investigation and reporting activities described in this Section 2.1 will be provided on a 24/7/365 basis.

2.2 System Health Monitoring and Notification. For Customers who have purchased the FireEye NX, EX, or FX Product, FireEye will provide Customer with notifications of system health issues such as connectivity problems.

2.3 Containment. When the Customer has purchased the HX Product, FireEye may, when appropriate, recommend containment of the target Covered System from the Customer's network. Containment must be executed by the Customer.

2.4 Portal Access. Alerts and FaaS Reports will be provided via an online portal ("FaaS Portal"), and FireEye will provide login credentials to the Customer to enable access to the FaaS Portal. The FaaS Portal will be available 99.9% of the time in any calendar month, other than Downtime, as defined below, and this FaaS Portal Service Level commitment will be subject to the Service Level Credits set forth in Section 3 below.

2.5 FireEye Intelligence Center. During the Subscription Term, FireEye will provide access to the FireEye Intelligence Center (FIC), which includes the Community Threat Intelligence (CTI) platform, subject to the following:

(a) Permitted Use; Reports. Customer may access, view and use FIC and content appearing on FIC ("FIC Content") solely for internal use. Some features of FIC may allow Customer to generate a report (each, a "FIC Report"). FIC Reports and FIC Content are FireEye IP. Subject to Customer's payment obligations, FireEye grants to Customer a limited, non-exclusive right to produce FIC Reports using FIC, and reproduce and distribute those FIC Reports and FIC Content internally for Customer's own business purposes.

(b) Additional Use Limitations. Customer may appoint up to fifteen (15) users of FIC at any time. Each day, all users on Customer's account may collectively make up to (A) one hundred (100) queries of IP addresses and domain names and (B) one hundred (100) queries of malware. Customer may request additional queries, to be evaluated by FireEye on a case by case basis.

(c) User Content. "User Content" means any communications, images, sounds, and all the material and information that Customer or anyone using Customer's account contributes to or through FIC, including any contributions to or through the CTI platform (e.g., comments to FIC Content, suspected malware that Customer uploads to FIC). Customer hereby grants FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive, license, including the right to sublicense to third parties, and right to reproduce, fix, adapt, modify, translate, reformat, create derivative works from, publish, distribute, sell, license, transmit, publicly display, publicly perform, or provide access to electronically, broadcast, display, perform, and use and practice such User Content as well as all modified and derivative works thereof. Customer represents that Customer has all necessary rights to grant the license referenced in the preceding sentence. FireEye may use and disclose any of the information it collects about its customers' use of FIC, including CTI, to the extent such information is de-identified.

(d) Restrictions. Customer may not access FIC by any means other than through the interface that is provided or approved by FireEye. Customer will not collect any information from or through FIC using any automated means, including without limitation any script, spider, "screen scraping," or "database scraping" application, and Customer will not damage, disable, overburden, or impair FIC or interfere with any other party's use and enjoyment of FIC.

(e) Customer acknowledges that some optional features and content appearing on FIC may require payment of additional fees.

2.6 Reseller and Partner Purchases. If Customer receives the Subscription via a FireEye authorized services or support partner (a "Partner"), Customer agrees that the Subscription and FaaS Reports may be delivered to Customer through the Partner. Notwithstanding any other confidentiality obligations between the parties, Customer authorizes FireEye to disclose information related to the Subscription and Customer Data to Partner.

2.7 Customer Networks. The Subscription may only be provided for computer systems and networks leased to or owned by Customer, and under Customer's control, up to the number of Nodes allowed, as set forth in the applicable Subscription Order.

2.8 Connectivity Requirements. Unless otherwise specified, the Subscription are provided by FireEye personnel remotely accessing Customer's environment from FireEye's networks. Customer must provide outbound TCP-based connectivity from all Products to FireEye for the establishment of a virtual private network (VPN). Details pertaining to specific network access requirements will be established in conjunction with installation activities.

2.9 **Credential Security.** Customer will be responsible for the following: (a) providing accurate information to FireEye for provisioning access to (and removal of) Customer personnel access to the FaaS Portal; (b) implementing and adhering to strong password standards; (c) providing accurate information to FireEye for domain whitelisting; and (d) reporting any security issues related to the Subscription (including the FaaS Portal) to FireEye immediately.

2.10 **Exclusions.** Notwithstanding anything else contained in this Agreement to the contrary, FireEye shall have no obligation or responsibility to provide the Subscription for (i) Products for which Customer does not have an active Subscription in place; (ii) Products that the Customer (or FireEye or another third party on Customer's behalf) has configured with a one-way feed of FireEye's Dynamic Threat Intelligence (DTI) Subscription; (iii)

Products with an installed FireEye operating system less than version 6.2; (iv) Products that have been declared end of life; (v) Products that have no active Support Service in place; (vi) Products for which software updates have not been applied; (vii) Products that have not been installed and deployed; or (viii) Products that are misconfigured or incorrectly deployed, which prevents the Products from monitoring the Covered Systems. Customer acknowledges that to facilitate FireEye's efficient performance of the Subscription, FireEye may control some features and functionality of the Products, and that such features or functionality may not be available for Customer's independent use during the Subscription Term.

3. FaaS Portal Availability

3.1 FireEye shall undertake commercially reasonable efforts to ensure the FaaS Portal availability for 99.9% of the time during each calendar month.

3.1.1 "Service Outage" is where the FaaS Portal is not available due to a failure or a disruption in the FaaS Portal that is not the result of Scheduled Maintenance, Emergency Maintenance, a force majeure event or of the act or omission of Customer.

3.1.2 "Scheduled Maintenance Period" is the period during which weekly scheduled maintenance of the FaaS Portal may be performed, or a maintenance window otherwise mutually agreed upon by FireEye and Customer.

3.1.3 "Emergency Maintenance" means any time outside of Scheduled Maintenance that FireEye is required to apply critical patches or fixes or undertake other urgent maintenance. If Emergency Maintenance is required, FireEye will contact Customer and provide the expected time frame of the Emergency Maintenance and availability of the FaaS Portal during the Emergency Maintenance.

3.1.4 "System Availability" means the percentage of total time during which the FaaS Portal shall be available to Customer, excluding the Scheduled Maintenance Period, Emergency Maintenance, force majeure events, or acts or omissions of the Customer that cause system downtime.

3.2. Remedy

3.2.1 In the event that the FaaS Portal does not meet the monthly service availability defined in 3.1, FireEye will provide a credit to the Customer in accordance to the table below ("Credit") for a validated SLA Claim (defined below).

Percent of FaaS Portal Availability per Calendar Month	Service Credit
<99.9%	2%
<99.0%	5%
<98.0%	10%

3.2.2 For determining the Credit, the duration of a Service Outage will be measured as the time starting when Customer experiences a disruption in availability of the FaaS Portal and ending when a successful solution or workaround allowing for full restoration of the FaaS Portal is provided by FireEye to Customer. Customer must notify FireEye in writing of any Service Outage no later than fifteen (15) days after the calendar month in which the Service Outage occurred ("SLA Claim") to be entitled to a Credit for that Service Outage.

3.2.3 Any Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Subscription Term for which the Credit applies. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated for non-renewal or for a material uncured breach by Customer, such credits shall become null and void. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated due to a material uncured breach by FireEye, FireEye will promptly pay Customer the amount of the Credit.

3.2.4 Customer shall not be entitled to receive a Credit that exceeds 10% of its prorated monthly Subscription Fee for a Service Outage for the applicable calendar month.

EXHIBIT B-2
SUBSCRIPTION TERMS FOR FIREEYE AS A SERVICE (FAAS) – CONTINUOUS VIGILANCE

The following terms govern the FireEye as a Service (FaaS) – Continuous Vigilance (CV) Subscription.

3 Definitions.

3.1 "**Alert**" means, individually and collectively, APT Alerts, High Priority Alerts, and Low Priority Alerts.

3.2 "**APT Alert**" means (a) with respect to Products other than HX, an alert generated by a Product, that is identified by the Product as being associated with a "targeted threat," which means advanced persistent threat (APT) actors or APT activity; (b) with respect to the HX Product, an alert designated by HX as XPLT, EXC, or PRE, that is triggered by a FireEye standard Indicator; and (c) with respect to the TAP Subscription, an "APT Alert" means a TAP Alert designated as an "APT Alert" in the table in Section 1.11 below.

3.3 "**APT Only Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of APT Alert. If Customer purchases the APT Only Service, FireEye will provide FaaS Reports and monitoring of only APT Alerts, and not any other Alerts.

3.4 "**Covered System**" means (i) a computing device (to the extent supported by FireEye) that Customer specifies as within the scope of the CV Subscription, and if the Customer has purchased the HX Product, on which a software agent has been installed to support CV Subscription delivery, or (ii) a computing device (to the extent supported by FireEye) whose network traffic is observable to support CV Subscription delivery; (iii) with respect to ETP Subscriptions, mailboxes monitored to support CV Subscription delivery; or (iv) any computing device that both Customer and FireEye agree is within scope of the CV Subscription.

3.5 "**Full Coverage Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of all Alerts, regardless of the severity level of the Alert as classified by the Product.

3.6 "**High Priority Alert Service**" means the Subscription level in which FireEye will provide FaaS Reports and monitoring of High Priority Alerts and APT Alerts.

3.7 "**FaaS Reports**" means the written reports relating to Alerts that FireEye creates and makes available to Customer through the CV Subscription.

3.8 "**High Priority Alert**" means (a) with respect to Products other than HX and FX, an alert generated by that Product that is classified by that Product as severity level "critical" or "major"; (b) with respect to the FX Product, any alert generated by the FX Product, including APT Alerts; and (c) with respect to a TAP subscription, a TAP Alert designated as a "High Priority Alert" in the table in Section 1.11 below.

3.9 "**Low Priority Alert**" means an alert generated by a Product or TAP Subscription (as applicable) that is not an APT Alert or a High Priority Alert.

3.10 "**Nodes**" or "**Node Band**" refers to number of Covered Systems within the Customer environment, which is reflected on the Subscription Order.

3.11 "**TAP Alert**" means an alert generated by the TAP Subscription, with a severity level assigned by the TAP Subscription (e.g., "Critical," "High," "Medium"). TAP Alerts are investigated and reported on as "APT Alerts" and "High Priority Alerts" as shown in the table below, depending on the TAP Rule Pack that invoked the TAP Alert:

FireEye Rule Pack	APT Alerts	High Priority Alerts
Application Detection		
Cloud Infrastructure		
Commodity Malware		All

Current Events	Critical, High	Critical, High
DTI Rules		All
Exploit Kits		All
FTP		
Industrial Control Systems	Critical, High, Medium	Critical, High, Medium
Intel Match	Critical, High, Medium	Critical, High, Medium
Linux		Critical, High
Malware Methodology		Critical, High
Phishing	Critical High	Critical, High
Point of Sale	All	All
Security Tools		Critical, High, Medium
Targeted Malware	All	All
Vendor – FireEye		
Vulnerability		Critical, High, Medium
Web Application Attacks		Critical, High, Medium
Windows		Critical, High

1.13 **"TAP Rule Packs"** means a predefined set of criteria that identifies suspicious events or threats based on the associated rule type within the TAP Subscription.

2 **Scope of FaaS – Continuous Vigilance (CV) Subscription**. During the Subscription Term, FireEye will provide the CV Subscription as set forth in this Section 2, according to the Subscription level purchased by Customer as set forth in the Subscription Order. If the Subscription Order does not specify the Subscription lvel purchased, then Customer will be deemed to have purchased the APT Only Service. All services Customer requests that are not described in this Section 2 will be performed at mutually agreed upon rates as set forth in Statements of Work. Unless otherwise specified, the CV Subscription is provided by FireEye personnel remotely accessing Customer's environment from FireEye's networks. The CV Subscription is available for the number of Nodes purchased (available for Customers who have purchased the FireEye NX, FX, or EX Product or the ETP or TAP Subscription). If the number of Nodes exceeds the amount reflected in the Subscription Order by more than ten percent (10%), FireEye will notify Customer in writing, and will issue an invoice for the next higher Node Band at FireEye's then-current rates pro-rated for the remaining portion of the then-current Subscription Term.

2.1 Event Analysis.

(e) Time to Begin Analysis. FireEye will begin analysis of an Alert within the times set forth in the table below, calculated from the time the Alert was generated by the Product or TAP Subscription (as applicable).

(f) Alerts Investigated. FireEye will investigate and report on the Alerts that correspond with the Subscription level the Customer purchased. If the Customer purchased the APT Only Service, FireEye will investigate and report on only APT Alerts. If the Customer purchased the High Priority Alerts Service, FireEye will investigate and report on only High Priority Alerts and APT Alerts. If the Customer purchased the All Alerts Service, FireEye will investigate and report on APT Alerts, High Priority Alerts, and Low Priority Alerts. FireEye has no obligation to investigate and report on Alerts that fall outside the purchased Subscription level.

(g) Initial Investigation. FireEye analysts will perform an initial analysis of the Customer's Covered Systems to determine if the Alert is a true or false positive, benign or suspicious activity.

(h) FaaS Reports. If FireEye's investigation determines that the Alert indicates a true compromise, FireEye will publish a FaaS Report to the FaaS Portal within one (1) hour of the time FireEye makes that determination. Regardless of whether FireEye's investigation determines that an Alert indicates a true compromise, FireEye will publish a FaaS Report on the Alert to the FaaS Portal within the times set forth in the table

below, based on the classification of the Alert (APT Alert, High Priority Alert, Low Priority Alert). Customer acknowledges that in some cases, when FireEye's investigation is not complete, a FaaS Report may provide only an update of current status of the Alert investigation.

Alerts Investigated (Level of Service)			FaaS Alert Classification	Time to Begin Investigation (from time Product or TAP Subscription generates Alert)	Time to Publish FaaS Report (from time FireEye validates actual compromise)	Time to Publish FaaS Report (when no validation of actual compromise; from time Product or TAP Subscription generates Alert)
APT Only Service	High Priority Alerts Service	Full Coverage Service				
Yes	Yes	Yes	APT Alert	1 hours	1 hour	24 hours
No	Yes	Yes	High Priority Alert	7 hours	1 hour	24 hours
No	No	Yes	Low Priority Alert	24 hours	1 hour	48 hours

The service levels noted in the table above will become effective thirty (30) days following the Order Effective Date, to allow time for Customer to install Products and for FireEye to determine the level of staffing needed to respond to Alerts in Customer's environment.

(e) Extended Investigations; Multiple Related Alerts. When FireEye has identified a true positive or suspicious activity, FireEye analysts may perform an extended investigation, and/or may aggregate and review multiple Alerts from related Covered Systems to determine the extent of activity related to the Alert. FireEye analysts may append results from the extended investigation or subsequent Alert investigations to the initial FaaS Report if FireEye determines that additional or subsequent Alerts are related, and in such cases, FireEye will not be required to issue a separate FaaS Report for each such related Alert.

(f) Non-Remediable Alerts. FireEye has no obligation to notify the Customer or generate a new FaaS Report on new Alerts that are directly related to previous investigations where a FaaS Report has been published and FireEye has provided recommended remediation steps, when the Customer has acknowledged the FaaS Report but chooses not to or cannot remediate the cause of these Alerts.

(g) Alert Priority. FireEye may re-prioritize Alerts, regardless of their severity classification, to provide focus to Alerts that FireEye determines may have the largest impact to the Customer's environment.

(h) Hunting. FireEye will conduct periodic proactive hunting techniques on Covered Systems to look for additional indicators of malicious or attacker activity. When FireEye's investigation reveals a compromise, then within one (1) hour of the time FireEye makes that determination, FireEye will publish a FaaS Report related to that activity to the FaaS Portal.

(i) Continuity of Monitoring. All monitoring, investigation and reporting activities described in this Section 2.1 will be provided on a 24/7/365 basis.

2.2 System Health Monitoring and Notification. For Customers who have purchased the FireEye NX, EX, or FX Product, FireEye will provide Customer with notifications of system health issues such as connectivity problems.

2.3 Containment. When the Customer has purchased the HX Product, FireEye may, when appropriate, recommend containment of the target Covered System from the Customer's network. Containment must be executed by the Customer.

2.4 Portal Access. Alerts and FaaS Reports will be provided via an online portal ("FaaS Portal"), and FireEye will provide login credentials to the Customer to enable access to the FaaS Portal. The FaaS Portal will be

available 99.9% of the time in any calendar month, other than Downtime, as defined below, and this FaaS Portal Service Level commitment will be subject to the Service Level Credits set forth in Section 3 below.

2.5 FireEye Intelligence Center. During the Subscription Term, FireEye will provide access to the FireEye Intelligence Center (FIC), which includes the Community Threat Intelligence (CTI) platform, subject to the following:

(f) Permitted Use; Reports. Customer may access, view and use FIC and content appearing on FIC ("FIC Content") solely for internal use. Some features of FIC may allow Customer to generate a report (each, a "FIC Report"). FIC Reports and FIC Content are FireEye IP. Subject to Customer's payment obligations, FireEye grants to Customer a limited, non-exclusive right to produce FIC Reports using FIC, and reproduce and distribute those FIC Reports and FIC Content internally for Customer's own business purposes.

(g) Additional Use Limitations. Customer may appoint up to fifteen (15) users of FIC at any time. Each day, all users on Customer's account may collectively make up to (A) one hundred (100) queries of IP addresses and domain names and (B) one hundred (100) queries of malware. Customer may request additional queries, to be evaluated by FireEye on a case by case basis.

(h) User Content. "User Content" means any communications, images, sounds, and all the material and information that Customer or anyone using Customer's account contributes to or through FIC, including any contributions to or through the CTI platform (e.g., comments to FIC Content, suspected malware that Customer uploads to FIC). Customer hereby grants FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive, license, including the right to sublicense to third parties, and right to reproduce, fix, adapt, modify, translate, reformat, create derivative works from, publish, distribute, sell, license, transmit, publicly display, publicly perform, or provide access to electronically, broadcast, display, perform, and use and practice such User Content as well as all modified and derivative works thereof. Customer represents that Customer has all necessary rights to grant the license referenced in the preceding sentence. FireEye may use and disclose any of the information it collects about its customers' use of FIC, including CTI, to the extent such information is de-identified.

(i) Restrictions. Customer may not access FIC by any means other than through the interface that is provided or approved by FireEye. Customer will not collect any information from or through FIC using any automated means, including without limitation any script, spider, "screen scraping," or "database scraping" application, and Customer will not damage, disable, overburden, or impair FIC or interfere with any other party's use and enjoyment of FIC.

(j) Customer acknowledges that some optional features and content appearing on FIC may require payment of additional fees.

2.6 Reseller and Partner Purchases. If Customer receives the Subscription via a FireEye authorized services or support partner (a "Partner"), Customer agrees that the Subscription and FaaS Reports may be delivered to Customer through the Partner. Notwithstanding any other confidentiality obligations between the parties, Customer authorizes FireEye to disclose information related to the Subscription and Customer Data to Partner.

2.7 Customer Networks. The Subscription may only be provided for computer systems and networks leased to or owned by Customer, and under Customer's control, up to the number of Nodes allowed, as set forth in the applicable Subscription Order.

2.8 Connectivity Requirements. Unless otherwise specified, the Subscription are provided by FireEye personnel remotely accessing Customer's environment from FireEye's networks. Customer must provide outbound TCV-based connectivity from all Products to FireEye for the establishment of a virtual private network (VPN). Details pertaining to specific network access requirements will be established in conjunction with installation activities.

2.9 **Credential Security.** Customer will be responsible for the following: (a) providing accurate information to FireEye for provisioning access to (and removal of) Customer personnel access to the FaaS Portal; (b) implementing and adhering to strong password standards; (c) providing accurate information to FireEye for domain whitelisting; and (d) reporting any security issues related to the Subscription (including the FaaS Portal) to FireEye immediately.

2.10 **Exclusions.** Notwithstanding anything else contained in this Agreement to the contrary, FireEye shall have no obligation or responsibility to provide the Subscription for (i) Products for which Customer does not have an active Subscription in place; (ii) Products that the Customer (or FireEye or another third party on Customer's behalf) has configured with a one-way feed of FireEye's Dynamic Threat Intelligence (DTI) Subscription; (iii) Products with an installed FireEye operating system less than version 6.2; (iv) Products that have been declared end of life; (v) Products that have no active Support Service in place; (vi) Products for which software updates have not been applied; (vii) Products that have not been installed and deployed; or (viii) Products that are misconfigured or incorrectly deployed, which prevents the Products from monitoring the Covered Systems. Customer acknowledges that to facilitate FireEye's efficient performance of the Subscription, FireEye may control some features and functionality of the Products, and that such features or functionality may not be available for Customer's independent use during the Subscription Term.

3. FaaS Portal Availability

3.1 FireEye shall undertake commercially reasonable efforts to ensure the FaaS Portal availability for 99.9% of the time during each calendar month.

3.1.1 "Service Outage" is where the FaaS Portal is not available due to a failure or a disruption in the FaaS Portal that is not the result of Scheduled Maintenance, Emergency Maintenance, a force majeure event or of the act or omission of Customer.

3.1.2 "Scheduled Maintenance Period" is the period during which weekly scheduled maintenance of the FaaS Portal may be performed, or a maintenance window otherwise mutually agreed upon by FireEye and Customer.

3.1.3 "Emergency Maintenance" means any time outside of Scheduled Maintenance that FireEye is required to apply critical patches or fixes or undertake other urgent maintenance. If Emergency Maintenance is required, FireEye will contact Customer and provide the expected time frame of the Emergency Maintenance and availability of the FaaS Portal during the Emergency Maintenance.

3.1.4 "System Availability" means the percentage of total time during which the FaaS Portal shall be available to Customer, excluding the Scheduled Maintenance Period, Emergency Maintenance, force majeure events, or acts or omissions of the Customer that cause system downtime.

3.2. Remedy

3.2.1 In the event that the FaaS Portal does not meet the monthly service availability defined in 3.1, FireEye will provide a credit to the Customer in accordance to the table below ("Credit") for a validated SLA Claim (defined below).

Percent of FaaS Portal Availability per Calendar Month	Service Credit
<99.9%	2%
<99.0%	5%
<98.0%	10%

3.2.2 For determining the Credit, the duration of a Service Outage will be measured as the time starting when Customer experiences a disruption in availability of the FaaS Portal and ending when a successful solution or workaround allowing for full restoration of the FaaS Portal is provided by FireEye to Customer. Customer must notify FireEye in writing of any Service Outage no later than fifteen (15) days after the calendar month in which the Service Outage occurred ("SLA Claim") to be entitled to a Credit for that Service Outage.

3.2.3 Any Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Subscription Term for which the Credit applies. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated for non-renewal or for a material uncured breach by Customer, such credits shall become null and void. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated due to a material uncured breach by FireEye, FireEye will promptly pay Customer the amount of the Credit.

3.2.4 Customer shall not be entitled to receive a Credit that exceeds 10% of its prorated monthly Subscription Fee for a Service Outage for the applicable calendar month.

EXHIBIT B-3
SUBSCRIPTION TERMS FOR FIREEYE THREAT ANALYTICS PLATFORM (TAP)

The following terms govern the Threat Analytics Platform Subscription, including purchase and support of TAP Cloud Collector™ Appliances and Support.

1. TAP Software, Alerts

1.1.1 TAP Software and Hardware. As part of the TAP Subscription, FireEye may deliver to Customer one or more software files (individually and collectively, "TAP Software"), and/or one or more "Cloud Collector" hardware appliances ("Cloud Collector Appliances"), which may contain TAP Software. Subject to full payment of all Fees associated with the TAP Subscription, FireEye grants to Customer a non-exclusive, limited right and license to install and run the TAP Software during the Subscription Term solely for purposes of using the TAP Subscription in accordance with the Documentation for the TAP Subscription.

1.1.2 Access; Customer Logs. FireEye will provide Customer with credentials to enable access to the TAP Subscription. Using the TAP Software, and subject to payment of Fees for the TAP Subscription and any Cloud Collector Appliances, Customer may upload Customer Logs to the TAP portal ("TAP Portal"). "Customer Logs" means any communications, logs and other content and information that Customer or anyone using Customer's account contributes to or through the TAP Portal. Customer grants to FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive license and right to reproduce, modify, create derivative works from, publish, distribute, sell, sub-license, transmit, publicly display and provide access to Customer Logs, for purposes of enhancing FireEye's products and services, so long as (i) FireEye ensures that any Customer Confidential Information is removed from Customer Logs, and (ii) FireEye's use of Customer Logs does not in any way identify Customer or its employees or in any other way allow a third party to identify Customer as the source of the Customer Logs. Customer Logs are Customer's property, and other than the licenses granted in herein, FireEye does not obtain any ownership rights in Customer Logs.

1.1.3 TAP Alerts. Some features of the TAP Subscription may generate alerts of suspected malicious activity (each, a "TAP Alert"). TAP Alerts are FireEye Materials. FireEye hereby grants to Customer a limited, non-exclusive right to use TAP Alerts, and reproduce and distribute those TAP Alerts internally for Customer's own business purposes.

1.1.4 Cloud Collector Management. If Customer has installed Cloud Collectors in connection with the TAP Subscription, then FireEye will continuously monitor the Customer's Cloud Collector Appliances or Cloud Collector TAP Software for system health issues such as monitoring to ensure proper throughput and relay of data.

1.1.5 Cloud Collector Appliances. If the Customer has purchased Cloud Collector Appliances, then during the TAP Subscription Term, FireEye will replace any defective Cloud Collector Appliances as follows:

a) Prior to any return, Customer shall verify that the Cloud Collector Appliance at issue is defective by logging a Support request via one of the mechanisms provided in the Documentation and in accordance with FireEye's RMA procedures, including providing the part number, serial number, quantity and reason for return, an explanation of all failure symptoms and other relevant information.

b) Upon confirmation by FireEye of a defect, Customer shall obtain from FireEye an RMA number. FireEye shall ship via a recognized express courier service a replacement Cloud Collector Appliance to Customer to arrive no later than next business day after FireEye's issuance of an RMA number, provided the RMA number was issued prior to the business day cutoff time local to the defective Cloud Collector Appliance, provided the replacement does not require any custom pre-configuration, and provided no external-to-FireEye circumstances prevent the delivery. The replacement Cloud Collector Appliance may be a new or reconditioned Cloud Collector Appliance (of equivalent or better quality) at FireEye's sole discretion.

c) FireEye shall pay the shipping costs to ship the replacement Cloud Collector Appliance to Customer, but Customer shall bear any and all risk of loss of or damage to said Cloud Collector Appliance at all times after said Cloud Collector Appliance is made available by FireEye to the common carrier.

d) Within five (5) business days after Customer receives the replacement Cloud Collector Appliance from FireEye, Customer shall package the defective Cloud Collector Appliance in its original packing material or equivalent, write the RMA number on the outside of the package and return the defective Cloud Collector Appliance, at FireEye's cost (provided Customer utilizes FireEye's designated courier service and properly packages the defective Cloud Collector Appliance according to FireEye's instructions), shipped properly insured, FOB FireEye's designated facility. Customer shall enclose with the returned Cloud Collector Appliance the applicable RMA form, and any other documentation or information requested by FireEye customer support. Customer shall assume any and all risk of loss of or damage to such Cloud Collector Appliance during shipping. Title to the defective Cloud Collector Appliance shall pass to FireEye upon FireEye's receipt thereof.

e) When a replacement Cloud Collector Appliance is provided and Customer fails to return the defective Cloud Collector Appliance to FireEye within ten (10) business days after Customer receives the replacement Cloud Collector Appliance from FireEye, FireEye may charge Customer, and Customer shall pay for the replacement Cloud Collector Appliance at the then-current list price.

2. Event Volume; True-Up

2.1.1 Fees for the TAP Subscription are divided into "Tiers" based on the volume of events processed through the TAP Subscription per second ("Event Volume"). If at any point during the Subscription Term, Customer's Event Volume exceeds the Tier upon which Customer's TAP Subscription Fees were based, FireEye will not guarantee that Customer Logs in excess of the purchased Tier will be ingested and processed by the TAP Subscription. In times of Event Volume in excess of the paid Tier, Customer Logs will enter a queue. Excessive queueing may cause Customer Logs to be lost from the queue. If at any point during the Subscription Term, Customer's average Event Volume for any consecutive thirty-day period exceeds the Tier upon which Customer's TAP Subscription Fees were based, FireEye may issue a true-up invoice for the pro-rated difference between the Fees already paid for that Subscription Term and FireEye's list prices for the Fees for the Tier associated with Customer's actual Event Volume for that thirty-day period, pro-rated to reflect that thirty-day period and the remainder of the Subscription Term. FireEye will apply any discounts that were applied to initial Fees to FireEye's list prices for any true-up invoice. Until such time that the True Up invoice is paid in full, the TAP Subscription will continue to ingest and process only the Event Volume of the purchased Tier, allowing any excess Customer Logs to enter queueing conditions. The Tier for any Renewal Subscription Term will be the Tier associated with the actual Event Volume for the immediately preceding Subscription Term.

2.1.2 At the end of the Initial Subscription Term and each Renewal Subscription Term, FireEye may true-up Fees for that Subscription Term, and if the average monthly Event Volume for that Subscription Term exceeds the maximum Event Volume for the Tier for which Customer previously paid Fees, then (a) FireEye will issue a true-up invoice reflecting the difference between the Fees already paid for that Subscription Term and the Fees for the Tier associated with Customer's actual Event Volume.

3. TAP Portal Availability

3.1 FireEye shall undertake commercially reasonable efforts to ensure the TAP Portal availability for 99.9% of the time during each calendar month.

3.1.1 "Service Outage" is where the TAP Portal is not available due to a failure or a disruption in TAP Portal that is not the result of Scheduled Maintenance, Emergency Maintenance, a force majeure event or of the act or omission of Customer.

3.1.2 "Scheduled Maintenance Period" is the period during which weekly scheduled maintenance of the TAP Portal may be performed, or a maintenance window otherwise mutually agreed upon by FireEye and Customer.

3.1.3 "Emergency Maintenance" means any time outside of Scheduled Maintenance that FireEye is required to apply critical patches or fixes or undertake other urgent maintenance. If Emergency Maintenance is required, FireEye will contact Customer and provide the expected time frame of the Emergency Maintenance and availability of the TAP Portal during the Emergency Maintenance.

3.1.4 "System Availability" means the percentage of total time during which the TAP Portal shall be available to Customer, excluding the Scheduled Maintenance Period, Emergency Maintenance, force majeure events, or acts or omissions of the Customer that cause system downtime.

3.2. Remedy

3.2.1 In the event that the TAP Portal does not meet the monthly service availability defined in 6.1, FireEye will provide a credit to the Customer in accordance to the table below ("Credit") for a validated SLA Claim (defined below).

Percent of TAP Portal Availability per Calendar Month	Service Credit
<99.9%	2%
<99.0%	5%
<98.0%	10%

3.2.2 For determining the Credit, the duration of a Service Outage will be measured as the time starting when Customer experiences unavailability of the TAP Portal and ending when a successful solution or workaround allowing for full restoration of the TAP Portal is provided by FireEye to Customer. Customer must notify FireEye in writing of any Service Outage no later than fifteen (15) days after the date the Service Outage occurred ("SLA Claim") to be entitled to a Credit for that Service Outage.

3.2.3 Any Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Subscription Term for which the Credit applies. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated for non-renewal or for a material uncured breach by Customer, such credits shall become null and void. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated due to a material uncured breach by FireEye, FireEye will promptly pay Customer the amount of the Credit.

3.2.4 Customer shall not be entitled to receive a Credit that exceeds 10% of its prorated monthly Subscription Fee for a Service Outage for the applicable calendar month.

4. FireEye Intelligence Center™ (FIC™), Community Threat Intelligence™ (CTI™). During the Subscription Term, FireEye will provide access to the FireEye Intelligence Center (FIC), which includes the Community Threat Intelligence (CTI) platform, subject to the following:

i. Permitted Use; Reports. Customer may view and use FIC and content appearing on FIC ("FIC Content") solely for internal use. Some features of FIC may allow Customer to generate a report (each, a "FIC Report"). FIC Reports and FIC Content are FireEye Materials. Subject to Customer's payment obligations, FireEye grants to Customer a limited, non-exclusive right to produce FIC Reports and FIC Content using FIC, and reproduce and distribute those FIC Reports and FIC Content internally for Customer's own business purposes.

ii. Additional Use Limitations. Customer may appoint up to fifteen (15) users of FIC at any time. Each day, all users on Customer's account may collectively make up to (A) one hundred (100)queries of IP addresses and domain names, and (ii) one hundred (100) queries of malware. Customer may request additional queries, to be evaluated by FireEye on a case by case basis.

iii. User Content. "User Content" means any communications, images, sounds, and all the material and information that Customer or anyone using Customer's account contributes to or through FIC including any contributions to or through the CTI platform (e.g., comments to FIC Content, suspected malware that Customer uploads to FIC). Customer hereby grants FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive, license, including the right to sublicense to third parties, and right to reproduce, fix, adapt, modify, translate, reformat, create derivative works from, publish, distribute, sell, license, transmit, publicly display, publicly perform, or provide access to electronically, broadcast, display, perform, and use and practice such User Content as well as all modified and derivative works thereof. Customer represents that Customer has all necessary rights to grant the license referenced in the preceding sentence. FireEye may use and disclose any of the information it collects about its customers' use of FIC, including the CTI platform, to the extent such information is de-identified.

iv. Restrictions. Customer may not access FIC by any means other than through the interface that is provided or approved by FireEye. Customer will not collect any information from or through FIC using any automated means, including without limitation any script, spider, "screen scraping," or "database scraping" application, and Customer will not damage, disable, overburden, or impair FIC or interfere with any other party's use and enjoyment of FIC.

v. Customer acknowledges that some optional features and content appearing on FIC may require payment of additional fees.

EXHIBIT B-4
SUBSCRIPTION TERMS FOR FIREEYE EMAIL THREAT PREVENTION (ETP) and MOBILE THREAT PREVENTION (MTP)

The following terms govern the Email Threat Prevention Subscription and Mobile Threat Prevention Subscription.

1. Definitions.

"Cloud Subscription" means the online, web-based applications and platform which is made accessible to Customer by FireEye via a designated website, which includes the associated offline Software components to be used in connection with FireEye Mobile Threat Prevention and/or FireEye Email Threat Prevention. FireEye Mobile Threat Prevention ("MTP") and FireEye Email Threat Prevention ("ETP") are separate Cloud Subscriptions and usage is conditional on what the Customer has indicated on an Order.

"Customer Data" means data, information, applications, and any other items originated by Customer that Customer submits to the Cloud Subscription.

"Customer Representatives" means any employee or contractor of Customer or Mobile Device Manager to whom Customer provides access to the Cloud Subscriptions (or any component thereof, including Software) for use on behalf of and for the benefit of the Customer and for Customer's internal business purposes, subject to all the terms and conditions of this Agreement.

"Licensed Device" means (i) with respect to MTP, the registered devices that Customer may have at any time that are registered to the Cloud Subscription; which maximum number shall be based on the subscription fees paid by Customer and identified on the relevant purchase order from Customer as approved and invoiced by FireEye; and (ii) with respect to ETP, the number of email inboxes Customer may have at any time that are registered to the Cloud Subscription; which maximum number shall be based on the subscription fees paid by Customer and identified on the relevant purchase order from Customer as approved and invoiced by FireEye. For the avoidance of doubt, with respect to MTP, "registered devices" are those devices which have loaded device Software and which have been registered to the Cloud Subscription and which have not been retired (meaning unregistered).

"Mobile Device Manager" shall mean a third party who has been engaged by the Customer to provide security services for Licensed Devices for the benefit of Customer. Where indicated as such, the Mobile Device Manager shall be a subset of the definition of the Customer Representatives solely as applicable to MTP.

"Software" means the object code version of FireEye's proprietary computer programs delivered to Customer hereunder for use in connection with the Cloud Subscriptions, including collectively and individually the device-side software used on devices registered to the Cloud Subscription ("Device Software") and any connector software and/or any other server-side software (collectively the "Premise Software") , each which are delivered to Customer hereunder for use in connection with the Cloud Subscriptions, and any Documentation, backup copies and updates, upgrades, maintenance releases, bug fixes to any of the forgoing provided to Customer hereunder.

2. Right of Access and Use. During the Subscription Term, and subject to the terms of this Agreement, FireEye grants to Customer a non-exclusive right to (a) permit those Customer Representatives authorized by Customer to access and use the Cloud Subscriptions on Customer's behalf in compliance with the terms of this Agreement, and (b) to install, copy and use Premise Software in connection with Cloud Subscriptions in accordance with the Agreement and this Exhibit, but solely on systems and hardware owned or controlled or otherwise managed by Customer on behalf of and for the benefit of Customer, (c) to install, copy and use Device Software in connection with Cloud Subscriptions in accordance with the Documentation, but solely on devices used by Customer Representatives on behalf of and for the benefit of Customer. Notwithstanding anything else herein, the number of devices Customer and/or Customer Representatives may register to the Cloud Subscriptions may not exceed the number of Licensed Devices.

Notwithstanding anything to the contrary herein, if Customer is using the Cloud Subscriptions for evaluation purposes then such Customer usage is solely for internal testing and evaluation and the Subscription Term shall not exceed fifteen (15) days unless otherwise mutually agreed upon in a signed Evaluation License Agreement.

3. Restrictions. Except as otherwise expressly permitted under this Agreement, Customer agrees that it shall not, nor shall it permit any third party to, (a) use the Cloud Subscriptions (or any portion thereof) in excess of or beyond the Subscription Term, the Licensed Device quantity, and/or other restrictions/limitations described in this Agreement; use the Cloud Subscriptions to store or transmit infringing, libelous, or otherwise unlawful or tortious material, or to store or transmit material in violation of third-party privacy or other rights; (d) interfere with or disrupt the integrity or performance of the Cloud Subscriptions or third-party data contained therein; (e) use the Software on equipment or devices which are not specified in the Documentation; (f) Cloud Subscription specific to ETP Cloud Subscriptions, Customer shall route email through a commercially available secure email gateway for anti-spam scanning prior to relay through the FireEye network. No rights or licenses are granted other than as expressly and unambiguously set forth herein. Customer access and usage for the Cloud Subscriptions is limited to the MTP or ETP Subscription that has been paid or are being evaluated by the Customer.

4. Updates, Malware Detection Content and Support Services. Updates and malware detection content and/or support services are not necessarily provided with the Software or Subscriptions, and may require additional payment or include additional terms and conditions. However, to the extent that an update to the Software and/or malware detection content is provided, such update/content shall be deemed "Software" provided subject to this Agreement. If malware detection content/support services are provided, FireEye reserves the right to change the scope or duration of such services at anytime, and to access, freely use and distribute data collected from Customer through such services. If such services are made available, Customer may be required to pay fees or other charges for use or access to some or all such services, which fees and terms will be specified in the invoice or order form for such service.

5. Device Count Increases; Reporting; Invoice. If the number of devices that Customer or Customer Representatives have registered to the Cloud Subscription ("Actual Device Count") exceeds Customer's then current Licensed Device count or if Customer wishes to increase the Licensed Device count, then Customer shall notify FireEye (or the applicable FireEye Partner) and submit an Order for the incremental Subscription Fees due, and upon receipt of such Order, the Licensed Device count shall be amended to reflect this change. Upon written request, Customer will provide FireEye a report identifying (i) the Actual Devices; (ii) the copies of and location of the Premise Software maintained; and (iii) any other information reasonably requested by FireEye at the time as it relates to the use of the Cloud Subscription to determine compliance with the terms of this Agreement. FireEye and/or its Authorized Resellers may invoice Customer if it learns of any shortfalls, i.e. that the Licensed Device Count is below the Actual Device count. The fees charged to Customer for increases in License Device counts will be based on the then-current Subscription Term pricing.

6. Cloud Subscription Availability

6.1 FireEye shall undertake commercially reasonable efforts to ensure the Cloud Subscription availability for 99.9% of the time during each calendar month.

6.1.1 "Service Outage" is where the Customer is not receiving Cloud Subscription due to a failure or a disruption in the Cloud Subscriptions and is not the result of Scheduled Maintenance, Emergency Maintenance, a force majeure event or of the act or omission of Customer.

6.1.2 "Scheduled Maintenance Period" is the period during which weekly scheduled maintenance of the Cloud Subscriptions may be performed, or a maintenance window otherwise mutually agreed upon by FireEye and Customer.

6.1.3 "Emergency Maintenance" means any time outside of Scheduled Maintenance that FireEye is required to apply critical patches or fixes or undertake other urgent maintenance. If Emergency Maintenance is required, FireEye will contact Customer and provide the expected time frame of the Emergency Maintenance and availability of the Cloud Subscriptions during the Emergency Maintenance.

6.1.4 "System Availability" means the percentage of total time during which the Cloud Subscriptions shall be available to Customer, excluding the Scheduled Maintenance Period, Emergency Maintenance, force majeure events, or acts or omissions of the Customer that cause system downtime.

6.2. Remedy

6.2.1 In the event that the Cloud Subscription does not meet the monthly service availability defined in 6.1, FireEye will provide a credit to the Customer in accordance to the table below ("Credit") for a validated SLA Claim (defined below).

Percent of System Availability per Calendar Month	Service Credit
<99.9%	25%
<99.0%	50%
<98.0%	100%

6.2.2 For determining the Credit, the duration of a Service Outage will be measured as the time starting when there is a disruption in Cloud Subscription and ending when a successful solution or workaround allowing for full restoration of the Cloud Subscriptions is provided by FireEye to Customer. Customer must notify FireEye in writing of any Service Outage no later than fifteen (15) days after the date the Service Outage occurred ("SLA Claim") to be entitled to a Credit for that Service Outage.

6.2.3 Any Credits earned by Customer hereunder will be applied to the Subscription Fees owed by Customer for the next Subscription Term for which the Credit applies. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated for non-renewal or for a material uncured breach by Customer, such credits shall become null and void. If Credits cannot be applied to future Subscription Fees because the Subscription Term has terminated due to a material uncured breach by FireEye, FireEye will promptly pay Customer the amount of the Credit.

6.2.4 Customer shall not be entitled to receive a Credit that exceeds 100% of its prorated monthly Subscription Fee for a Service Outage for the applicable calendar month.

EXHIBIT B-5
SUBSCRIPTION TERMS FOR FIREEYE ADVANCED THREAT INTELLIGENCE PLUS (ATI+)

The following terms govern the Advanced Threat Intelligence Plus (ATI+) Subscription.

The ATI+ Subscription comprises two features: Continuous Monitoring ("CM" or "Continuous Monitoring") and the FireEye Intelligence Center™ (FIC™) ("FIC").

1. Continuous Monitoring

The Continuous Monitoring portion of the Subscription is purchased in connection with one or more FireEye Products, and includes the following during the Subscription Term for the specific Products for which Continuous Monitoring was purchased (some Products may not be eligible for CM):

(a) Critical Event Notification. For Customers who have purchased the FireEye NX, FX, HX or EX Product, MVX Smart Grid with Network Smart node product combination, or the ETP or TAP Subscription, FireEye will provide Customer with proactive notifications of events FireEye determines to be critical that are logged by the Products ("Alerts"). FireEye will also provide Customer with access to a detailed description of the Alert. Alerts are not proof of vulnerability, threats or attacks on Customer.

(b) System Health Monitoring and Notification. For Customers who have purchased the FireEye NX, EX, FX, HX AX or FX Product, or MVX Smart Grid w/Network Smart node combination (hardware only), FireEye will provide Customer with proactive notifications of serious system health issues related to the hardware for Products covered by Continuous Monitoring. Customers will also be provided with metrics on critical event notifications and, for purchased hardware, the status of monitored hardware parameters.

(c) Portal Access. Alerts and critical event notifications from Continuous Monitoring will be provided via an online portal, and FireEye will provide login credentials to the Customer to enable access to that portal.

(d) Continuity of Monitoring. The monitoring activities described in (a)-(c) above will be provided on a 24/7 basis.

(f) Reseller and Partner Purchases. If Customer receives the Subscription via a FireEye Partner, Customer agrees that the Subscription may be delivered to Customer through the Partner. Notwithstanding any other confidentiality obligations between the parties, Customer authorizes FireEye to disclose information related to the Subscription to the Partner.

(g) Exclusions. Notwithstanding anything else contained in this Agreement to the contrary, FireEye shall have no obligation or responsibility to provide the Subscription for (i) Products for which Customer does not have an active Subscription in place; (ii) Products that the Customer (or FireEye or another third party on Customer's behalf) has configured with a one-way feed of FireEye's Dynamic Threat Intelligence subscription; (iii) Products with an installed FireEye operating system less than version 6.2; (iv) Products that are end of life; (v) Products that have no active support service in place; (vi) Products for which software updates have not been applied; or (vii) Products that have not been installed and deployed.

2. FireEye Intelligence Center™ (FIC™), Community Threat Intelligence™ (CTI™)

FireEye will provide the FIC portion of the Subscription, which includes the Community Threat Intelligence (CTI) platform, during the Subscription Term, as set forth below:

2.1 Permitted Use; Reports. Customer may view and use FIC and content appearing on FIC ("FIC Content") solely for internal use. Some features of FIC may allow Customer to generate a report (each, a "FIC Report"). FIC Reports and FIC Content are FireEye Materials. Subject to Customer's payment obligations, FireEye grants to Customer a limited, non-exclusive right to produce FIC Reports and FIC Content using FIC, and reproduce and distribute those FIC Reports and FIC Content internally for Customer's own business purposes.

2.2 Additional Use Limitations. Customer may appoint up to fifteen (15) users of FIC at any time. Each day, all users on Customer's account may collectively make up to (i) one hundred (100) queries of IP addresses and domain names, and (ii) one hundred (100) queries of malware per day. Customer may request additional queries, to be evaluated by FireEye on a case by case basis.

2.3 User Content. "User Content" means any communications, images, sounds, and all the material and information that Customer or anyone using Customer's account contributes to or through FIC including any contributions to or through the CTI platform. Customer hereby grants FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive, license, including the right to sublicense to third parties, and right to reproduce, fix, adapt, modify, translate, reformat, create derivative works from, publish, distribute, sell, license, transmit, publicly display, publicly perform, or provide access to electronically, broadcast, display, perform, and use and practice such User Content as well as all modified and derivative works thereof. Customer represents that Customer has all necessary rights to grant the license referenced in the preceding sentence. FireEye may use and disclose any of the information it collects about its customers' use of FIC, including the CTI platform to the extent such information is de-identified.

2.4 Restrictions. Customer may not access FIC by any means other than through the interface that is provided or approved by FireEye. Customer will not collect any information from or through FIC using any automated means, including without limitation any script, spider, "screen scraping," or "database scraping" application, and Customer will not damage, disable, overburden, or impair FIC or interfere with any other party's use and enjoyment of FIC. Customer acknowledges that some optional features and content appearing on FIC may require payment of additional fees.

EXHIBIT B-6
SUBSCRIPTION TERMS FOR FIREEYE INTELLIGENCE CENTER™ (FIC™) (INCLUDING COMMUNITY THREAT INTELLIGENCE™ (CTI™))

The following terms govern the FireEye Intelligence Center™ (FIC™) Subscription, which includes access to the Community Threat Intelligence™ (CTI™) platform.

1. During the Subscription Term, FireEye will provide access to the FireEye Intelligence Center (FIC), which includes the Community Threat Intelligence (CTI) platform, subject to the following:

i. Permitted Use; Reports. Customer may view and use FIC and content appearing on FIC ("FIC Content") solely for internal use. Some features of FIC may allow Customer to generate a report (each, a "FIC Report"). FIC Reports and FIC Content are FireEye Materials. Subject to Customer's payment obligations, FireEye grants to Customer a limited, non-exclusive right to produce FIC Reports and FIC Content using FIC, and reproduce and distribute those FIC Reports and FIC Content internally for Customer's own business purposes.

ii. Additional Use Limitations. Customer may appoint up to fifteen (15) users of FIC at any time. Each day, all users on Customer's account may collectively make up to (A) one hundred (100)queries of IP addresses and domain names, and (ii) one hundred (100) queries of malware. Customer may request additional queries, to be evaluated by FireEye on a case by case basis.

iii. User Content. "User Content" means any communications, images, sounds, and all the material and information that Customer or anyone using Customer's account contributes to or through FIC including any contributions to or through the CTI platform (e.g., comments to FIC Content, suspected malware that Customer uploads to FIC). Customer hereby grants FireEye a perpetual, irrevocable, worldwide, paid-up, non-exclusive, license, including the right to sublicense to third parties, and right to reproduce, fix, adapt, modify, translate, reformat, create derivative works from, publish, distribute, sell, license, transmit, publicly display, publicly perform, or provide access to electronically, broadcast, display, perform, and use and practice such User Content as well as all modified and derivative works thereof. Customer represents that Customer has all necessary rights to grant the license referenced in the preceding sentence. FireEye may use and disclose any of the information it collects about its customers' use of FIC, including the CTI platform, to the extent such information is de-identified.

iv. Restrictions. Customer may not access FIC by any means other than through the interface that is provided or approved by FireEye. Customer will not collect any information from or through FIC using any automated means, including without limitation any script, spider, "screen scraping," or "database scraping" application, and Customer will not damage, disable, overburden, or impair FIC or interfere with any other party's use and enjoyment of FIC.

v. Customer acknowledges that some optional features and content appearing on FIC may require payment of additional fees.

EXHIBIT B-7
SUBSCRIPTION TERMS FOR FIREEYE iSIGHT INTELLIGENCE

The following terms govern the FireEye iSIGHT Intelligence Subscription ("iSIGHT" or "iSIGHT Subscription"). FireEye will provide the iSIGHT Subscription purchased by the Customer, as shown on the Order.

1. Definitions.

1.1 "Access Method(s)" or "Access Methods" means the MySIGHT Portal ("MySIGHT"), Software Development Kit ("SDK"), Application Programming Interface ("API"), Browser Plugin, iSIGHT App for Splunk, or any other method provided by FireEye for Customer to access the iSIGHT Subscription, individually or collectively. All Access Methods are FireEye Material as defined in the Agreement.

1.2 "Application" is a software program the Customer creates, or causes to have created on its behalf, that is designed to access the Content, which includes the features of the SDK/API but adds significant functionality beyond that provided by the SDK/API.

1.3 "Application Programming Interface" or "API" means the latest version of the iSIGHT Application Programming Interface software made generally available by iSIGHT, with its developer's guide and other related material (available at http://www.isightpartners.com).

1.4 "Browser Plugin" means the iSIGHT Browser Plugin which a Customer may install on Google Chrome and/or other commercially available and supported browsers that allows the Customer to access and view the Content when licensed to do so. The Browser Plugin displays the iSIGHT logo and links to MySIGHT. The Browser Plugin includes the latest version of the Browser Plugin software, its documentation and any html embedded code.

1.5 "Content" means the cyber threat intelligence data and any reports, threat indicators, trends, events, information, documentation or functionality provided in connection with the iSIGHT Subscription. All Content is FireEye Material as defined in the Agreement.

1.6 "End User" means the Customer or the Customer's employees, as applicable.

1.7 "Software Development Kit" or "SDK" shall mean the latest publicly-available version of the iSIGHT Software Development Kit and any associated documentation, tools, libraries, technical notes, software code, or other materials.

1.8 "iSIGHT App for Splunk" means the application provided by FireEye, which a Customer may install on Splunk, that allows the Customer to access and view the Content in accordance with this Agreement. The iSIGHT App for Splunk includes the latest version of the iSIGHT App for Splunk software, its documentation and any html embedded code.

1.9 "iSIGHT Subscription" includes but is not limited to, Cyber Crime, Cyber Espionage, Critical Infrastructure, Enterprise, Hacktivism, Vulnerability and Exploitation, MySIGHT Portal, Global Response, Analyst Access, iSIGHT SDK, iSIGHT API, iSIGHT Research Reports, or the current offering(s) as listed on the iSIGHT website, and as purchased by the Customer as shown on the Order.

2. License; Access to iSIGHT Subscription and Content.

2.1. Grant of Limited License. During the Subscription Term, FireEye grants to Customer in strict accordance with the terms of this Agreement, a limited, worldwide, revocable, non-exclusive, non-transferable, non-assignable, non-sublicensable royalty-free right and license to:

(a) use MySIGHT, the iSIGHT Subscription, and any Content provided by FireEye for internal use only. The ISIGHT Subscription can be used by End Users who have a valid "need to know" within Customer's organization, typically defined as a person or group that has a direct role in securing information system or networks. FireEye agrees to provide support for the ISIGHT Subscription in accordance with Section 3 below ("Subscription Support" or "Support").

(b) use the API to search, display, and otherwise access the Content. The API can be used to develop, display, or integrate applications, scripts, tools or workflows that interoperate with iSIGHT Subscriptions for the Customer's internal use. FireEye agrees to provide Support for the latest version of the API in accordance with Section 3 below.

(c) download, install and use the Software Development Kit ("SDK") to design, develop and test an Application(s), for the Customer's internal use only, for the purpose of customizing access to the Content. The Customer may modify the source code versions of sample files, if any, included with the SDK for the purpose of creating Customer's Application(s), and may make a reasonable number of copies of the SDK as necessary to develop Customer's Application(s), provided that Customer must reproduce complete copies of the SDK, including without limitation all "read me" files, copyright notices, and other legal notices and terms. FireEye agrees to provide Support for the ISIGHT SDK in accordance with Section 3 below.

(d) use the Browser Plugin to search, display and otherwise access the Content for the Customer's internal use only. Customer may install and use one copy of the Browser Plugin on a single computer per license. FireEye agrees to provide Support for the latest version of the Browser Plugin in accordance with Section 3 below

(e) use the ISIGHT App for Splunk to search, display and otherwise access the Content for the Customer's internal use only. Customer may install and use one copy of the ISIGHT App for Splunk on a single computer per license. FireEye agrees to provide Support for the latest version of the ISIGHT App for Splunk in accordance with Section 3 below.

2.2. Access Keys. Use of the Access Methods and access to the ISIGHT Subscription and the Content by Customer's End Users is provided through access keys or login credentials. Access keys in association with the Access Methods and ISIGHT Subscription shall be kept in confidence by Customer and Customer's End Users. Access keys will be issued to individual End Users by FireEye in accordance with each particular Access Method's parameters and will not be shared between End Users. Customer may not establish group accounts. Any unauthorized disclosure or dissemination of access keys by Customer or End Users shall be deemed a material breach of this Agreement. Customer shall inform FireEye of any data breach concerning login credentials in a timely manner. FireEye reserves the right to change, suspend, remove, or disable Customer's access keys to the Access Methods, ISIGHT Subscription , and Content upon notice if a material breach is suspected and not rectified upon notification.

2.3. Latest Version. The license granted to Customer under this Agreement is for the current version of the Access Methods. FireEye may release future versions of the Access Methods as determined in the sole discretion of FireEye. Nothing in this Agreement is a commitment to Customer of compatibility between the existing Access Methods and any future versions of the Access Methods. FireEye reserves the right to discontinue offering particular Access Methods (or any updates thereto) or to modify the Access Methods at any time in its sole discretion.

2.4. Multiple Copies. Customer may receive software for an Access Method in more than one medium and/or in multiple copies. The Customer's license rights are in accordance with the Order regardless of the number of copies received.

2.5. Additional Licenses. Customer may purchase additional licenses for the Browser Plugin for its authorized End Users through the Chrome Web Store. Customer may purchase additional licenses for the ISIGHT App for Splunk for its authorized End Users through Splunk. Additional licenses for the Browser Plugin and ISIGHT App for Splunk may be purchased and will be valid for the current Subscription Term as provided in the Order.

2.6. Customer Application. The Customer may allow Customer's employees to access and use the SDK/API on Customer's behalf to design an Application. The Customer may not rent, lease, sell, transfer, sublicense or time-share the Customer's Application to any third-party without the express consent of FireEye. Customer shall retain all right, title or interest in the Application and as such, Customer agrees to indemnify and hold harmless FireEye for any claims of infringement made against FireEye in connection with any Application. The Customer's Application(s) must perform in accordance with the terms of this Agreement and must ensure the security and confidentiality of FireEye's Confidential Information. Customer assumes full responsibility for any breach of

security caused by Customer's Application(s) in connection with the Content, API, SDK, and specifically to any unauthorized disclosure of any FireEye Materials or FireEye Confidential Information.

2.7. Content Modifications. Customer may access the Content from the MySIGHT Portal, via email, SMS, HTML, API, any other Access Methods as officially distributed by FireEye or an FireEye sanctioned third-party integration. FireEye reserves the right to modify, amend, augment, reduce or alter the Content's format, or Access Methods, or mode of retrieval of the Content, that in the sole judgment of FireEye is in its customers' best interests. Customer will be entitled to retrieve the Content with any updates, modifications, additions or changes in the Content. These changes may require Customer to upgrade its systems, hardware or software and FireEye will not be responsible for the costs of any such changes.

2.8. Prohibited Usage. Customer must comply with any Intellectual Property rights asserted in any materials contained in the Content. The following conduct and usage restrictions apply during Customer's download, installation, and use of the Content and/or Access Methods, and survive termination of the Agreement or Subscription Term. Customer and its authorized End Users may not:

a. rent, lease, lend, sell, redistribute or sublicense any part of the ISIGHT Subscription or Access Methods to any other party;

b. share the ISIGHT Subscription , Access Methods, Content or Confidential Information with any third-parties, except as expressly authorized in advance by this Agreement or by FireEye in writing;

c. use the ISIGHT Subscription or Access Methods in the operation of a service or in any way to provide services to any third-party;

d. create derivative works for external distribution or use based upon the Content;

e. create apps, extensions, or other products and services that use Content except as set forth herein;

f. display, post, frame, or scrape the Content, except as allowed under this Agreement;

g. use the Access Methods for any other purpose than to access the ISIGHT Subscription and the Content;

h. use the Access Methods for any illegal or unauthorized purpose to promote or provide instructional information about illegal activities or to promote stalking, physical harm or injury against any group or individual, or any use that violates the rights of privacy and publicity of others;

i. create, place, or disseminate any materials or other items that are inappropriate, defamatory, obscene, pornographic, harassing, threatening, abusive, hateful or otherwise offensive, or is unlawful (including any content that infringes any patent, trademark, service mark, copyright, trade secret or other proprietary right of any third-party without appropriate permissions);

j. transmit any viruses, worms, defects, Trojan horses, time-bombs, malware, spyware, or any other computer code of a destructive or interruptive nature in connection with use of the Access Methods;

k. use the Access Methods in connection with or to promote any products, services, or materials that constitute, promote or are used primarily for the purpose of dealing in spyware, adware, or other malicious programs or code, counterfeit goods, unsolicited mass distribution of email ("spam"), hacking, surveillance, interception, descrambling equipment, stolen products and items used for theft;

l. create any Application that exposes or provides functionality of the Access Methods to any third party;

m. interfere, restrict or inhibit any other customer from using the Access Methods or Content or disrupt any services offered by FireEye through any medium;

n. attempt to exceed or exceed the usage limits established by FireEye for the Customer (http://www.isightpartners.com/doc/sdk-bp-docs/#/rate_limiting).

2.9. Restrictions. FireEye expressly reserves the right to limit the number and/or frequency of requests for Content made through the Access Methods in its sole discretion in line with technical design and performance standards as documented in the publicly available developers guide. FireEye may limit the number of network calls that any Application may make via the Access Methods, the maximum file size, or the maximum amount of ISIGHT material that may be accessed. FireEye may change such usage limitations at any time and without notice. In addition to any other rights under this Agreement, FireEye may utilize technical measures to prevent over-usage or to stop usage of any Access Methods or any Application after any usage limitations are exceeded. The most current API/SDK documentation and developers guide can be found at http://www.isightpartners.com/doc/sdk-bp-docs/#/, and these documents detail the current rates and capabilities of the API.

2.10. Customer recognizes and agrees that certain information and data that will be provided by Customer to FireEye pursuant to the ISIGHT Subscription is not owned by Customer and is not Confidential Information of

Customer. Malware submitted by Customer to FireEye for analysis under ISIGHT Global Response, and other information submitted by Customer to FireEye that is not unique to and/or developed by Customer (collectively "Submissions") shall not be considered Confidential Information or Intellectual Property of the Customer. FireEye may use the Submissions, aggregate the Submissions with submissions from other FireEye customers as well as original research and analysis, and share that aggregated intelligence with Customer and with other FireEye customers to enhance the services FireEye provides to its customers. FireEye will anonymize all Submissions prior to distribution, and will not identify the source of any Submission without written permission in each case.

3. Service Levels.

3.1. Service Call and Subscription Support

FireEye maintains a service desk in order to assist its customers with issues, trouble or general questions concerning use of the FireEye ISIGHT Products. Customer may initiate a service call as follows:

Description	Details
FireEye Service Desk (Primary, escalation and off-hours contact)	servicedesk@isightpartners.com
Service Desk Hours	24 x 7
Service Call Response Time ("Response Time Standard")	4 hours for initial response (confirmation of receipt is immediate through an automated ticketing system)
ISIGHT API	General information regarding ISIGHT API which can be accessed at http://www.isightpartners.com/doc/api2.0/docs/#/
Other resources (all other Subscription Support issues)	Existing Clients – Contact your assigned Intelligent Account Manager at: client-engagement@isightpartners.com Prospective Clients – Contact your assigned Sales Engineer at: sales-engineering@isightpartnerns.com Partners, Resellers, Referrals – Contact partners program representative at: partners@isightpartners.com

FireEye will catalog and evaluate all bugs or software issues as they are reported. Such issues will be prioritized based on variables such as customer impact, security impact, etc. and will be scheduled for release accordingly. When applicable, FireEye will notify Customer of urgent patches or bug fixes. Support Services do not include custom programming services, on-site support, or other services including installation of hardware or software, or training.

3.2. Maintenance and Updates

(a) When feasible and appropriate, FireEye will provide Customer prior notification about major releases at least two weeks in advance via communication from FireEye representatives.
(b) Scheduled system maintenance will be performed during the targeted times of 01:00 – 07:00 UTC on Thursdays and 12:00 – 19:00 UTC on Sundays. Prior notification will be provided in the event of any impact to customer facing applications.
(c) Emergency maintenance notifications will be provided by FireEye as early as possible but with a goal of six (6) hours' prior notice provided. Further, FireEye will strive to minimize the impact of any maintenance on any critical system during standard business hours around the globe.

3.3. Subscription Availability

(a) The FireEye ISIGHT API will have at least 99% system uptime ("API Uptime Standard").

(b) The iSIGHT MySIGHT Portal will have at least a 99% system uptime ("Portal Uptime Standard").

(c) FireEye realizes that a failure to meet the Response Time Standard, API Uptime Standard and the Portal Uptime Standard (collectively, the "Service Level Standards") could have an adverse impact to Customer. If FireEye fails to meet any of the Service Level Standards ("Service Level Failure"), FireEye will: (i) promptly investigate and report on the root cause of the problem; (ii) advise Customer of the remedial efforts being undertaken with respect to this failure to meet the Service Level Standards; (iii) use commercially reasonable efforts to correct the problem and begin meeting the Service Level Standards; and (iv) take appropriate preventative measures designed to ensure that the problem does not recur.

EXHIBIT C
FIREEYE SUPPORT SERVICES APPLICABLE FOR FIREEYE PRODUCTS

1. SUPPORT PURCHASED SEPARATELY FROM THE PRODUCTS. In the event Customer has purchased the Products and pass-through Support Services from FireEye through a FireEye authorized reseller (a "Reseller"), Customer will be entitled to all the rights herein set forth related to the level of Support Service requested and paid for by it, provided Customer: (a) is the original purchaser of the covered Products, (b) has provided true, accurate, current and complete information to FireEye included with its purchase; and (c) has maintained and updated this information to keep it true, accurate, current, and complete.

2. SUPPORT SERVICES PROVIDED BY FIREEYE.

FireEye offers a range of programs for the support of its Products as described below ("Support Programs"). Customer shall be entitled to receive the Support Services specified on the applicable support invoice and described below to the extent that Customer has paid in full the applicable Fees for Support Services.

2.1 Software Maintenance Services – include each of the following:

Software Updates. During the Support Term , FireEye shall provide Customer notification of bug fixes, maintenance patches and new releases which may contain minor enhancements to the features or functions of the Product ("**Updates**"). FireEye may designate a particular release of the Product as an Update at its sole discretion. Customer may obtain Updates either through delivery of a machine-readable copy pursuant to instructions contained in the document notifying Customer of an available Update or by downloading the Update from FireEye's server via the Internet. FireEye reserves the right to impose additional charges for releases of Products (i) that provide major enhancements to the features or functions of the Products, as determined by FireEye at its sole discretion; or, (ii) that provide additional features or perform additional functions not provided or performed by the Products.

Software Error Corrections. During the Support Term, FireEye shall use commercially reasonable efforts to correct any reproducible programming error in the software associated with the Product attributable to FireEye, employing a level of effort commensurate with the severity of the error, provided, however, that FireEye shall have no obligation to correct all errors in the Products. Upon identification of any programming error, Customer shall notify FireEye of such error in writing and shall provide FireEye with enough information to locate and reproduce the error. FireEye shall not be responsible for correcting any errors not attributable to FireEye. Errors attributable to FireEye shall be those that are reproducible by FireEye on unmodified Products. If it is found that a particular error is fixed in the most current Product release, then FireEye shall have no obligation to fix the error in any prior Product release and Customer will need to upgrade to the current Product release in order to obtain the fix.

2.2 Support Programs

(a) Platinum Support includes all of the services set forth above under Software Maintenance Service (section 2.1) and additionally:

- *Email, Live Chat, Web or Telephone Support.* During the Support Term, FireEye shall provide Customer technical email, live chat, web or telephone support for the Products twenty-four (24) hours per day, 365 days a year. FireEye's support technician shall only be obligated to respond to Customer's fifteen (15) designated contacts.
- FireEye shall use commercially reasonable efforts to respond to the request for support as detailed in the Initial Response Times table found at https://www.fireeye.com/support/programs.html regarding use or installation of the Product that is communicated to FireEye via one of the mechanisms above to the attention of FireEye's support engineers.
- *Product Return.* During the term of this Agreement, Customer shall have the right to return to FireEye any defective Product subject to the limited warranty. Additionally, FireEye will fulfill the following Advance Return provisions below.

- Advance Replacement. Prior to any return as to which Advance Replacement applies, Customer shall verify that said Product is defective by logging a Support request via one of the mechanisms described above and in accordance with FireEye's RMA procedures, including providing the part number, serial number, quantity and reason for return, an explanation of all failure symptoms and other relevant information. Upon confirmation by FireEye of a defect, Customer shall obtain from FireEye an RMA number. FireEye shall ship via a recognized express courier service a replacement Product to Customer to arrive no later than next business day after FireEye's issuance of an RMA number, provided the RMA number was issued prior to the business day cutoff time local to the defective Product, provided the replacement does not require any custom pre-configuration, and provided no external-to-FireEye circumstances prevent the delivery. The replacement Product may be a new or reconditioned Product (of equivalent or better quality) at FireEye's sole discretion. FireEye shall pay the shipping costs to ship the replacement Product to Customer, but Customer shall bear any and all risk of loss of or damage to said Product at all times after said Product is made available by FireEye to the common carrier. The support service will transfer from the defective Product to the replacement Product. Within five (5) business days after Customer receives the replacement Product from FireEye, Customer shall package said defective Product in its original packing material or equivalent, write the RMA number on the outside of the package and return said defective Product, at FireEye's cost provided Customer utilizes FireEye's designated courier service and properly packages the defective Product according to FireEye's instructions, shipped properly insured, FOB FireEye's designated facility (except that FireEye shall pay for shipping). Customer shall enclose with the returned Product the applicable RMA form, and any other documentation or information requested by FireEye customer support. Customer shall assume any and all risk of loss of or damage to such Product during shipping. Title to the defective Product shall pass to FireEye upon FireEye's receipt thereof. When a replacement Product is provided and Customer fails to return the defective Product to FireEye within ten (10) business days after Customer receives the replacement Product from FireEye, FireEye may charge Customer, and Customer shall pay for the replacement Product at the then-current list price.

(b) Platinum Priority Plus Support iincludes all of the services set forth above under Platinum Support [section 2.2(a)] and additionally:

- *Access to Support*. Customer will be provided with direct priority access to Level 2 Advanced Engineering support who shall respond to Customer's unlimited number of designated contacts. A Designated Support Engineer (DSE) point of contact, who is available during Customer's business hours (for single Customer site if Product(s) installed at multiple Customer sites), will be made available to be the focal point of contact within FireEye, to project manage Customer's technical issues.
- *Onsite Support*. Onsite visits for problem assistance at DSE's sole discretion.
- *Reporting*. FireEye will supply Customer with monthly reports detailing technical support provided during the previous month. Quarterly business reviews will also be conducted.

(c) Government Support, if available, includes all of the services set forth above under Platinum Support [section 2.2(a)] and additionally:

- *Email, Live Chat, Web or Telephone Support*. For the specified country, access to citizens of that country for the fulfillment of Level 1 and 2 technical support requests.

(d) Government Priority Plus Support includes all of the services set forth above under Government Support [section 2.2(c)] and additionally:

- *Access to Support*. Customer will be provided with direct priority access to Level 2 Advanced Engineering support who are citizens of that country and shall respond to Customer's unlimited number of designated contacts. A Designated Support Engineer (DSE) point of contact who is a citizen of that country and available during Customer's business hours (for single Customer site if Product(s) installed at multiple Customer sites), will be made available to be the focal point of contact within FireEye, to project manage Customer's technical issues.
- *Onsite Support*. Onsite visits for problem assistance at DSE's sole discretion.
- *Reporting*. FireEye will supply Customer with monthly reports detailing technical support provided during the previous month. Quarterly business reviews will also be scheduled.

(e) Special Services. FireEye agrees to use commercially reasonable efforts to respond to any requests by Customer for support services not specifically provided for above. Customer acknowledges that all such services provided by FireEye shall be at FireEye's discretion and then-current fees and policies.

3. CUSTOMER RESPONSIBILITIES.

3.1 Requesting Support Services. When requesting Support Services from FireEye under this Agreement, Customer should have the following information available to provide to FireEye, if requested: (i) detailed problem description, including operating system ("OS") version, Product model and serial number(s), of the affected Product, and a detailed description of the troubleshooting that has already been done to try to resolve the problem; (ii) detailed system log files; (iii) configuration and login details to allow FireEye access as needed to the Products via the Internet for the purpose of providing support services and permissions needed in order for FireEye to conduct such remote access; (iv) a detailed description of changes to the environment; and (v) Customer's unique ID, Account ID, the serial number(s) of the Product(s) covered by this Agreement or other unique customer identifier as assigned to Customer by FireEye. Customer acknowledges and agrees that failure to have any or all information or access available as needed by FireEye in order to provide the Support Services may result in delays in FireEye's response, may hinder FireEye's ability to perform the Support Services and/or may cause incorrect Support Program fulfillment. FireEye will not be responsible for any such delays and inability to perform due to causes not due to FireEye.

3.2 Customer Assistance. Customer agrees to: (i) ensure that their site complies with any and all applicable FireEye published system environmental specifications; (ii) follow FireEye's procedures when requesting Support Services; (iii) provide FireEye reasonable access to all necessary personnel to answer questions or resolve problems reported by Customer regarding the Products; (iv) promptly implement all Updates and error corrections provided by FireEye under this Agreement; (v) maintain FireEye supported versions of required third party software, if any; and (v) notify FireEye promptly of any relocation of the Products from the location to which the Products were originally shipped. Customer agrees to use reasonable efforts to resolve internally any support questions prior to requesting Support Services pursuant to this Agreement. During the Support Term, FireEye may obtain information regarding Customer's email communication and Customer agrees that, as a condition to FireEye's provision of Support Services, FireEye may use statistical data generated regarding Customer's email correspondence with customer support so long as the source or content of the emails is not being disclosed.

3.3 Contact People. Customer shall appoint the specified number of individuals (depending upon the Support Program purchased) within Customer's organization to serve as contacts between Customer and FireEye and to receive support through FireEye's telephone support center. Customer's contacts shall have been adequately trained on the Products and shall have sufficient technical expertise, training and experience. All of Customer's support inquiries shall be initiated through these contacts.

4. EXCLUSIONS. Notwithstanding anything else contained in this Agreement to the contrary, FireEye shall have no obligation or responsibility to provide any Support Services relating to problems arising out of or related to (i) Customer's failure to implement all Updates to the Product which are made available to Customer under this Agreement; (ii) the failure to provide a suitable installation environment; (iii) any alteration, modification, enhancement or addition to the Products performed by parties other than FireEye; (iv) use of the Products in a manner, or for a purpose, for which they were not designed; (v) accident, abuse, neglect, unauthorized repair, inadequate maintenance or misuse of the Products; or relocation of the Products (including without limitation damage caused by use of other than FireEye shipping containers), (vi) operation of the Products outside of environmental specifications; (vii) interconnection of the Products with other products not supplied by FireEye; (viii) use of the Products on any systems other than the specified hardware platform for such Products; or (ix) introduction of data into any database used by the Products by any means other than the use of the software associated with the Products. Notwithstanding anything else contained in this Agreement to the contrary, FireEye will support all generally available ("GA") versions of the FireEye OS, for a minimum of one (1) year from GA release date, regardless of the number of supported OS GA versions. FireEye will also support the two (2) most current OS GA versions, regardless of the elapsed time from GA release date. If available, and at FireEye's sole discretion, support for any other OS versions or for other problems not covered under this Agreement may be obtained at FireEye's then-current fees and policies for such services. FireEye's complete end of life policy can be found at http://www.fireeye.com/support/supported-products.html

5. LAPSED SUPPORT AND UPGRADED SUPPORT.

5.1 Lapsed Support. After any lapse of Support Services, the parties subsequently may elect to reinstate such Support Services for Products for which the Support Services lapsed pursuant to the terms and conditions set forth in this Agreement; provided, however, that (i) Customer agrees to pay for the period of time that has lapsed as well as any renewal term, and (ii) such Products must be in good working condition, as solely determined by FireEye or its designee.

5.2 Support Program Upgrade. At any time during the Term, Customer may upgrade to FireEye's next level of Support Program by (i) notifying FireEye of Customer's desire to upgrade; (ii) acknowledging in writing the then-current terms and conditions for the relevant Support Program; and (iii) paying FireEye the additional Support Fee owed in connection with such upgraded Support Program.

Exhibit A
Product Passthrough Terms – Google Apps for Work (for Customers)

Customer has entered into a certain written agreement (the "Agreement") pursuant to which Customer has purchased the right to access and use the Product. These Product Passthrough Terms set forth the terms and conditions under which Customer may access and use such Product.

1. Product.

   1.1 Facilities and Data Transfer. All facilities used to store and process Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Provider stores and processes its own information of a similar type. Provider has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data, protect against anticipated threats or hazards to the security or integrity of Customer Data, and protect against unauthorized access to or use of Customer Data. As part of providing the Product, Provider may transfer, store and process Customer Data in the United States or any other country in which Provider or its agents maintain facilities. By using the Product, Customer consents to this transfer, processing and storage of Customer Data.

   1.2 Modifications.

      a. To the Product. Provider may make commercially reasonable changes to the Product, from time to time. If Provider makes a material change to the Product, Customer may be informed of such change, provided that Customer has subscribed with Provider to be informed about such change.

      b. To URL Terms. Provider may make commercially reasonable changes to the URL Terms from time to time. If Provider makes a material change to the URL Terms, Customer may be informed of such change through the Notification Email Address or via the Admin Console. If the change has a material adverse impact on Customer and Customer does not agree to the change, Customer must so notify Partner or Provider via the Help Center within thirty days after receiving notice of the change. Upon such notification, Customer will remain governed by the URL Terms in effect immediately prior to the change until the end of the then-current term for the affected Product. If the affected Product is renewed, they will be renewed under Provider's then current URL Terms.

   1.3 Customer Domain Name Ownership. Prior to providing the Product, Provider or Partner may verify that Customer owns or controls the Customer Domain Names. If Customer does not own, or control, the Customer Domain Names, then Provider will have no obligation to provide Customer with the Product.

   1.4 Federal Information Security Management Act (FISMA). The Provider's Product known as "Google Apps Core Services" received a FISMA "Authorization to Operate" for a Moderate impact system. Provider will continue to maintain a System Security Plan (SSP) for the Google Apps Core Services, based on NIST 800-53 Rev. 3, or a similarly applicable standard. If Provider does not maintain this SSP as stated, Customer's sole and exclusive remedy, and Provider's entire liability, will be Customer's ability to terminate use of the Product upon thirty days prior written notice.

2. Customer Obligations.

   2.1 Compliance. Customer will use the Product in accordance with the Acceptable Use Policy. Provider may make new applications, features or functionality for the Product available from time to time, the use of which may be contingent upon Customer's agreement to additional terms. In addition, Provider will make other Non-Google Apps Products (beyond the Product) available to Customer and its End Users in accordance with the Non-Google Apps Product Terms and the applicable product-specific Provider terms of service. If Customer does not desire to enable any of the Non-Google Apps Products, Customer can enable or disable them at any time through the Admin Console.

   2.2 Customer Administration of the Product. Customer may specify one or more Administrators through the Admin Console who will have the rights to access Admin Account(s) and to administer the End User Accounts. Customer and Partner are responsible for: (a) maintaining the confidentiality of the password and Admin Account(s); (b) designating those individuals who are authorized to access the Admin Account(s); and (c) ensuring that all activities that occur in connection with the Admin Account(s) comply with these

Product Passthrough Terms. Customer agrees that Provider's responsibilities do not extend to the internal management or administration of the Product for Customer and that Provider is merely a data-processor.

2.3 End User Consent. Customer's Administrators may have the ability to access, monitor, use, or disclose data available to End Users within the End User Accounts. Customer will obtain and maintain all required consents from End Users to allow: (i) Customer's access, monitoring, use and disclosure of this data and Provider providing Customer with the ability to do so, and (ii) Provider to provide the Product.

2.4 Unauthorized Use. Customer will use commercially reasonable efforts to prevent unauthorized use of the Product, and to terminate any unauthorized use. Customer or Reseller will promptly notify Provider of any unauthorized use of, or access to, the Product of which it becomes aware.

2.5 Restrictions on Use. Unless Provider specifically agrees in writing, Customer will not, and will use commercially reasonable efforts to make sure a third party does not: (a) sell, resell, lease, or the functional equivalent, the Product to a third party (unless expressly authorized in these Product Passthrough Terms); (b) attempt to reverse engineer the Product or any component; (c) attempt to create a substitute or similar service through use of, or access to, the Product; (d) use the Product for High Risk Activities; or (e) use the Product to store or transfer any Customer Data that is controlled for export under Export Control Laws. Customer is solely responsible for any applicable compliance with HIPAA.

2.6 Third Party Requests. Customer is responsible for responding to Third Party Requests. Provider will, to the extent allowed by law and by the terms of the Third Party Request: (a) promptly notify Customer of its receipt of a Third Party Request; (b) comply with Customer's reasonable requests regarding its efforts to oppose a Third Party Request; and (c) provide Customer with the information or tools required for Customer to respond to the Third Party Request. Customer will first seek to obtain the information required to respond to the Third Party Request on its own, and will contact Provider only if it cannot reasonably obtain such information.

3. Technical Support Services.

3.1 By Customer. Customer or Partner will, at its own expense, respond to questions and complaints from End Users or third parties relating to Customer's or End Users' use of the Product. Customer or Partner will use commercially reasonable efforts to resolve support issues before escalating them to Provider.

3.2 By Provider. If Customer or Partner cannot resolve a support issue consistent with the above, then Customer or Partner (as applicable based on the agreement between Provider and Partner) may escalate the issue to Provider in accordance with the TSS Guidelines. Provider will provide TSS to Customer or Partner (as applicable) in accordance with the TSS Guidelines.

4. Suspension.

4.1 Of End User Accounts by Provider. If Provider becomes aware of an End User's violation of these Product Passthrough Terms, then Provider may specifically request that Customer Suspend the applicable End User Account. If Customer fails to comply with Provider's request to Suspend an End User Account, then Provider may do so. The duration of any Suspension by Provider will be until the applicable End User has cured the breach which caused the Suspension.

4.2 Emergency Security Issues. Notwithstanding the foregoing, if there is an Emergency Security Issue, then Provider may automatically Suspend the offending use. Suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the Emergency Security Issue. If Provider Suspends an End User Account for any reason without prior notice to Customer, at Customer's request, Provider will provide Customer the reason for the Suspension as soon as is reasonably possible.

5. Confidential Information.

5.1 Obligations. Customer and Provider will: (a) protect the other's Confidential Information with the same standard of care it uses to protect its own Confidential Information; and (b) not disclose the Confidential Information, except to Affiliates, employees and agents who need to know it and who have agreed in writing to keep it confidential. Customer and Provider (and any Affiliates, employees and agents to whom it has disclosed Confidential Information) may use Confidential Information only to exercise rights and fulfill its obligations under these Product Passthrough Terms, while using reasonable care to protect it. Customer

and Provider, respectively, will be responsible for any actions of its Affiliates, employees and agents in violation of this Section.

5.2 Exceptions. Confidential Information does not include information that: (a) the recipient of the Confidential Information already knew; (b) becomes public through no fault of the recipient; (c) was independently developed by the recipient; or (d) was rightfully given to the recipient by a third party.

5.3 Required Disclosure. Customer and Provider may disclose the other's Confidential Information when required by law but only after it, if legally permissible: (a) uses commercially reasonable efforts to notify the other; and (b) gives the other the chance to challenge the disclosure.

6. Intellectual Property Rights; Brand Features.

6.1 Intellectual Property Rights. Except as expressly set forth herein, these Product Passthrough Terms does not grant either Customer or Provider any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the Customer and Provider, Customer owns all Intellectual Property Rights in Customer Data, and Provider owns all Intellectual Property Rights in the Product.

6.2 Display of Brand Features. Provider may display those Customer Brand Features authorized by Customer (such authorization is provided by Customer uploading its Brand Features into the Product), and within designated areas of the Service Pages. Customer may specify the nature of this use using the Admin Console. Provider may also display Provider Brand Features on the Service Pages to indicate that the Product are provided by Provider. Neither party may display or use the other party's Brand Features beyond what is allowed in these Product Passthrough Terms without the other's prior written consent.

6.3 Brand Features Limitation. Any use of Brand Features will inure to the benefit of the entity holding Intellectual Property Rights in those Brand Features. Any right to use its Brand Features pursuant to these Product Passthrough Terms may be revoked at any time with written notice to the other and a reasonable period to stop the use.

7. Publicity. Customer agrees that Provider may include Customer's name or Brand Features in a list of Provider customers, online or in promotional materials. Customer also agrees that Provider may verbally reference Customer as a customer of the Provider's Product that is the subject of these Product Passthrough Terms.

8. Representations, Warranties and Disclaimers.

8.1 Representations and Warranties. Customer and Provider represent that each will comply with all laws and regulations applicable to its provision, or use, of the Product, as applicable (including applicable security breach notification law). Provider warrants that it will provide the Product in accordance with the applicable SLA.

8.2 Disclaimers. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR HEREIN, NEITHER PARTY MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. PROVIDER MAKES NO REPRESENTATIONS ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE PRODUCT. CUSTOMER ACKNOWLEDGES THAT THE PRODUCT IS NOT A TELEPHONY SERVICE AND THAT THE PRODUCT IS NOT CAPABLE OF PLACING OR RECEIVING ANY CALLS, INCLUDING EMERGENCY PRODUCT CALLS, OVER PUBLICLY SWITCHED TELEPHONE NETWORKS.

9. Term and Termination.

9.1 Term. The term for the Product will be as decided upon between Partner and Customer. These Product Passthrough Terms will remain in effect for the Term.

9.2 Termination for Breach. The Services may be suspended or terminated, if: (i) Customer is in material breach of these Product Passthrough Terms and fails to cure that breach within thirty days after receipt of written notice; (ii) Customer ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within ninety days; or (iii) Customer is in material breach of these Product Passthrough Terms more than two times notwithstanding any cure of such breaches.

9.3 Effects of Termination. If Services are terminated, then: (i) the rights granted by Provider to Customer, and Customer to Provider will cease immediately (except as set forth in this Section); (ii) neither Customer nor Partner will have access to, or the ability to export, the Customer Data; (iii) Provider will begin to delete Customer Data; and (iv) upon request will promptly use commercially reasonable efforts to return or destroy all other Confidential Information of the other.

10. Miscellaneous.

10.1 Product Development. The Product was developed solely at private expense and is commercial computer software and related documentation within the meaning of the applicable civilian and military federal acquisition regulations and any supplements thereto.

10.2 Force Majeure. Due to circumstances beyond Provider's controls, Provider may not be able to provide the Product.

10.3 No Waiver. Failure to enforce any provision of these Product Passthrough Terms will not constitute a waiver.

10.4 No Agency. These Product Passthrough Terms do not create any agency, partnership or joint venture.

10.5 No Third-Party Beneficiaries. There are no third-party beneficiaries to these Product Passthrough Terms. Customer's sole remedies will be set forth in its agreement with the Partner.

10.6 Survival. The following sections will survive expiration or termination of these Product Passthrough Terms: Sections 5, 6, 9.3, 10 and 12.

10.7 Severability. If any term (or part of a term) of these Product Passthrough Terms is invalid, illegal, or unenforceable, the rest of these Product Passthrough Terms will remain in effect.

10.8 Conflicting Terms. If there is a conflict between any terms of these Product Passthrough Terms and any other document that makes up the entire agreement as needed for Customer to use the Product, the terms of these Product Passthrough Terms will take precedence.

11. Additional Product Terms.

11.1 Ads. Provider does not serve Ads in the Product or use Customer Data for Ads purposes.

11.2 Aliases. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names but Provider may monitor emails sent to these aliases for Customer Domain Names to allow Provider to identify Product abuse.

11.3 Google Apps Vault Retention. If Customer is using Google Apps Vault, Provider will have no obligation to retain any archived Customer Data beyond the retention period specified by Customer. If Customer does not renew Google Apps Vault, Provider will have no obligation to retain any archived Customer Data.

12. Definitions.

"Acceptable Use Policy" means the acceptable use policy for the Product available at http://www.google.com/a/help/intl/en/admins/use_policy.html. The Acceptable Use Policy and such URL link may be updated or modified by Provider from time to time.

"Admin Account(s)" means the administrative account(s) provided to Customer for the purpose of administering the Product. The use of the Admin Account(s) requires a password, which Provider will provide to Customer or Partner.

"Admin Console" means the online tool Customer may use in reporting and certain other administration functions.

"Administrators" mean the Customer-designated technical personnel who administer the Product to End Users on Customer's behalf.

"Ads" means online advertisements displayed by Provider to End Users, excluding advertisements provided by any advertising products that are not part of the Product that Customer chooses to use in connection with the Product.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with an entity.

"Brand Features" means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured from time to time.

"Confidential Information" means information disclosed or exchanged under these Product Passthrough Terms that is marked as confidential or would normally be considered confidential under the circumstances. Customer Data is Customer's Confidential Information.

"Customer Data" means data, including email, provided, generated, transmitted or displayed via the Product by Customer, End Users, or Partner on behalf of Customer.

"Customer Domain Names" mean the domain names owned or controlled by Customer, which will be used in connection with the Product.

"Emergency Security Issue" means either: (a) Customer's use of the Product in violation of the Acceptable Use Policy, which could disrupt: (i) the Product; (ii) other customers' use of the Product; or (iii) the Provider network or servers used to provide the Product; or (b) unauthorized third party access to the Product.

"End Users" means the individuals Customer permits to use the Product.

"End User Account" means a Provider-hosted account established by Customer through the Product for an End User.

"Export Control Laws" means all applicable export and reexport control laws and regulations, including trade and economic sanctions maintained by the Treasury Department's Office of Foreign Assets Control, and the International Traffic in Arms Regulations ("ITAR") maintained by the Department of State.

"Google Apps Core Services" means the applicable Product purchased by Customer from Partner which are more fully described here: http://www.google.com/a/help/intl/en/users/user_features.html. The Google Apps Core Services and such URL link may be updated or modified by Provider from time to time.

"Help Center" means the Provider help center accessible at http://www.google.com/support/. The Help Center and such URL link may be updated or modified by Provider from time to time.

"High Risk Activities" means uses such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Product could lead to death, personal injury, or environmental damage.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as may be amended from time to time, and any regulations issued thereunder.

"Intellectual Property Rights" means current and future worldwide rights under patent law, copyright law, trade secret law, trademark law, moral rights law, and other similar rights.

"Non-Google Apps Products" means Provider products which are not part of the Product, but which may be accessed by End Users using their End User Account login and password. The Non-Google Apps Products are set forth at the following URL: http://www.google.com/support/a/bin/answer.py?hl=en&answer=181865. The Non-Google Apps Products and such URL link may be updated or modified by Provider from time to time.

"Non-Google Apps Product Terms" means the terms found at the following URL: http://www.google.com/apps/intl/en/terms/additional_services.html. The Non-Google Apps Product Terms and such URL link may be updated or modified by Provider from time to time.

"Notification Email Address" means the email address designated by Customer to receive email notifications from Provider. Customer may provide a Partner email address for this purpose if it so chooses. Customer may change this email address through the Admin Console.

"Provider" means the third party provider of the Product.

"Partner" means the entity Customer is paying to provide access to and use of the Product.

"Service Pages" mean the web pages displaying the Product to End Users.

"Product" means, as applicable, the Google Apps Core Services purchased from Partner.

"SLA" means the Service Level Agreement located here for applicable Google Apps Core Services: http://www.google.com/apps/intl/en/terms/reseller_sla.html. The SLA and such URL link may be updated or modified by Provider from time to time.

"Suspend" means the immediate disabling of access to the Product, or components of the Product, as applicable, to prevent further use of the Product.

"Term" means the term of these Product Passthrough Terms, which will continue for as long as Customer is receiving Product from Provider, unless terminated earlier pursuant to these Product Passthrough Terms, or pursuant to Customer's agreement with Partner.

"Third Party Request" means a request from a third party for records relating to an End User's use of the Product. Third Party Requests can be a lawful search warrant, court order, subpoena, other valid legal order, or written consent from the End User permitting the disclosure.

"TSS" means the technical support Product provided by Provider to the Administrators during the Term pursuant to the TSS Guidelines.

"TSS Guidelines" means Provider's technical support Product guidelines then in effect for the Product. TSS Guidelines are at the following URL: http://www.google.com/a/help/intl/en/admins/tssg.html. The TSS Guidelines and such URL link may be updated or modified by Provider from time to time.

"URL Terms" means the Acceptable Use Policy, the SLA and the TSS Guidelines.

SALESFORCE Service Terms

"AppExchange" means the online directory of on-demand applications that work with the Service, located at http://www.appexchange.com or at any successor websites.

"Service" means the online, Web-based application provided by Salesforce.com (sometimes referred to as "SFDC") via http://www.salesforce.com and/or other designated websites, including associated offline components but excluding AppExchange applications.

"Third-Party Applications" means online, Web-based applications and offline software products that are provided by third parties, interoperate with the Service, and are identified as third-party applications, including but not limited to those listed on the AppExchange.

"User Guide" means the online user guide for the Services, accessible via http://www.salesforce.com, as updated from time to time.

"Users" means Your employees, representatives, consultants, contractors or agents who are authorized to use the Service and have been supplied user identifications and passwords by You (or by Salesforce.com or Your reseller at Your request).

"You" and **"Your"** means the customer entity which has contracted to purchase subscriptions to use the Service subject to the conditions of these SFDC Service Terms.

"Your Data" means all electronic data or information submitted by You to the Service.

1. **Use of Service**

(a) User subscriptions cannot be shared or used by more than one User (but may be reassigned from time to time to new Users who are replacing former Users who have terminated employment with You or otherwise changed job status or function and no longer require use of the Service).

(b) You (i) are responsible for all activities occurring under Your User accounts; (ii) are responsible for the content of all Your Data; (iii) shall use commercially reasonable efforts to prevent unauthorized access to, or use of, the Service, and shall notify Your reseller or Salesforce.com promptly of any such unauthorized use You become aware of; and (iv) shall comply with all applicable federal laws and regulations in using the Service.

(c) You shall use the Service solely for Your internal business purposes and shall not: (i) license, sublicense, sell, resell, rent, lease, transfer, assign, distribute, time share or otherwise commercially exploit or make the Service available to any third party, other than to Users or as otherwise contemplated by these SFDC Service Terms; (ii) send spam or otherwise duplicative or unsolicited messages in violation of applicable laws; (iii) send or store infringing, obscene, threatening, libelous, or otherwise unlawful or tortious material, including material that is harmful to children or violates third party privacy rights; (iv) send or store viruses, worms, time bombs, Trojan horses and other harmful or malicious code, files, scripts, agents or programs; (v) interfere with or disrupt the integrity or performance of the Service or the data contained therein; or (vi) attempt to gain unauthorized access to the Service or its related systems or networks.

(d) You shall not (i) modify, copy or create derivative works based on the Service; (ii) frame or mirror any content forming part of the Service, other than on Your own intranets or otherwise for its own internal business purposes; (iii) reverse engineer the Service; or (iv) access the Service in order to (A) build a competitive product or service, or (B) copy any ideas, features, functions or graphics of the Service.

2. **Service Provision.** Salesforce.com will use commercially reasonable efforts to make the Services available 24 hours a day, 7 days a week, except for: (a) planned downtime (of which SFDC shall give at least 8 hours notice via the Services and which SFDC shall schedule to the extent practicable during the weekend hours from 6:00 p.m. Pacific time Friday to 3:00 a.m. Pacific time Monday), or (b) any unavailability caused by circumstances beyond SFDC's reasonable control, including without limitation, acts of God, acts of government, flood, fire, earthquakes, civil unrest, acts of terror, strikes or other labor problems (other than those involving SFDC employees), or Internet service provider failures or delays.

Salesforce.com will provide the Services only in accordance with applicable laws and government regulations.

3. **Acquisition of Third-Party Products and Services.** Any acquisition by You of third-party products or services, including but not limited to Third-Party Applications and implementation, customization and other consulting services, and any exchange of data between You and any third-party provider, is solely between You and the applicable third-party provider. Salesforce.com does not warrant or support third-party products or services, whether or not they are designated by Salesforce.com as "certified" or otherwise. No purchase of third-party products or services is required to use the Service as provided by Salesforce.com.

4. **Third-Party Applications and Your Data.** If You install or enable Third-Party Applications for use with the Service, You acknowledge that Salesforce.com may allow providers of those Third-Party Applications to access You Data as required for the interoperation of such Third Party Applications with the Service. Salesforce.com shall not be responsible for any disclosure, modification or deletion of You Data resulting from any such access by Third-Party Application providers. The Service shall allow You to restrict such access by restricting Users from installing or enabling such Third-Party Applications for use with the Service.

5. **Google Services.** Service features that interoperate with Google services depend on the continuing availability of the Google application programming interface ("API") and program for use with the Service. If Google Inc. ceases to make the Google API or program available on reasonable terms for the Service, Salesforce.com may cease providing such Service features without entitling You to any refund, credit, or other compensation.

6. **Proprietary Rights.** Subject to the limited rights expressly granted hereunder, Salesforce.com reserves all rights, title and interest in and to the Service, including all related intellectual property rights. The Service is deemed Salesforce.com confidential information, and You will not use it or disclose it to any third party except as permitted in these SFDC Service Terms and except as required by law, upon notice to Salesforce.com.

7. **Your Data.** As between Salesforce.com and You, You exclusively own all rights, title and interest in and to all of Your Data. Your Data is deemed your confidential information, and Salesforce.com shall not access Your User accounts, including Your Data, except to respond to service or technical problems or at your request.

8. **Compelled Disclosure.** If either You or Salesforce.com is compelled by law to disclose confidential information of the other party, it shall provide the other party with prior notice of such

compelled disclosure (to the extent legally permitted) and reasonable assistance, at the other party's cost, if the other party wishes to contest the disclosure.

9. **Suggestions.** You agree that Salesforce.com shall have a royalty-free, worldwide, transferable, sublicenseable, irrevocable, perpetual license to use or incorporate into the Service any suggestions, enhancement requests, recommendations or other feedback provided by You or Your Users relating to the operation of the Service.

10. **Fees.** Contracted for fees for use of the Service represent a firm commitment and the number of User subscriptions contracted for cannot be reduced in the middle of a subscription term.

11. **Termination.** The master contract governs your termination (FAR 52.212-4(l) & (m)) and cancellation rights with the contractor, and the contract requires continued performance while any disputes are resolved (FAR 52.233-1(i)).

12. **Data Storage.** You are entitled to a cumulative amount of storage per User subscription for no additional charge as set forth in the User Guide for the Service subscription type purchased. You may purchase additional storage if necessary, and you may contact Your reseller for then-current rates listed in master contract price list.

13. **Support.** SFDC will provide You with basic support as described from time to time by SFDC at www.salesforce.com. In the event that You have purchased an upgraded support package, then upgraded support contact information will be provided to You together with your initial account set up information.

14. **No Warranty.** SALESFORCE.COM MAKES NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE REGARDING THE SERVICE AND/OR SUPPORT, AND SPECIFICALLY DISCLAIMS ALL IMPLIED WARRANTIES, INCLUDING ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. IN THE EVENT THAT YOUR AGREEMENT WITH YOUR RESELLER PROVIDES ANY WARRANTIES WITH RESPECT TO THE SERVICE AND/OR SUPPORT, SUCH WARRANTIES ARE SOLELY BETWEEN YOU AND YOUR RESELLER. This clause does not disclaim any warranties expressly provided in a contract with the U.S. Government."

15. **No Liability.** IN NO EVENT SHALL SALESFORCE.COM HAVE ANY LIABILITY TO YOU OR ANY USER FOR ANY DAMAGES WHATSOVER, INCLUDING BUT NOT LIMITED TO DIRECT, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR DAMAGES BASED ON LOST PROFITS, HOWEVER CAUSED AND, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, WHETHER OR NOT EITHER YOU OR SALESFORCE.COM HAVE BEEN ADVISED OF THE POSSIBILI TY OF SUCH DAMAGES. This clause shall not impair the

U.S. Government's right to recover for fraud or crimes arising out of or related to this Contract under any federal fraud statute, including the False Claims Act, 31 U.S.C. §§ 3729-3733. Furthermore, this clause shall not impair nor prejudice the U.S. Government's right to EXPRESS remedies provided in the Contract (i.e. clause 552.238-72 – Price Reductions, clause 52.212-4(h) – Patent Indemnification, Liability for Injury or Damage (Section 3 of the Price List), and GSAR 552.215-72 – Price Adjustment – Failure to Provide Accurate Information).

16. **Further Contact.** Salesforce.com may contact you regarding new Salesforce.com service features and offerings.

17. **Third Party Beneficiary.** SFDC shall be a third party beneficiary to the agreement between You and Reseller solely as it relates to these SFDC Service Terms.

SOFTWARE LICENSE AND SUPPORT AGREEMENT
General Terms and Conditions
("GTC")

1. DEFINITIONS.

1.1 "Add-on" means any development using SAP API's that adds new and independent functionality, but does not modify existing SAP functionality.

1.2 "Agreement" means these GTCs, any Order Form referencing these GTCs, and the Use Terms and Schedules referenced by these GTCs and/or such Order Forms. All such components are integral to the agreement, and collectively are referred to herein as the "Agreement".

1.3 "API" means SAP's application programming interfaces, as well as other SAP code that allow other software products to communicate with or call on SAP Software (for example, SAP Enterprise Services, BAPIs, Idocs, RFCs and ABAP or other user exits) provided under this Agreement.

1.4 "Affiliate" mean any legal entity in the Territory in which the Licensee, directly or indirectly, holds more than fifty percent (50%) of the shares or voting rights. Any such legal entity shall be considered an Affiliate for only such time as such equity interest is maintained.

1.5 "Business Partner" means a legal entity that requires access to the Software in connection with Licensee's internal business operations, such as customers, distributors and/or suppliers of Licensee.

1.6 "Confidential Information" means, with respect to SAP, all information which SAP protects against unrestricted disclosure to others, including but not limited to: (a) the Software and Documentation and other SAP Materials, including without limitation the following information regarding the Software: (i) computer software (object and source codes), programming techniques and programming concepts, methods of processing, system designs embodied in the Software; (ii) benchmark results, manuals, program listings, data structures, flow charts, logic diagrams, functional specifications, file formats; and (iii) discoveries, inventions, concepts, designs, flow charts, documentation, product specifications, application program interface specifications, techniques and processes relating to the Software; (b) the research and development or investigations of SAP; (c) product offerings, content partners, product pricing, product availability, technical drawings, algorithms, processes, ideas, techniques, formulas, data, schematics, trade secrets, know-how, improvements, marketing plans, forecasts and strategies; and (d) any information about or concerning any third party (which information was provided to SAP subject to an applicable confidentiality obligation to such third party). With respect to Licensee, "Confidential Information" means all information which Licensee protects against unrestricted disclosure to others and which (i) if in tangible form, Licensee clearly identifies as confidential or proprietary at the time of disclosure; and (ii) if in intangible form (including disclosure made orally or visually), Licensee identifies as confidential at the time of disclosure, summarizes the Confidential Information in writing, and delivers such summary within thirty (30) calendar days of any such disclosure.

1.7 "Documentation" means SAP's documentation which is delivered or made available to Licensee with the Software under this Agreement.

1.8 "Intellectual Property Rights" means patents of any type, design rights, utility models or other similar invention rights, copyrights, mask work rights, trade secret or confidentiality rights, trademarks, trade names and service marks and any other intangible property rights, including applications and registrations for any of the foregoing, in any country, arising under statutory or common law or by contract and whether or not perfected, now existing or hereafter filed, issued, or acquired.

1.9 "Modification" means (i) a change to the delivered source code or metadata; or (ii) any development, other than a change to the delivered source code or metadata, that customizes, enhances, or changes existing functionality of the Software including, but not limited to, the creation of any new application program interfaces, alternative user interfaces or the extension of SAP data structures; or (iii) any other change to the Software (other than an Add-on) utilizing or incorporating any SAP Materials (defined below).

1.10 "Professional Services Schedule" means the terms and conditions governing SAP's delivery of professional services, attached hereto and made a part hereof.

1.11 "SAP Materials" means any software, programs, tools, systems, data, or other materials made available by SAP to Licensee in the course of the performance under this Agreement including, but not limited to, the Software and Documentation, as well as any information, materials or feedback provided by Licensee to SAP relating to the Software and Documentation.

1.12 "SAP Support" means SAP's then-current SAP support offering specified in the applicable Order Forms and made available to Licensee as stated in the applicable SAP Support Schedule found at www.sap.com/company/legal/index.epx as of the effective date of the first Software Order Form issued under these GTCs. Such SAP Support Schedule is incorporated herein by reference. For the avoidance of doubt, such SAP Support Schedule shall apply to all Order Forms issued under these GTCs, unless otherwise agreed by the parties. SAP recommends Licensee prints a copy of the applicable SAP Support Schedule for Licensee's own records.

1.13 "Software" means (i) any and all software products licensed to Licensee under this Agreement as specified in Software Order Forms hereto, all as developed by or for SAP, SAP AG, Business Objects Software Limited and/or any of their affiliated companies and delivered to Licensee hereunder; (ii) any new releases thereof made available through unrestricted shipment pursuant to the respective support agreement and (iii) any complete or partial copies of any of the foregoing.

1.14 "Software Order Form" means the order form for the Software and related SAP Support ordered by Licensee thereunder, including information on Software, SAP Support, fees, and other information necessary for the delivery of such items to Licensee.

The Software Order Form does not include fees for professional services, which shall be billed under separate statements of work in accord with the Professional Services Schedule.

1.15 "Territory" means the world except for those countries prohibited by United States' export laws, and further subject to Section 12.4 of the GTC.

1.16 "Third Party Software" means (i) any and all software products and content licensed to Licensee under this Agreement as specified in Software Order Forms hereto, all as developed by companies other than SAP, SAP AG, Business Objects Software Limited and/or any of their affiliated companies and delivered to Licensee hereunder; (ii) any new releases thereof made available through unrestricted shipment pursuant to the respective SAP Support Schedule and (iii) any complete or partial copies of any of the foregoing.

1.17 "Use" means to activate the processing capabilities of the Software, load, execute, access, employ the Software, or display information resulting from such capabilities.

1.18 "Use Terms" means, with regard to Software specified in a Software Order Form, the SAP Software Use Rights document current at the time of execution of such Software Order Form, copies of which are found at www.sap.com/company/legal/index.epx and made a part hereof. Such SAP Software Use Rights documents are incorporated herein by reference. SAP recommends Licensee prints copies of the applicable SAP Software Use Rights documents for Licensee's own records

2. LICENSE GRANT.

2.1 License.

2.1.1 Subject to Licensee's compliance with all the terms and conditions of this Agreement, SAP grants to Licensee a non-exclusive, perpetual (except for subscription based or term licenses) license to Use the Software, Documentation, and other SAP Materials at specified site(s) within the Territory to run Licensee's and its Affiliates' internal business operations (including customer back-up and passive disaster recovery) and to provide internal training and testing for such internal business operations and as further set forth in the Software Order Form, unless terminated in accordance with Section 5 herein. This license does not permit Licensee (without being limited specifically to such restrictions) to: (i) use the SAP Materials to provide services to third parties (e.g., business process outsourcing, service bureau applications or third party training) other than to Affiliates (subject to Section 2.2); (ii) lease, loan, resell, sublicense or otherwise distribute the SAP Materials, other than distribution to Affiliates (subject to Section 2.2); (iii) make any Use of or perform any acts with respect to the SAP Materials other than as expressly permitted in accordance with the terms of this Agreement; or (iv) use Software components other than those specifically identified in the Software Order Form, even if it is also technically possible for Licensee to access other Software components. Business Partners may Use the Software only through screen access and solely in conjunction with Licensee's Use and may not Use the Software to run any of Business Partners' business operations.

2.1.2 Licensee agrees to install the Software only on information technology devices (e.g. hard disks or central processing units) identified by Licensee pursuant to this Agreement and that has been previously approved by SAP in writing or otherwise officially made known to the public as appropriate for Use or interoperation with the Software (the "Designated Unit"). Licensee must hold the required licenses as stated herein and in the applicable Order Forms, for any individuals that Use the Software, including employees or agents of Affiliates and Business Partners. Use may occur by way of an interface delivered with or as a part of the Software, a Licensee or third-party interface, or another intermediary system.

2.1.3 The terms and conditions of this Agreement relative to "Software" apply to Third Party Software except as otherwise stated in the Software Use Rights Schedule, a Schedule, an Order Form, or an Amendment.

2.2 Affiliate Use. Affiliates' Use of the Software, Documentation and other SAP Materials to run their internal business operations as permitted under Section 2.1.1 is subject to the following: (i) the Affiliate agrees to be bound by the terms herein in the form of Schedule A ("Affiliate Use Agreement") attached hereto; and (ii) a breach of such Affiliate Use Agreement by Affiliate shall be considered a breach by Licensee hereunder. If Licensee has an affiliate or subsidiary with a separate agreement for SAP software licenses and/or support services with SAP AG, any SAP AG affiliate (including SAP) or any other distributor of SAP software, the Software shall not be Used to run such affiliate's or subsidiary's business operations and such affiliate or subsidiary shall not receive any support services under this Agreement even if such separate agreement has expired or is terminated, unless otherwise agreed to in writing by the parties.

2.3 Outsourcing Services. With SAP's prior written consent, Licensee may permit services providers to access the Software solely for the purpose of providing facility, implementation, systems, application management or disaster recovery services to Licensee in connection with the business of Licensee for which the Software is herein licensed provided: (i) Licensee and such services provider execute a written agreement that includes provisions requiring such services provider's compliance with the terms of this Agreement prior to such access, including without limitation non-disclosure of SAP Confidential Information; (ii) Licensee shall hold the required licenses as stated in the Use Terms for all employees of such services provider authorized to access the Software; (iii) such services provider shall be permitted to Use the Software solely to install and configure the Software in accordance with the business of Licensee as set forth herein (or in the case of a disaster recovery vendor, to provide disaster recovery services only); (iv) under no circumstances may such services provider Use the Software to operate or provide processing services to Licensee or any other party, or in connection with such services provider's own business operations; (v) Licensee shall be responsible for any additional Software, migration tools, or third party software needed to effect such transition; and (vi) Licensee expressly agrees to indemnify SAP, its officers, employees, agents and subcontractors from and against all claims, liabilities, losses, damages and costs (including reasonable attorney fees) suffered by SAP arising from a breach by the services provider of the conditions of this Agreement. Upon SAP request, Licensee shall provide written confirmation to SAP that items (i)-(iv) are fulfilled.

3. VERIFICATION. SAP shall be permitted to audit (at least once annually and in accordance with SAP standard procedures, which may include on-site and/or remote audit) the usage of the SAP Materials. Licensee shall cooperate reasonably in the conduct of such audits. In the event an audit reveals that (i) Licensee underpaid license fees and/or SAP Support fees to SAP and/or (ii) that Licensee has Used the Software in excess of the license quantities or levels stated in the Software Order Form, Licensee shall pay such underpaid fees and/or for such excess usage based on SAP List of Prices and Conditions Software and Support governing use in effect at the time of the audit, and shall execute an additional Software Order Form in accordance with the terms of this Agreement

to affect the required licensing of any additional quantities or levels. Reasonable costs of SAP's audit shall be paid by Licensee if the audit results indicate usage in excess of the licensed quantities or levels. SAP reserves all rights at law and equity with respect to both Licensee's underpayment of License fees or SAP Support fees and usage in excess of the license quantities or levels.

4. PRICE, PAYMENT, AND DELIVERY.

4.1 Fees. Licensee shall pay to SAP license fees for the Software and fees for SAP Support on the terms in Software Order Forms hereto. Fees for consulting services will be paid as set forth in the Professional Services Schedule. Any fees not paid when due shall accrue interest at the rate of 18% (eighteen percent) per annum, but not to exceed the maximum amount as allowed by law.

4.2 Taxes. Fees and other charges described in this Agreement do not include federal, state or local sales, foreign withholding, use, property, excise, service, or similar transaction taxes ("Tax(es)") now or hereafter levied, all of which shall be for Licensee's account. Any applicable direct pay permits or valid tax-exempt certificates must be provided to SAP prior to the execution of this Agreement. If SAP is required to pay Taxes, Licensee shall reimburse SAP for such amounts. Licensee hereby agrees to indemnify SAP for any Taxes and related costs, interest and penalties paid or payable by SAP.

4.3 Delivery of the Software and SAP Support. SAP will deliver the Software and SAP Support by making it available for electronic download through the SAP ServiceMarketplace (http://service.sap.com/swdc) to Licensee. Risk of loss passes at the time of such electronic delivery. Licensee agrees not to request any physical delivery of Software or SAP Support and should it occur that any such delivery will be rejected by Licensee. Licensee agrees and understands that the calculation of Taxes may be affected by the delivery method and delivery location of the Software and corresponding SAP Support.

5. TERM.

5.1. Term. This Agreement and the license granted hereunder shall become effective as of the date first set forth in the first Software Order Form issued under these GTCs, and shall continue in effect thereafter unless this Agreement is terminated upon the earliest to occur of the following: (i) thirty days after Licensee gives SAP written notice of Licensee's direction to terminate this Agreement, for any reason, but only after payment of all license and SAP Support fees then due and owing; (ii) thirty days after SAP gives Licensee notice of Licensee's material breach of any provision of the Agreement (other than Licensee's breach of its obligations under Sections 6, 10 or 11, which breach shall result in immediate termination), including more than thirty days delinquency in Licensee's payment of any money due hereunder, unless Licensee has cured such breach during such thirty day period; (iii) immediately if Licensee files for bankruptcy, becomes insolvent, or makes an assignment for the benefit of creditors. For the avoidance of any doubt, termination of the Agreement shall strictly apply to all licenses under the Agreement, its appendices, schedules, addenda and order documents and any partial termination of the Agreement by Licensee shall not be permitted in respect of any part of the Agreement, its appendices, schedules, addenda, order documents.

5.2 End of Term Duties. Upon any termination hereunder, Licensee and its Affiliates shall immediately cease Use of all SAP Materials and Confidential Information. Within thirty (30) days after any termination, Licensee shall irretrievably destroy or upon SAP's request deliver to SAP all copies of the SAP Materials and Confidential Information in every form, except to the extent it is legally required to keep it for a longer period in which case such return or destruction shall occur at the end of such period. Licensee must certify to SAP in writing that it has satisfied its obligations under this Section 5.2. Licensee agrees to certify in writing to SAP that it and each of its Affiliates has performed the foregoing. Sections 3, 4, 5.2, 6, 7.2, 8, 9, 10, 12.4, 12.5, 12.6 and 12.8 shall survive such termination. In the event of any termination hereunder, Licensee shall not be entitled to any refund of any payments made by Licensee. Termination shall not relieve Licensee from its obligation to pay fees that remain unpaid.

6. INTELLECTUAL PROPERTY RIGHTS.

6.1 Reservation of Rights. The SAP Materials, and all Intellectual Property Rights embodied in the foregoing, shall be the sole and exclusive property of SAP, SAP AG (the parent company of SAP) or its or their licensors, subject to any rights expressly granted to Licensee in Section 2 and 6.3 herein. Except for the rights set forth in Section 6.3 herein, Licensee is not permitted to modify or otherwise make derivative works of the Software. Any such unauthorized works developed by Licensee, and any Intellectual Property Rights embodied therein, shall be the sole and exclusive property of SAP or SAP AG.

6.2 Protection of Rights. Licensee shall not copy, translate, disassemble, or decompile, nor create or attempt to create the source code from the object code of the Software in any manner. Reverse engineering of the Software and other SAP Materials is prohibited. Licensee is permitted to back up data in accordance with good information technology practice and for this purpose to create the necessary backup copies of the Software. Backup copies on transportable discs or other data media must be marked as backup copies and bear the same copyright and authorship notice as the original discs or other data media. Licensee must not change or remove SAP's copyright and authorship notices.

6.3 Modifications/Add-ons.

6.3.1 Conditioned on Licensee's compliance with the terms and conditions of this Agreement, Licensee may make Modifications and/or Add-ons to the Software in furtherance of its permitted Use under this Agreement, and shall be permitted to use Modifications and Add-ons with the Software in accordance with the License grant to the Software set forth in Section 2.1.1 herein. Licensee shall comply with SAP's registration procedure prior to making Modifications or Add-ons. All Modifications and all rights associated therewith shall be the exclusive property of SAP and SAP AG. All Add-ons developed by SAP (either independently or jointly with Licensee) and all rights associated therewith shall be the exclusive property of SAP and SAP AG. Licensee agrees to execute those documents reasonably necessary to secure SAP's rights in the foregoing. All Add-ons developed by or on behalf of Licensee without SAP's participation ("Licensee Add-on"), and all rights associated therewith, shall be the exclusive property of Licensee subject to SAP's rights in and to the Software; provided, Licensee shall not commercialize, market, distribute, license, sublicense, transfer, assign or otherwise alienate any such Licensee Add-ons. SAP retains the right to independently develop its own Modifications or Add-ons to the Software, and Licensee agrees not to take any action that would limit SAP's sale, assignment, licensing or use of its own Software or Modifications or Add-ons thereto.

6.3.2 Any Modification developed by or on behalf of Licensee without SAP's participation or Licensee Add-on must not (and subject to other limitations set forth herein): enable the bypassing or circumventing any of the restrictions set forth in this Agreement and/or provide Licensee with access to the Software to which Licensee is not directly licensed; nor permit mass data extraction from

Software to any non-SAP software, including use, modification saving or other processing of data in the non-SAP software; nor unreasonably impair, degrade or reduce the performance or security of the Software; nor render or provide any information concerning SAP software license terms, Software, or any other information related to SAP products.

6.3.3 Licensee covenants, on behalf of itself and its successors and assigns, not to assert against SAP or its affiliated companies, or their resellers, distributors, suppliers, commercial partners and customers, any rights in any Modifications developed by or on behalf of Licensee without SAP participation or Licensee Add-ons , or any other functionality of the SAP Software accessed by such Modification developed by or on behalf of Licensee without SAP participation or Licensee Add-on.

7. PERFORMANCE WARRANTY.

7.1 Warranty. SAP warrants that the Software will substantially conform to the specifications contained in the Documentation for six months following delivery. The warranty shall not apply: (i) if the Software is not used in accordance with the Documentation; or (ii) if the defect is caused by a Modification or Add-on (other than a Modification or Add-on made by SAP and which is provided through SAP Support or under warranty), Licensee or third-party software. SAP does not warrant that the Software will operate uninterrupted or that it will be free from minor defects or errors that do not materially affect such performance, or that the applications contained in the Software are designed to meet all of Licensee's business requirements. Provided Licensee notifies SAP in writing with a specific description of the Software's nonconformance within the warranty period and SAP validates the existence of such nonconformance, SAP will, at its option: a) repair or replace the nonconforming Software, or b) refund the license fees paid for the applicable nonconforming Software in exchange for a return of such nonconforming Software. This is Licensee's sole and exclusive remedy under this warranty.

7.2 Express Disclaimer. SAP AND ITS LICENSORS DISCLAIM ALL OTHER WARRANTIES EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE EXCEPT TO THE EXTENT THAT ANY WARRANTIES IMPLIED BY LAW CANNOT BE VALIDLY WAIVED.

8. INDEMNIFICATION.

8.1 Infringement and Defense of Licensee. SAP shall defend Licensee against claims brought against Licensee in the Territory by any third party alleging that Licensee's Use of the Software, in accordance with the terms and conditions of this Agreement, constitutes a direct infringement or misappropriation of a patent claim(s), copyright or trade secret rights, and SAP will pay damages finally awarded against Licensee (or the amount of any settlement SAP enters into) with respect to such claims. This obligation of SAP shall not apply if the alleged infringement or misappropriation results from Use of the Software in conjunction with any other software, an apparatus other than a Designated Unit, failure to use an update promptly provided by SAP if such infringement or misappropriation could have been avoided by use of the update, or unlicensed activities. This obligation of SAP also shall not apply if Licensee fails to timely notify SAP in writing of any such claim. SAP is permitted to control fully the defense and any settlement of any such claim as long as such settlement shall not include a financial obligation on Licensee. In the event Licensee declines SAP's proffered defense, or otherwise fails to give full control of the defense to SAP's designated counsel, then Licensee waives SAP's obligations under this Section 8.1. Licensee shall cooperate fully in the defense of such claim and may appear, at its own expense, through counsel reasonably acceptable to SAP. SAP expressly reserves the right to cease such defense of any claim(s) in the event the Software is no longer alleged to infringe or misappropriate, or is held not to infringe or misappropriate, the third party's rights. SAP may settle or mitigate damages arising from any claim or potential claim, by substituting alternative substantially equivalent non-infringing programs and supporting documentation for the Software. Licensee shall not undertake any action in response to any infringement or misappropriation, or alleged infringement or misappropriation of the Software that is prejudicial to SAP's rights.

8.2 THE PROVISIONS OF THIS SECTION 8 STATE THE SOLE, EXCLUSIVE, AND ENTIRE LIABILITY OF SAP AND ITS LICENSORS TO LICENSEE, AND IS LICENSEE'S SOLE REMEDY, WITH RESPECT TO THE INFRINGEMENT OR MISAPPROPRIATION OF THIRD-PARTY INTELLECTUAL PROPERTY RIGHTS.

9. LIMITATIONS OF LIABILITY.

9.1 Not Responsible. SAP and its licensors will not be responsible under this Agreement (i) if the Software is not used in accordance with the Documentation; or (ii) if the defect or liability is caused by Licensee, a Modification or Add-on (other than a Modification or Add-on made by SAP which is provided through SAP Support or under warranty), or third-party software. SAP AND ITS LICENSORS SHALL NOT BE LIABLE FOR ANY CLAIMS OR DAMAGES ARISING FROM INHERENTLY DANGEROUS USE OF THE SOFTWARE AND/OR THIRD-PARTY SOFTWARE LICENSED HEREUNDER.

9.2 Exclusion of Damages; Limitation of Liability. ANYTHING TO THE CONTRARY HEREIN NOTWITHSTANDING, EXCEPT FOR DAMAGES RESULTING FROM UNAUTHORIZED USE OR DISCLOSURE OF CONFIDENTIAL INFORMATION OR DEATH OR PERSONAL INJURY ARISING FROM EITHER PARTY'S GROSS NEGLIGENCE OR WILLFUL MISCONDUCT, UNDER NO CIRCUMSTANCES AND REGARDLESS OF THE NATURE OF ANY CLAIM SHALL SAP, ITS LICENSORS OR LICENSEE BE LIABLE TO EACH OTHER OR ANY OTHER PERSON OR ENTITY FOR AN AMOUNT OF DAMAGES IN EXCESS OF THE PAID LICENSE FEES FOR THE SOFTWARE DIRECTLY CAUSING THE DAMAGES OR BE LIABLE IN ANY AMOUNT FOR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR INDIRECT DAMAGES, LOSS OF GOOD WILL OR BUSINESS PROFITS, WORK STOPPAGE, DATA LOSS, COMPUTER FAILURE OR MALFUNCTION, ATTORNEYS' FEES, COURT COSTS, INTEREST OR EXEMPLARY OR PUNITIVE DAMAGES. The provisions of this Agreement allocate the risks between SAP and Licensee. The license fees reflect this allocation of risk and the limitations of liability herein.

10. CONFIDENTIALITY.

10.1. Use of Confidential Information. Confidential Information shall not be reproduced in any form except as required to accomplish the intent of this Agreement. Any reproduction of any Confidential Information of the other shall remain the property of the disclosing party and shall contain any and all confidential or proprietary notices or legends which appear on the original. With respect to the Confidential Information of the other, each party : (a) shall take all Reasonable Steps (defined below) to keep all Confidential Information strictly confidential; and (b) shall not disclose any Confidential Information of the other to any person other than its bona fide individuals whose access is necessary to enable it to exercise its rights hereunder. As used herein "Reasonable Steps" means those steps the receiving party takes to protect its own similar proprietary and confidential information, which shall not be less than a reasonable standard of care. Confidential Information of either party disclosed prior to execution of this Agreement shall be subject to the protections afforded hereunder.

10.2 Exceptions. The above restrictions on the use or disclosure of the Confidential Information shall not apply to any Confidential Information that: (a) is independently developed by the receiving party without reference to the disclosing party's Confidential Information, or is lawfully received free of restriction from a third party having the right to furnish such Confidential Information; (b) has become generally available to the public without breach of this Agreement by the receiving party; (c) at the time of disclosure, was known to the receiving party free of restriction; or (d) the disclosing party agrees in writing is free of such restrictions.

10.3 Confidential Terms and Conditions; Publicity. Licensee shall not disclose the terms and conditions of this Agreement or the pricing contained therein to any third party. Neither party shall use the name of the other party in publicity, advertising, or similar activity, without the prior written consent of the other, except that Licensee agrees that SAP may use Licensee's name in customer listings or, at times mutually agreeable to the parties, as part of SAP's marketing efforts (including without limitation reference calls and stories, press testimonials, site visits, SAPPHIRE participation).

11. ASSIGNMENT. Licensee may not, without SAP's prior written consent, assign, delegate, pledge, or otherwise transfer this Agreement, or any of its rights or obligations under this Agreement, or the SAP Materials or SAP Confidential Information, to any party, whether voluntarily or by operation of law, including by way of sale of assets, merger or consolidation. SAP may assign this Agreement to any of its affiliates.

12. GENERAL PROVISIONS.

12.1 Severability. It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such invalidity or unenforceability shall not affect the other provisions of this Agreement, and this Agreement shall be construed as if such invalid or unenforceable provision had never been contained herein.

12.2 No Waiver. If either party should waive any breach of any provision of this Agreement, it shall not thereby be deemed to have waived any preceding or succeeding breach of the same or any other provision hereof.

12.3 Counterparts. This Agreement may be signed in two counterparts, each of which shall be deemed an original and which shall together constitute one Agreement.

12.4 Regulatory Matters. The Software, Documentation and SAP Materials are subject to the export control laws of various countries, including without limit the laws of the United States and Germany. Licensee agrees that it will not submit the Software, Documentation or other SAP Materials to any government agency for licensing consideration or other regulatory approval without the prior written consent of SAP, and will not export the Software, Documentation and SAP Materials to countries, persons or entities prohibited by such laws. Licensee shall also be responsible for complying with all applicable governmental regulations of the country where Licensee is registered, and any foreign countries with respect to the use of the Software, Documentation or other SAP Materials by Licensee and/or its Affiliates.

12.5 Governing Law; Limitations Period. This Agreement and any claims arising out of or relating to this Agreement and its subject matter shall be governed by and construed under the laws of Commonwealth of Pennsylvania without reference to its conflicts of law principles. In the event of any conflicts between foreign law, rules, and regulations, and United States law, rules, and regulations, United States law, rules, and regulations shall prevail and govern. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement. The Uniform Computer Information Transactions Act as enacted shall not apply. Licensee must initiate a cause of action for any claim(s) arising out of or relating to this Agreement and its subject matter within one (1) year from the date when Licensee knew, or should have known after reasonable investigation, of the facts giving rise to the claim(s).

12.6 Notices. All notices or reports which are required or may be given pursuant to this Agreement shall be in writing and shall be deemed duly given when delivered to the respective executive offices of SAP and Licensee at the addresses first set forth in any Software Order Form. Where in this section 12.6 or elsewhere in this Agreement written form is required, that requirement can be met by facsimile transmission, exchange of letters or other written form.

12.7 Force Majeure. Any delay or nonperformance of any provision of this Agreement (other than for the payment of amounts due hereunder) caused by conditions beyond the reasonable control of the performing party shall not constitute a breach of this Agreement, and the time for performance of such provision, if any, shall be deemed to be extended for a period equal to the duration of the conditions preventing performance.

12.8 Entire Agreement. This Agreement constitutes the complete and exclusive statement of the agreement between SAP and Licensee, and all previous representations, discussions, and writings are merged in, and superseded by this Agreement and the parties disclaim any reliance on any such representations, discussions and writings. This Agreement may be modified only by a writing signed by both parties. This Agreement shall prevail over any additional, conflicting, or inconsistent terms and conditions which may appear on any purchase order or other document furnished by Licensee to SAP. This Agreement shall prevail over any additional, conflicting or inconsistent terms and conditions which may appear in any clickwrap end user agreement included in the Software. Signatures sent by electronic means (facsimile or scanned and sent via e-mail) shall be deemed original signatures. This Agreement does not create any partnership, joint venture or principal and agent relationship.

12.9 Hierarchy. The following order of precedence shall be applied in the event of conflict or inconsistency between provisions of the components of this Agreement: (i) the Software Order Form; (ii) the Schedules; (iii) the Use Terms; and (iv) the GTC.

Schedule B to the GTC
"Professional Services Schedule"

The parties agree that this Schedule is hereby annexed to and made a part of the GTC. In each instance in which provisions of this Schedule contradict or are inconsistent with the provisions of the GTC, the provisions of this Schedule shall prevail and govern.

WHEREAS, Licensee licensed from SAP the right to Use SAP Software pursuant to the Agreement and SAP provides, through its employees, affiliates, and third party contractors ("Consultants"), consulting and professional services ("Services") including support of installation and implementation of the licensed Software in the United States.

1. Services. Upon request by Licensee, SAP will provide a Consultant(s) to perform, at Licensee's direction, consulting and professional services including support of installation and implementation of the applicable SAP Software ("Services"). Any Statement(s) of Work ("SOW") more fully describing the project assumptions, scope, duration and fees for the Services shall reference this Schedule. All Services of the SAP Consultant(s) will be coordinated with the designated Licensee representative. Licensee is responsible for making the necessary internal arrangements for the carrying out of the Services on a non-interference basis.

2. Satisfaction with Performance. If at any time Licensee or SAP is dissatisfied with the material performance of an assigned Consultant or a Licensee project team member, the dissatisfied party shall immediately report such dissatisfaction to the other party in writing and may request a replacement. The other party shall use its reasonable discretion in accomplishing any such change.

3. Compensation of SAP. All Services will be provided by SAP on a time and expense basis at SAP's then current rates, unless otherwise agreed by the parties in a SOW.

4. Taxes. The fees listed in the applicable SOW do not include taxes. If SAP is required to pay sales, use, property, value-added or other taxes based on the Services provided under this Schedule, then such taxes shall be billed to and paid by Licensee. This section shall not apply to taxes based on SAP's income. Licensee also agrees to pay SAP for additional tax amounts if any, created by the taxability of Consultants reimbursed travel and living expenses resulting from long term assignments at Licensee's locations.

5. Work Product. Unless otherwise agreed to in writing by the parties in a SOW, SAP shall have the sole and exclusive right, title and ownership to any and all ideas, concepts, or other intellectual property rights related in any way to the techniques, knowledge or processes of the SAP Services and deliverables, whether or not developed for Licensee.

6. Warranty. SAP warrants that its Services shall be performed consistent with generally accepted industry standards. SAP MAKES NO WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, NOR ANY OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, IN CONNECTION WITH THIS SCHEDULE AND THE SERVICES PROVIDED HEREUNDER.

7. Limitation of Liability. WITH RESPECT TO SERVICES, ANYTHING TO THE CONTRARY NOTWITHSTANDING, EXCEPT FOR DAMAGES RESULTING FROM UNAUTHORIZED USE OR DISCLOSURE OF THE PROPRIETARY INFORMATION AND SAP'S RIGHT TO COLLECT UNPAID FEES, UNDER NO CIRCUMSTANCES SHALL SAP, ITS CONSULTANTS OR LICENSEE BE LIABLE TO EACH OTHER OR ANY OTHER PERSON OR ENTITY FOR AN AMOUNT OF DAMAGES IN EXCESS OF THE FEES PAID FOR THE APPLICABLE SERVICES HEREUNDER OR BE LIABLE IN ANY AMOUNT FOR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR INDIRECT DAMAGES, LOSS OF GOOD WILL OR BUSINESS PROFITS, WORK STOPPAGE, DATA LOSS, COMPUTER FAILURE OR MALFUNCTION, OR EXEMPLARY OR PUNITIVE DAMAGES. The provisions of the Schedule allocate the risks between SAP and Licensee. The License Fees reflect this allocation of risk and the limitations of liability herein.

8. Termination. The terms of this Schedule shall be effective as of the Effective Date of the Agreement and shall remain in effect until terminated by either party upon thirty (30) days prior written notice or otherwise in accordance with a particular SOW. Licensee shall be liable for payment to SAP for all Services provided prior to the effective date of any such termination, including any expenses incurred pursuant to the provision of such Services, in accord with the applicable SOW.

9. General Provisions.
   9.1 SAP may subcontract all or part of the Services to be performed to a qualified third party.
   9.2 With respect to the Services provided by SAP under this Schedule and any SOW hereto, the relationship of SAP and Licensee is that of an independent contractor.
   9.3 This Schedule, including any applicable SOWs, constitutes the entire agreement between the parties with respect to the subject matter hereof and supersedes all prior agreements between the parties, whether written or oral, relating to the same subject matter. In the event of any inconsistencies between this Schedule and a SOW, the SOW shall take precedence over the Schedule. Any purchase order or other document issued by Licensee is for administrative convenience only.

10. Survival. Sections 5 and 7 above shall survive any termination of this Schedule.

SUBSCRIPTION SERVICE AGREEMENT

This Subscription Service Agreement (including the Subscription Service Guide, attached hereto) ("***Agreement***") is made between the ServiceNow entity ("***ServiceNow***") and the customer entity ("***Customer***") on the ordering document and becomes effective on the last signature date of the ordering document issued by ServiceNow ("***Effective Date***").

The Subscription Service Guide includes: (1) the Customer Support Policy; (2) the Upgrade Policy; (3) the Data Security Guide; and (4) any other attachment set forth or referenced in the Subscription Service Guide. The Subscription Service Guide is posted on www.servicenow.com/schedules.do and incorporated herein by reference.

Pursuant to a separate transaction between Customer and ServiceNow's authorized reseller ("***Reseller***"), Customer has purchased from Reseller certain services to be delivered by ServiceNow. This Agreement specifies the terms and conditions under which those services will be provided, apart from price, payment and other terms specified in the separate agreement between Customer and Reseller.

1. DEFINITIONS

1.1. "***Confidential Information***" means: (a) ServiceNow Core Technology (which is Confidential Information of ServiceNow); (b) Customer Data and Customer Technology (which are Confidential Information of Customer); (c) any other information of a party that is disclosed in writing or orally and is designated as *Confidential* or *Proprietary* at the time of disclosure (and, in the case of oral disclosures, summarized in writing within thirty (30) days of the initial disclosure and delivered to the receiving party), or that due to the nature of the information the receiving party would clearly understand it to be confidential information of the disclosing party; and (d) the specific terms and conditions of this Agreement, any Use Authorization, any SOW, and any amendment and attachment thereof, between the parties. Confidential Information shall not include any information that: (i) is or becomes generally known to the public through no fault or breach of this Agreement by the receiving party; (ii) was rightfully in the receiving party's possession at the time of disclosure without restriction on use or disclosure; (iii) is independently developed by the receiving party without use of the disclosing party's Confidential Information; or (iv) was or is rightfully obtained by the receiving party from a third party not under a duty of confidentiality and without restriction on use or disclosure.

1.2. "***Customer Data***" means electronic data uploaded by or for Customer and Customer's agents, employees and contractors, and processed in the Subscription Service, excluding the ServiceNow Core Technology.

1.3. "***Customer Technology***" means software, methodologies, templates, business processes, documentation or other material authored, invented or otherwise created or licensed (other than by or from ServiceNow) by Customer using or for use with the Subscription Service, excluding the ServiceNow Core Technology.

1.4. "***Development Tools***" means source code, application programming interfaces (APIs), executable software and tools in human readable format made available by ServiceNow for the implementation, customization, configuration, and use of the Subscription Service, such as scripts, code snippets, sample code, and development tools published by ServiceNow.

1.5. "***Documentation***" means the ServiceNow product documentation relating to the operation and use of the Subscription Service, Software and Development Tools, including technical program or interface documentation, user manuals, operating instructions and release notes, as updated from time to time by ServiceNow.

1.6. "***Product Overview***" means the description of the ordered products and their functionalities attached to a Use Authorization or referenced therein.

1.7. "***Professional Services***" means any services provided by ServiceNow pursuant to an agreed SOW or Service Description.

1.8. "***Service Description***" means the written description for a packaged Professional Service, attached to a Use Authorization or referenced therein.

1.9. "***ServiceNow Core Technology***" means: (a) the Subscription Service; Software; Development Tools, Documentation; and ServiceNow technology and methodologies (including, without limitation, products, software tools, hardware designs, algorithms, templates, software (in source and object forms), architecture, class libraries, objects and documentation) existing as of the Effective Date or otherwise arising outside of work under a Professional Service; (b) updates, upgrades, improvements, configurations, extensions, and derivative works of the foregoing and related technical or end user documentation or manuals; and (c) intellectual property anywhere in the world relating to the foregoing.

1.10. "***Software***" means software provided by ServiceNow to Customer that operates on Customer-provided machines solely to facilitate the use of the Subscription Service.

1.11. "***SOW***" means a statement of work for Professional Services.

1.12. "***Subscription Service***" means the ServiceNow software as a service (SaaS) offering identified in a Use Authorization.

1.13. "***Subscription Term***" means the term of authorized use of the Subscription Service as set forth in the Use Authorization.

1.14. "***Use Authorization***" means a written document provided to Customer specifying the services that Customer has purchased, along with the term and scope of the authorized use thereof.

2. GRANT OF USE RIGHTS

2.1. SUBSCRIPTION SERVICE. Subject to the terms of this Agreement, ServiceNow authorizes Customer to access and use the purchased Subscription Service during the Subscription Term as set forth in an applicable Use Authorization for its internal business purposes in accordance with the Documentation. Customer shall not use or otherwise access the Subscription Service in a manner that exceeds Customer's authorized use as set forth in this Agreement and the applicable Use Authorization.

2.2. SOFTWARE. ServiceNow grants Customer a limited, personal, worldwide, non-sublicensable, non-transferable (except as set forth in Section 10.1 (Assignment)), non-exclusive license during the Subscription Term to install and execute Software on machines operated by or for Customer solely to facilitate Customer's authorized access to and use of the purchased Subscription Service. The Software may include code that is licensed under third party license agreements, including open source made available or provided with the Software. Software is licensed and not sold even if for convenience ServiceNow makes reference to words such as *sale* or *purchase*.

2.3. DEVELOPMENT TOOLS. In support of Customer's authorized internal business use of the Subscription Service during the Subscription Term, ServiceNow grants to Customer a limited, personal, worldwide, non-sublicensable, non-transferable (except as set forth in Section 10.1 (Assignment)), non-exclusive license to download and make a reasonable number of copies of the Development Tools, and to use, copy, modify and create derivative works of the Development Tools, in: (a) using, implementing and integrating the ServiceNow applications with other software and systems; and (b) creating applications on the ServiceNow platform (to the extent Customer has purchased authorized use of the Subscription Service to create applications on the ServiceNow platform). Customer shall not use the Development Tools in a manner that causes it to exceed the limits of its authorized use of the Subscription Service as set forth in this Agreement and the Use Authorization. From time to time, ServiceNow may provide Development Tools subject to the terms and conditions of separate agreements which will be provided to Customer for review and to which Customer will be required to agree prior to use of such Development Tools; provided that ServiceNow shall not require Customer to agree to separate terms and conditions for any Development Tool that is necessary for Customer's use of its ordered Subscription Service in conformance with the Product Overview unless set forth on the Use Authorization.

2.4. RESTRICTIONS. Customer shall not (and shall not permit others to) do the following with respect to the ServiceNow Core Technology: (i) use the Subscription Service with external programs in a manner that intentionally circumvents contractual usage restrictions; (ii) license, sub-license, sell, re-sell, rent, lease, transfer, distribute or time share or otherwise make any of it available for access by third parties except as otherwise expressly provided in a Use Authorization; (iii) access it for the purpose of developing or operating products or services intended to be offered to third parties in competition with the Subscription Service; (iv) disassemble, reverse engineer or decompile it; (v) copy, create derivative works based on or otherwise modify it except as permitted in this Agreement; (vi) remove or modify a copyright or other proprietary rights notice in it; (vii) use it to reproduce, distribute, display, transmit or use material protected by copyright or other intellectual property right (including the rights of publicity or privacy) without first obtaining the permission of the owner; (viii) use it to create, use, send, store or run viruses or other harmful computer code, files, scripts, agents or other programs or otherwise engage in a malicious act or disrupt its security, integrity or operation; or (ix) access or disable any ServiceNow or third party data, software or network (other than Customer's instance of the Subscription Service in accordance with this Agreement). Before Customer exercises any of the foregoing actions that Customer believes it is entitled to, Customer shall provide ServiceNow with thirty (30) days' prior written notice to legalnotices@servicenow.com (or, if applicable law or the relevant court order does not allow for such notice, then the maximum amount of notice allowable), and provide reasonably requested information to allow ServiceNow to assess Customer's claim and, at ServiceNow's sole discretion, provide alternatives that reduce adverse impacts on ServiceNow's intellectual property and other rights.

3. ORDERING

3.1. RESELLER ORDERS. Customer shall order and purchase the Subscription Service and Professional Services directly from Reseller pursuant to a separate agreement specifying price, payment and other commercial terms. ServiceNow is not a party to such separate agreement but will provide the purchased services pursuant to this Agreement. For each order, Reseller or ServiceNow will provide Customer with a Use Authorization for Customer to sign and return to ServiceNow. ServiceNow will have no obligation to provide services unless and until it has received a Use Authorization signed by Customer. Reseller is not authorized to make any changes to this Agreement (including any Use Authorizations issued hereunder) or bind ServiceNow to any additional or different terms or conditions. Additional orders for ServiceNow products or services may be placed either through Reseller or ServiceNow, provided that if Customer places an order directly through ServiceNow, Customer shall sign an addendum to this Agreement setting forth pricing, payment and other commercial terms between Customer and ServiceNow.

3.2. USE VERIFICATION. ServiceNow or Reseller may remotely review Customer's use of the Subscription Service, and upon ServiceNow or Reseller's written request Customer shall provide any reasonable assistance, to verify Customer's compliance with the Agreement. If ServiceNow determines that Customer has exceeded its permitted use of the Subscription Service then ServiceNow will notify Customer and within thirty (30) days thereafter Customer shall either: (i) disable any unpermitted use or (ii) purchase additional subscriptions commensurate with Customer's actual use. If Customer fails to regain compliance within such thirty (30) day period or fails to make payment as provided in its agreement with Reseller, ServiceNow may suspend Customer's use of the Subscription Service or terminate this Agreement for cause in accordance with Section 9 (Term and Termination), in addition to any other rights or remedies ServiceNow may have.

4. INTELLECTUAL PROPERTY

4.1. SERVICENOW OWNERSHIP. As between ServiceNow and Customer, all rights, title, and interest in and to all intellectual property rights in the ServiceNow Core Technology are owned exclusively by ServiceNow notwithstanding any other provision in this Agreement. Except as expressly provided in this Agreement, ServiceNow reserves all rights in the ServiceNow Core Technology and does not grant Customer any rights, express or implied or by estoppel.

4.2. CUSTOMER OWNERSHIP. As between Customer and ServiceNow, Customer shall retain all of its rights, title, and interest in and to its intellectual property rights in Customer Data and Customer Technology. Customer hereby grants to ServiceNow a royalty-free, fully-paid, non-exclusive, non-transferable (except as set

forth in Section 10.1 (Assignment)), sub-licensable, worldwide right to use Customer Data and Customer Technology solely for the purpose of providing the Subscription Service and Professional Services to Customer.

4.3. FEEDBACK. ServiceNow encourages Customer to provide suggestions, proposals, ideas, recommendations or other feedback regarding improvements to ServiceNow's services and related resources. To the extent Customer provides such feedback, Customer grants to ServiceNow a royalty-free, fully paid, sub-licensable, transferable (notwithstanding Section 10.1 (Assignment)), non-exclusive, irrevocable, perpetual, worldwide right and license to make, use, sell, offer for sale, import and otherwise exploit feedback (including by incorporation of such feedback into the ServiceNow Core Technology) without restriction.

4.4. PROFESSIONAL SERVICES. Subject to the provisions of this Section 4.4, ServiceNow shall assign to Customer any Newly Created IP (as defined below) in Deliverables upon payment in full by Customer of all amounts due for the Professional Service under which the Deliverable was created. A "***Deliverable***" is a deliverable that is identified in the applicable SOW or Service Description and that is created by ServiceNow for Customer in the performance of the Professional Services. "***Newly Created IP***" means intellectual property in any inventions or works of authorship that are made by ServiceNow specifically for Customer in the course of performing Professional Services for Customer that is identified as "Newly Created IP" in an SOW, excluding the ServiceNow Core Technology. To the extent (if at all) any ServiceNow Core Technology is incorporated into a Deliverable, ServiceNow grants to Customer a non-exclusive, royalty-free, non-transferable, non-sublicensable worldwide license to use the ServiceNow Core Technology solely to use the Deliverable in connection with the Subscription Service as contemplated under this Agreement during the Subscription Term. Nothing in this Agreement shall be deemed to restrict or limit ServiceNow's right to perform similar Professional Services for any other party or to assign any employees or subcontractors to perform similar Professional Services for any other party or to use any information incidentally retained in the unaided memories of its employees providing Professional Services.

5. WARRANTIES

5.1. LIMITED SUBSCRIPTION SERVICE WARRANTY. ServiceNow warrants that during the Subscription Term Customer's production instances of the Subscription Service shall materially conform to the Product Overview. To submit a warranty claim under this Section, Customer shall (1) reference this Section; and (2) submit a support request to resolve the non-conformity as provided in the Subscription Service Guide. If the non-conformity persists without relief more than thirty (30) days after written notice of a warranty claim provided to ServiceNow under this Section 5.1, then Customer may terminate the affected Subscription Service and submit to Reseller a claim for refund of any prepaid subscription fees covering the remainder of the Subscription Term of the affected Subscription Service after the date of termination. Notwithstanding the foregoing, this warranty shall not apply to any non-conformity due to a modification of or defect in the Subscription Service that is made or caused by any person other than ServiceNow or a person acting at ServiceNow's direction. THIS SECTION 5.1 SETS FORTH CUSTOMER'S EXCLUSIVE RIGHTS AND REMEDIES (AND SERVICENOW'S SOLE LIABILITY) IN CONNECTION WITH THIS WARRANTY.

5.2. LIMITED PROFESSIONAL SERVICES WARRANTY. ServiceNow warrants that the Professional Services will be performed in a competent and workmanlike manner in accordance with accepted industry standards and practices and all material requirements set forth in the SOW or Service Description. Customer shall notify ServiceNow in writing of any breach within thirty (30) days after performance of the non-conforming Professional Services. Upon receipt of such notice, ServiceNow, at its option, shall either use commercially reasonable efforts to re-perform the Professional Services in conformance with these warranty requirements or shall terminate the affected Professional Services, in which case Customer may submit to Reseller a claim for a refund of any amounts paid for the nonconforming Professional Services. THIS SECTION 5.2 SETS FORTH CUSTOMER'S EXCLUSIVE RIGHTS AND REMEDIES (AND SERVICENOW'S SOLE LIABILITY) IN CONNECTION WITH THIS WARRANTY.

5.3. DISCLAIMER OF WARRANTIES. EXCEPT FOR THE WARRANTIES EXPRESSLY STATED IN THIS AGREEMENT, TO THE MAXIMUM EXTENT ALLOWED BY LAW, SERVICENOW DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING WARRANTIES

ARISING UNDER STATUTE, WARRANTIES OF MERCHANTABILITY, ACCURACY, TITLE, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE OR ANY WARRANTIES ARISING FROM USAGE OF TRADE, COURSE OF DEALING OR COURSE OF PERFORMANCE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, SERVICENOW SPECIFICALLY DOES NOT WARRANT THAT THE SUBSCRIPTION SERVICE, SOFTWARE, PROFESSIONAL SERVICES, DEVELOPMENT TOOLS, DOCUMENTATION OR DELIVERABLES WILL MEET THE REQUIREMENTS OF CUSTOMER OR OTHERS OR THAT THEY WILL BE ACCURATE OR OPERATE WITHOUT INTERRUPTION OR ERROR. CUSTOMER ACKNOWLEDGES THAT IN ENTERING THIS AGREEMENT IT HAS NOT RELIED ON ANY PROMISE, WARRANTY OR REPRESENTATION NOT EXPRESSLY SET FORTH HEREIN.

6. CONFIDENTIAL INFORMATION

6.1. CONFIDENTIALITY OBLIGATIONS. The recipient of Confidential Information shall: (i) at all times protect it from unauthorized disclosure with the same degree of care that it uses to protect its own confidential information, and in no event using less than reasonable care; and (ii) not use it except to the extent necessary to exercise rights or fulfill obligations under this Agreement. Each party shall limit the disclosure of the other party's Confidential Information to those of its employees and contractors with a need to access such Confidential Information for a party's exercise of its rights and obligations under this Agreement, provided that all such employees and contractors are subject to binding disclosure and use restrictions at least as protective as those set forth herein. Each party's obligations set forth in this Section 6 shall remain in effect during the term and three (3) years after termination of this Agreement. The receiving party shall, at the disclosing party's request or upon termination of this Agreement, return all originals, copies, reproductions and summaries of Confidential Information and other tangible materials and devices provided to the receiving party as Confidential Information, or at the disclosing party's option, certify destruction of the same. Provisions for the return of Customer Data are set forth in Section 9.3 (Return of Customer Data).

6.2. REQUIRED DISCLOSURES. A party may disclose the disclosing party's Confidential Information to a court or governmental body pursuant to a valid court order, law, subpoena or regulation, provided that the receiving party: (a) promptly notifies the disclosing party of such requirement as far in advance as possible to the extent advanced notice is lawful; and (b) provides reasonable assistance to the disclosing party in any lawful efforts by the disclosing party to resist or limit the disclosure of such Confidential Information.

6.3. EQUITABLE REMEDIES. The parties agree that the receiving party's disclosure of Confidential Information except as provided herein may result in irreparable injury for which a remedy in money damages may be inadequate. The parties further agree that in the event of such disclosure or threatened disclosure, the disclosing party may be entitled to seek an injunction to prevent the breach or threatened breach without the necessity of proving irreparable injury or the inadequacy of money damages, in addition to remedies otherwise available to the disclosing party at law or in equity.

7. INDEMNIFICATION

7.1. SERVICENOW OBLIGATION. Subject to the exclusions set forth below, ServiceNow shall: (i) defend Customer, its officers, directors and employees against any third party suit, claim, action or demand (each a "***Claim***") to the extent alleging: (A) that the Subscription Service used in accordance with this Agreement infringes any third party patent, copyright or trademark, or misappropriates any third party trade secret; or (B) that ServiceNow's personnel when onsite at Customer's premises caused death, bodily harm or damage to tangible personal property due to their negligence or willful misconduct; and (ii) pay any court-ordered award of damages or settlement amount to the extent arising from any such Claims. If any portion of the Subscription Service becomes the subject of a Claim under Section 7.1(i)(A), ServiceNow may: (a) contest the Claim; (b) obtain permission from the claimant for Customer's continued use of the Subscription Service; (c) replace or modify the Subscription Service to avoid infringement, if such replacement or modification has substantially the same capabilities as the Subscription Service; or, if the foregoing (a), (b), and (c) are not available on commercially reasonable terms in ServiceNow's judgment, then (d) terminate Customer's use of the affected Subscription Service upon sixty (60) days' written notice, whereupon Customer may submit to Reseller a claim for a refund of any prepaid subscription fees covering the remaining portion of the applicable Subscription Term for the affected

Subscription Service after the date of termination. Notwithstanding the above, ServiceNow shall have no obligation or liability for any Claim under Section 7.1(i)(A) arising in whole or in part from: (1) any use of the Subscription Service which exceeds the authorized use permitted under this Agreement or not in accordance with the Documentation; (2) Customer Data or Customer Technology; (3) use of the Subscription Service by Customer in violation of applicable law; (4) use of the affected Subscription Service after termination in accordance with clause (d) of this Section 7.1; (5) modifications to the Subscription Service made to Customer's specifications or otherwise made by any person other than ServiceNow or a person acting at ServiceNow's direction if the Claim would have been avoided by use of the unmodified Subscription Service; or (6) use of the Subscription Service in combination with any hardware, software, application or service that was not provided by ServiceNow, if the Claim would have been avoided by the non-combined or independent use of the Subscription Service.

7.2. CUSTOMER OBLIGATION. Customer shall: (i) defend ServiceNow, its officers, directors and employees against any Claim alleging that: (A) Customer Data, (B) Customer Technology or (C) a modification to the Subscription Service made to Customer's specifications or otherwise made by or on behalf of Customer by any person other than ServiceNow or a person acting at ServiceNow's direction (but only if the Claim would have been avoided by use of the unmodified Subscription Service), infringes any patent, copyright or trademark, misappropriates any third party trade secret, or violates any third party privacy rights; and (ii) pay any court-ordered award of damages or settlement amount to the extent arising from such Claim.

7.3. PROCESS. All of the foregoing indemnity obligations of ServiceNow and Customer are conditioned on the indemnified party notifying the indemnifying party promptly in writing of any actual or threatened Claim, the indemnified party giving the indemnifying party sole control of the defense thereof and any related settlement negotiations, and the indemnified party cooperating and, at the indemnifying party's request and expense, assisting in such defense. SECTION 7 STATES EACH PARTY'S ENTIRE LIABILITY AND THE OTHER PARTY'S EXCLUSIVE REMEDY FOR THIRD PARTY CLAIMS AND ACTIONS.

8. LIMITATIONS OF LIABILITY

8.1. LIMITATIONS OF LIABILITY. SERVICENOW SHALL HAVE NO LIABILITY FOR ANY REFUND THAT, IN ACCORDANCE WITH THE TERMS OF THIS AGREEMENT, IS TO BE PAID BY RESELLER. TO THE EXTENT PERMITTED BY LAW, THE TOTAL, CUMULATIVE LIABILITY OF EACH PARTY ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE PRODUCTS OR SERVICES PROVIDED HEREUNDER WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR ANY OTHER LEGAL OR EQUITABLE THEORY, SHALL BE LIMITED TO THE AMOUNTS PAID BY CUSTOMER FOR THE PRODUCTS OR SERVICES GIVING RISE TO THE CLAIM DURING THE TWELVE (12) MONTH PERIOD PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY. THE EXISTENCE OF MORE THAN ONE CLAIM SHALL NOT ENLARGE THIS LIMIT. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO: (1) CUSTOMER'S OBLIGATION TO PAY FOR PRODUCTS, SERVICES OR TAXES; (2) A PARTY'S OBLIGATIONS IN SECTION 7 (INDEMNIFICATION); AND (3) INFRINGEMENT BY A PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS.

8.2. EXCLUSION OF DAMAGES. TO THE EXTENT PERMITTED BY LAW, NEITHER SERVICENOW NOR CUSTOMER SHALL BE LIABLE TO THE OTHER OR ANY THIRD PARTY FOR LOST PROFITS (WHETHER DIRECT OR INDIRECT) OR LOSS OF USE OR DATA, COVER, SUBSTITUTE GOODS OR SERVICES, OR FOR INCIDENTAL, CONSEQUENTIAL, PUNITIVE, SPECIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGE TO BUSINESS, REPUTATION OR GOODWILL), OR INDIRECT DAMAGES OF ANY TYPE HOWEVER CAUSED, WHETHER BY BREACH OF WARRANTY, BREACH OF CONTRACT, IN TORT (INCLUDING NEGLIGENCE) OR ANY OTHER LEGAL OR EQUITABLE CAUSE OF ACTION EVEN IF SUCH PARTY HAS BEEN ADVISED OF SUCH DAMAGES IN ADVANCE OR IF SUCH DAMAGES WERE FORESEEABLE. THE FOREGOING EXCLUSIONS SHALL NOT APPLY TO: (1) PAYMENTS TO A THIRD PARTY ARISING FROM A PARTY'S OBLIGATIONS UNDER SECTION 7 (INDEMNIFICATION); AND (2) INFRINGEMENT BY A PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS.

8.3. GROSS NEGLIGENCE; WILFUL MISCONDUCT. AS PROVIDED BY LAW, NOTHING HEREIN SHALL BE INTENDED TO LIMIT A PARTY'S LIABILITY IN AN ACTION IN TORT (SEPARATE AND DISTINCT

FROM A CAUSE OF ACTION FOR BREACH OF THIS AGREEMENT) FOR THE PARTY'S GROSS NEGLIGENCE OR WILFUL MISCONDUCT.

9. TERM AND TERMINATION

9.1. TERM AND TERMINATION. This Agreement continues until terminated under the terms of this Agreement. Each party may terminate this Agreement in its entirety either: (i) upon thirty (30) days' prior written notice to the other party, if at the time of notice there are no Use Authorizations in effect; or (ii) upon written notice if the other party becomes the subject of a petition in bankruptcy or any proceeding related to its insolvency, receivership or liquidation, in any jurisdiction, that is not dismissed within sixty (60) days of its commencement or an assignment for the benefit of creditors. Either party may terminate a Subscription Service or Professional Services upon written notice if the other party materially breaches this Agreement or the applicable Use Authorization for the affected service and does not cure the breach within thirty (30) days after receiving written notice thereof from the non-breaching party. Professional Services are separately ordered from the Subscription Service, and are not required for the Subscription Service. A breach by a party of its obligations with respect to Professional Services shall not by itself constitute a breach by that party of its obligations with respect to the Subscription Service even if the services are enumerated in the same Use Authorization.

9.2. EFFECT OF TERMINATION OF SUBSCRIPTION SERVICE. Upon termination of the Subscription Service for any reason, Customer shall stop using, and ServiceNow shall stop providing, the Subscription Service and all rights granted to Customer in this Agreement shall terminate. If the Subscription Service is terminated by Customer due to ServiceNow's breach, then Customer may submit to Reseller a claim for refund of all prepaid fees for the remaining portion of the Subscription Term for the terminated Subscription Service after the effective date of termination. Within thirty (30) days following the effective date of a termination by ServiceNow for Customer's breach, Customer shall pay all remaining amounts for the Subscription Term applicable to the Subscription Service covering the remainder of the Subscription Term regardless of the due dates specified in Reseller's order form to Customer.

9.3. TRANSITION SERVICES. At least thirty (30) days prior to either the expiration of the Subscription Term (where Customer elects not to renew) or in connection with the termination by Customer of the Subscription Service in accordance with Section 9.1, provided that Customer signs an addendum to this Agreement setting forth payment and other commercial terms between Customer and ServiceNow, Customer may purchase the following services from ServiceNow: (i) one (1) extension of the Subscription Service for up to six (6) months ("***Transition Subscription Service***"); and (ii) Professional Services. Prior to the commencement of any Transition Subscription Service or Professional Services, Customer shall sign an ordering document and shall pay in advance for the Transition Subscription Service and any Professional Services plus verifiable travel and expenses.

9.4. RETURN OF CUSTOMER DATA. ServiceNow shall provide Customer Data in its standard database export format, excluding the ServiceNow Core Technology, to Customer upon Customer's written request and at no additional cost to Customer, provided that ServiceNow receives such request from Customer within forty-five (45) days following the expiration or termination of this Agreement for the Subscription Service (including any Transition Subscription Service term, if applicable).If ServiceNow has not received a request within the foregoing time frame, ServiceNow shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, have the right to delete all Customer Data in its systems or otherwise in its possession or under its control and delete Customer's instances of the Subscription Service.

9.5. SURVIVAL. Sections 2.4 (Restrictions), 4.1 (ServiceNow Ownership), 4.2 (Customer Ownership), 4.3 (Feedback) and 6 (Confidential Information) through 10 (General Provisions) of this Agreement, together with any other provision required for their construction or enforcement, shall survive termination of this Agreement for any reason.

10. GENERAL PROVISIONS

10.1. ASSIGNMENT. Neither party may assign its rights or obligations under this Agreement, whether by operation of law or otherwise, without the prior written consent of the other party. Notwithstanding the

foregoing, either party may, upon notice and without the other party's consent: (i) in connection with a merger, reorganization or sale of all or substantially all of the assets or equity of such party, assign this Agreement in its entirety to such party's successor; and (ii) assign this Agreement in its entirety to any Affiliate. "***Affiliates***" shall mean any person or entity directly or indirectly Controlling, Controlled by or under common Control with a party to the Agreement, where "***Control***" means the legal power to direct or cause the direction of the general management of the company, partnership or other legal entity. Any attempted or purported assignment in violation of this Section 10.1 will be null and void. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

10.2. COMPLIANCE WITH LAWS. ServiceNow shall comply with any statutes and regulations that apply to its provision of the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables, under the Agreement, including but not limited to those applicable to the privacy and security of personal information, including trans-border data transfers and data breach notification requirements as required of ServiceNow by law. Customer shall comply with all laws that apply to its use of the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables, under the Agreement, including but not limited to those applicable to collection and processing of Customer Data in ServiceNow systems through the Subscription Service. Customer agrees to provide any required disclosures to and obtain any required consents for the transfer of Customer Data to ServiceNow. ServiceNow shall not be responsible for compliance with any laws applicable to Customer and its industry that are not generally applicable to information technology service providers.

10.3. EXPORT COMPLIANCE. Each party shall comply with United States and foreign export control laws and regulations. Customer acknowledges that the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables are subject to the U.S. Export Administration Regulations (the "***EAR***") and that Customer shall comply with the EAR. Without limiting the foregoing, Customer represents and warrants that: (i) Customer is not located in, and shall not use the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables from, any country that is subject to U.S. export restrictions (currently including, but not necessarily limited to, Cuba, Iran, North Korea, Sudan and Syria); (ii) Customer shall not use the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables in the design, development or production of nuclear, chemical or biological weapons, or rocket systems, space launch vehicles, sounding rockets or unmanned air vehicle systems; and (iii) Customer is not prohibited from participating in U.S. export transactions by any federal agency of the U.S. government. In addition, Customer is responsible for complying with any local laws which may impact Customer's right to import, export or use the Subscription Service, Professional Services, Software, Documentation, Development Tools and Deliverables.

10.4. US GOVERNMENT RIGHTS. All ServiceNow software (including Software) is commercial computer software and all services are commercial items. "***Commercial computer software***" has the meaning set forth in Federal Acquisition Regulation ("***FAR***") 2.101 for civilian agency purchases and the Department of Defense ("***DOD***") FAR Supplement ("***DFARS***") 252.227-7014(a)(1) for defense agency purchases. If the software is licensed or the services are acquired by or on behalf of a civilian agency, ServiceNow provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of this Agreement as required in FAR 12.212 (Computer Software) and FAR 12.211 (Technical Data) and their successors. If the software is licensed or the services are acquired by or on behalf of any agency within the DOD, ServiceNow provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of this Agreement as specified in DFARS 227.7202-3 and its successors. Only if this is a DOD prime contract or DOD subcontract, the Government acquires additional rights in technical data as set forth in DFARS 252.227-7015. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFARS or other clause or provision that addresses Government rights in computer software or technical data.

10.5. NOTICE. Except as otherwise provided herein, all notices shall be in writing and deemed given upon: (i) personal delivery; (ii) when received by the addressee if sent by a recognized overnight courier (receipt requested); (iii) the second business day after mailing; or (iv) the first business day after sending by email with

confirmation of receipt, except that email shall not be sufficient for notices regarding a Claim. Notices shall be sent to the parties as set forth on the signature page of this Agreement or as subsequently updated in writing.

10.6. FORCE MAJEURE. No party shall be liable or responsible to the other party, nor be deemed to have defaulted under or breached this Agreement, for any failure or delay in fulfilling or performing any term of this Agreement (excluding Customer's failure to pay amounts owed when due), when and to the extent such failure or delay is caused by or results from acts beyond the affected party's reasonable control, including without limitation: strikes, lock-outs or other industrial disputes (whether involving its own workforce or a third party's), trespassing, sabotage, theft or other criminal acts, failure of energy sources or transport network, acts of God, export bans, sanctions and other government actions, war, terrorism, riot, civil commotion, interference by civil or military authorities, national or international calamity, armed conflict, malicious damage, breakdown of plant or machinery, nuclear, chemical or biological contamination, explosions, collapse of building structures, fires, floods, storms, earthquakes, epidemics or similar events, natural disasters or extreme adverse weather conditions (each a "***Force Majeure Event***"). The party suffering a Force Majeure Event shall use reasonable efforts to mitigate against the effects of such Force Majeure Event.

10.7. HIGH RISK ACTIVITIES. Customer shall use the ServiceNow Core Technology within the intended business purposes described in the Documentation, and not for any purpose that requires fail-safe performance including, but not limited to, stock trading, financial transaction processing, management of hazardous facilities or applications for which failure could result in death, personal injury, or severe physical or environmental damage ("***High Risk Activity***"). ServiceNow, its licensors and suppliers expressly disclaim all warranties of fitness for any such use and Customer shall release and hold ServiceNow, its licensors and suppliers harmless from liability arising out of the use of the ServiceNow Core Technology for High Risk Activity.

10.8. USE OF AGGREGATE DATA. Customer agrees that ServiceNow may collect, use and disclose quantitative data derived from the use of the Subscription Service for industry analysis, benchmarking, analytics, marketing, and other business purposes. All data collected, used, and disclosed will be in aggregate form only and will not identify Customer or its users.

10.9. ENTIRETY. This Agreement, together with the Use Authorizations, Product Overviews, SOWs, Service Descriptions, and the Subscription Service Guide (including the Customer Support Policy, the Upgrade Policy and the Data Security Guide), is the final and entire agreement between the parties regarding the products and services provided hereunder and supersedes all prior or contemporaneous oral or written agreements, representations, understandings, undertakings and negotiations with respect to the subject matter hereof. The terms of this Agreement apply to the exclusion of any other terms that Customer seeks to impose or incorporate, or which are implied by trade, custom, practice or course of dealing. Customer acknowledges that it has not relied on any statement, promise or representation made or given by or on behalf of ServiceNow that is not set out in this Agreement. Customer's orders are not contingent on, and Customer has not relied on, the delivery of any future functionality regardless of any verbal or written communication about ServiceNow's future plans. This Agreement may be executed in counterparts, each of which shall be deemed to be an original.

10.10. WAIVER AND AMENDMENT. A waiver of any right is only effective if it is in writing and only against the party who signed such writing and for the circumstances given. Any modification of this Agreement must be in writing and signed by authorized representatives of both parties.

10.11. RELATIONSHIP OF THE PARTIES. The parties are independent contractors. Nothing in this Agreement shall be construed to create a partnership, joint venture or agency relationship. Neither party shall have any right or authority to assume or create any obligation of any kind expressed or implied in the name of or on behalf of the other party.

10.12. GOVERNING LAW; JURISDICTION AND VENUE. This Agreement shall be governed by the laws of the state of California, without regard to its conflict of laws principles. The parties hereby irrevocably consent to the exclusive jurisdiction of, and venue in, any federal or state court of competent jurisdiction located in Santa Clara County, California, for the purposes of adjudicating any dispute arising out of this Agreement. Each party hereto expressly consents to service of process by registered mail. To the extent permitted by law, choice of law rules and the United Nations Convention on Contracts for the International Sale of Goods shall not apply.

Notwithstanding the foregoing, either party may at any time seek and obtain appropriate legal or equitable relief in any court of competent jurisdiction for claims regarding such party's intellectual property rights.

10.13. CONSTRUCTION. Products and services shall be provided in the English language unless agreed otherwise. The parties confirm that they have requested that this Agreement and all related documents be drafted in English at the express wishes of the parties. Les parties confirment avoir expressément exigé que le présent contrat et les documents de ServiceNow qui y sont attachés soient rédigés en anglais. Section headings are for convenience only and are not to be used in interpreting this Agreement.

SUBSCRIPTION SERVICE GUIDE

Capitalized terms not defined herein shall have the meaning set forth in the ordering agreement or the use agreement between Customer and ServiceNow.

1. SUPPORT

During the Subscription Term, ServiceNow or its authorized reseller, as applicable, shall provide support for the Subscription Service as set forth in the ***Customer Support Policy*** attached hereto, and incorporated herein by reference.

2. UPGRADES

ServiceNow determines whether and when to develop, release and apply any Upgrade (as defined in the ***Upgrade Policy*** attached hereto, and incorporated herein by reference) to Customer's instances of the Subscription Service.

3. DATA SECURITY

ServiceNow shall implement and maintain security procedures and practices appropriate to information technology service providers to protect Customer Data from unauthorized access, destruction, use, modification, or disclosure, as described in the ***Data Security Guide*** attached hereto, and incorporated herein by reference.

4. INSURANCE

ServiceNow agrees to maintain in effect during the Subscription Term, at ServiceNow's expense, the following minimum insurance coverage:

(i) (a) Workers' Compensation Insurance, in accordance with applicable statutory, federal, and other legal requirements and (b) Employers' Liability Insurance covering ServiceNow's employees in an amount of not less than $1,000,000 for bodily injury by accident, $1,000,000 policy limit for bodily injury by disease, and $1,000,000 each employee for bodily injury by disease;

(ii) Commercial General Liability Insurance written on an occurrence form and including coverage for bodily injury, property damage, products and completed operations, personal injury, advertising injury arising out of the services and/or products provided by ServiceNow under this Agreement with minimum limits of $1,000,000 per occurrence/$2,000,000 aggregate;

(iii) Commercial Automobile Liability Insurance providing coverage for hired and non-owned automobiles used in connection with this Agreement in an amount of not less than $1,000,000 per accident combined single limit for bodily injury and property damage;

(iv) Combined Technology Errors' & Omission Policy with a $5,000,000 per Claim limit, including: (a) Professional Liability Insurance providing coverage for the services and software in this Agreement. Such coverage to be maintained for at least two (2) years after the termination of this Agreement; and (b) Privacy, Security, and Media Liability Insurance providing liability coverage for unauthorized access or disclosure, security breaches or system attacks, as well as infringements of copyright and trademark that might result from this Agreement; and

(v) Excess Liability over Employers' Liability, Commercial General Liability and Commercial Automobile Liability with a $5,000,000 aggregate limit.

For the purpose of this Section, a "***Claim***" means a written demand for money or a civil proceeding which is commenced by service of a complaint or similar pleading.

5. AVAILABILITY SERVICE LEVEL

5.1. DEFINITIONS

(a) "***Available***" means that the Subscription Service can be accessed by authorized users.

(b) "***Excused Downtime***" means: (i) Maintenance Time of up to two (2) hours per month; and (ii) any time the Subscription Service is not Available due to circumstances beyond ServiceNow's control, including without limitation modifications of the Subscription Service by any person other than ServiceNow or a person acting at ServiceNow's direction, a Force Majeure Event, general Internet outages, failure of Customer's infrastructure or connectivity (including without limitation, direct connectivity and virtual private network (VPN) connectivity to the Subscription Service), computer and telecommunications failures and delays, and network intrusions or denial-of-service or other criminal attacks.

(c) "***Maintenance Time***" means the time the Subscription Service is not Available due to service maintenance.

(d) "***Availability SLA***" means the percentage of total time during which Customer's production instances of the Subscription Service are Available during a calendar month, excluding Excused Downtime.

5.2. AVAILABLITY

If Customer's production instances of the Subscription Service fall below the Availability SLA of ninety-nine and eight-tenths percent (99.8%) during a calendar month, Customer's exclusive remedy for failure of the Subscription Service to meet the Availability SLAs is either: (1) to request that the affected Subscription Term be extended for the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA; or (2) to request that ServiceNow issue a service credit to Customer for the dollar value of the number of minutes the Subscription Service was not Available in the month in accordance with the Availability SLA (determined at the deemed per minute rate ServiceNow charges to Customer for Customer's use of the affected Subscription Service), which Customer may request ServiceNow apply to the next invoice for subscription fees.

5.3. REQUESTS

Customer must request all service credits or extensions in writing to ServiceNow within thirty (30) days of the end of the month in which the Availability SLA was not met, identifying the support requests relating to the period Customer's production instances of the Subscription Service was not Available. The total amount of service credits for any month may not exceed the subscription fee for the affected Subscription Service for the month, and has no cash value. ServiceNow may delay issuing service credits until such amounts reach one thousand U.S. dollars ($1,000) or equivalent currency specified in the applicable Order Form.

CUSTOMER SUPPORT POLICY

This Customer Support Policy governs the support that ServiceNow or its authorized reseller, as applicable, will provide for the Subscription Service. This Policy may be updated from time to time.

Scope

The purpose of Customer Support is to resolve defects that cause the Subscription Service to perform not in substantial conformance to the Product Overview. A resolution to a defect may consist of a fix, workaround or other relief ServiceNow deems reasonable.

Customer Support does not include:

- implementation services
- configuration services
- integration services
- customization services or other custom software development
- training
- assistance with administrative functions

Customer Support is not required to provide resolutions for immaterial defects or defects due to modifications of the Subscription Service made by any person other than ServiceNow or a person acting at ServiceNow's direction.

Business Hours

Customer Support is available 24 hours a day, 7 days a week, including all holidays.

Access Contacts

Customer may contact ServiceNow using one of the following means:

- Support Portal at https://hi.service-now.com/. Customer may get login access to this self-service portal by contacting its ServiceNow administrator.
- Phone using one of the numbers at http://servicenow.com/support/contact-support.html.

Customer shall contact ServiceNow's authorized reseller in accordance with its agreement with the reseller.

Incident Priority

Incident priority for a defect is determined using the guidelines below:

Priority	Definition
P1	Any defect that causes an instance to be unavailable.
P2	Any defect that causes a critical function to fail.
P3	Any defect that significantly impedes work or progress.
P4	Any defect that does not significantly impede work or progress.

Response Times and Level of Effort

Customer submits an incident with ServiceNow via phone or web and with ServiceNow's authorized reseller as directed by reseller. All support requests are tracked online and can be viewed by Customer's authorized contacts. Response times do not vary if the incident was filed via phone or web.

ServiceNow or its authorized reseller, as applicable, will use reasonable efforts to meet the target response times and target level of effort stated in the table below. Support from the reseller may be limited to business hours only.

Priority	Target Response Times	Target Level of Effort
P1	30 minutes	Continuously, 24 hours per day, 7 days per week
P2	2 hours	Continuously, but not necessarily 24 hours per day, 7 days per week
P3	1 business day	As appropriate during normal business hours
P4	N/A	Varies

Customer Responsibilities

Customer's obligations are as follows:

(a) Customer agrees to receive from ServiceNow or its authorized reseller, as applicable, communications via email, phone or through the Support Portal regarding the Subscription Service.

(b) Customer shall appoint no more than five (5) contacts ("***Customer Authorized Contacts***") to engage Customer Support for questions and/or technical issues.

(i) Only Customer Authorized Contacts are authorized to contact Customer Support.

(ii) Customer must ensure the information for these contacts is current in the Support Portal at https://hi.service-now.com/.

(iii) Customer Authorized Contacts are trained on the use and administration of the Subscription Service.

(c) Customer shall cooperate to enable ServiceNow to deliver the Subscription Service and support for the service.

(d) Customer is solely responsible for the use of the Subscription Service by its authorized users.

Support Resources

- ServiceNow Website (http://www.servicenow.com/services/overview.html)
- ServiceNow Community (https://community.servicenow.com/welcome)
- Release Notes (http://wiki.service-now.com/index.php?title=Main_Page)
- Product Documentation (http://wiki.service-now.com/index.php?title=Main_Page)
- Knowledge Base (https://hi.service-now.com/nav_to.do?uri=kb_home.do)
- Support Community (https://community.servicenow.com/community/support)

UPGRADE POLICY

1. UPGRADES

"***Upgrades***" are ServiceNow's releases of the Subscription Service for repairs, enhancements or new features applied by ServiceNow to Customer's instances of the Subscription Service at no additional fee during the Subscription Term. ServiceNow has the discretion to provide new functionality as an Upgrade or as different software or service for a separate fee. ServiceNow determines whether and when to develop, release and apply any Upgrade to Customer's instances of the Subscription Service.

2. NOTICE; MAINTENANCE DOWNTIME

ServiceNow shall use reasonable efforts to give Customer thirty (30) days prior notice of any Upgrade to the Subscription Service. ServiceNow shall use reasonable efforts to give Customer ten (10) days prior notice of any Upgrade to the cloud infrastructure network, hardware, or software used by ServiceNow to operate and deliver the Subscription Service if ServiceNow in its reasonable judgment believes that the infrastructure Upgrade will impact Customer's use of its production instances of the Subscription Service. ServiceNow will use commercially reasonable efforts to limit the period of time during which the Subscription Service is unavailable due to the application of Upgrades to no more than two (2) hours per month. Notwithstanding the foregoing, ServiceNow may provide Customer with a shorter or no notice period of an Upgrade if necessary, in the reasonable judgment of ServiceNow, to maintain the availability, security or performance of the Subscription Service or the ability of ServiceNow to efficiently provide the Subscription Service.

3. NOMENCLATURE

A pending Upgrade may be a "Feature Release", "Patch" or "Hotfix." A "***Feature Release***" is an Upgrade that includes new features or enhancements. A "***Patch***" or a "***Hotfix***" is an Upgrade to a Feature Release that maintains the functionality of the Feature Release and does not include new functionality. ServiceNow refers to each Feature Release and its associated Patches and Hotfixes as a "***Release Family***." For example, ServiceNow's Feature Release "Aspen" established the "Aspen" Release Family, and ServiceNow's subsequent Feature Release "Berlin" established the "Berlin" Release Family.

4. PINNING REQUESTS

Customer may submit a support request for "no Upgrade" not fewer than five (5) business days' prior to a pending Upgrade of the Subscription Service. Subject to the terms and conditions of this Upgrade Policy, Customer's "no Upgrade" request shall be granted, and the Upgrade shall not be applied to Customer's instances of the Subscription Service.

5. SUPPORTED AND NON-SUPPORTED RELEASE FAMILIES

ServiceNow offers support for the then current Release Family and the prior two (2) Release Families ("***Supported Release Families***") as set forth in the Customer Support Policy. A Customer using a Supported Release Family may be required to Upgrade to a Patch or Hotfix within the Supported Release Family to correct a defect. At its discretion, ServiceNow may offer limited support for additional Release Families ("***Non-Supported Release Families***"). Without limiting ServiceNow's discretion to determine the availability of support for Non-Supported Release Families, a Customer using a Non-Supported Release Family may be required to Upgrade to a Supported Release Family to correct a defect. Any service level agreements, recovery time objectives or recovery point objectives are not applicable to Non-Supported Release Families. Details of ServiceNow support are further set forth in the Customer Support Policy.

Customer acknowledges that the current Release Family is the most current feature, availability, performance and security version of the Subscription Service. Within a Supported Release Family, the most recent Patch contains the most current feature, availability, performance and security version of the Subscription Service for that Release Family. A Customer that has submitted a "no Upgrade" request may experience defects, for which Customer hereby agrees that ServiceNow is not responsible, including without limitation those that affect the features, availability, performance and security of the Subscription Service, that are fixed in the most

current version of the Subscription Service.

6. REQUIRED UPGRADES

If Customer has requested "no Upgrade" it may nevertheless be required to Upgrade if in the reasonable judgment of ServiceNow the Upgrade is necessary to maintain the availability, security or performance of the Subscription Service or the ability of ServiceNow to efficiently provide the Subscription Service, as follows:

6.1. SUPPORTED RELEASE FAMILY. If Customer is using a Supported Release Family, it may be required to Upgrade to a Patch or Hotfix within the Supported Release Family.

6.2. NON-SUPPORTED RELEASE FAMILY. If Customer is using a Non-Supported Release Family, it may be required to Upgrade to a Supported Release Family.

7. EXCEPTIONS

Notwithstanding the other provisions of this Upgrade Policy, Customer may not submit a support request for "no Upgrade" for any Upgrade to, or that is essential for, the infrastructure network, hardware, or software used by ServiceNow to operate and deliver the Subscription Service.

DATA SECURITY GUIDE

Security Statement of an Enterprise IT Cloud Company

The ServiceNow cloud is built for the enterprise customer with every aspect aimed towards meeting the customer's demand for reliability, availability and security. ServiceNow's comprehensive approach to address this demand is enabled by the following: (a) ServiceNow's robust cloud infrastructure runs on its own applications and utilizes industry best-of-breed technology to automate mission critical functionalities in the cloud service with around-the-clock and around-the-world delivery; (b) ServiceNow achieves flexibility and control in its ability to deliver a stable user experience to the customer by having a logical single tenant architecture; (c) ServiceNow's application development which has a paramount focus on quality, security, and the user experience is closely connected to the operations of delivering those applications in a reliable and secure cloud environment; (d) ServiceNow invests in a comprehensive compliance strategy that allows its customers to attain their own compliance to applicable laws by obtaining attestations and certifications and running its subscription service from paired data centers situated close to where its customers are located; and (e) ServiceNow's homogeneous environment where all applications are on a single platform offers ServiceNow a competitive advantage in being able to concentrate its efforts to make the customer's user experience the best possible.

This Data Security Guide describes the measures ServiceNow takes to protect Customer Data when it resides in the ServiceNow cloud. This Data Security Guide forms a part of any legal agreement into which this Data Security Guide is explicitly incorporated by reference (the "***Agreement***") and is subject to the terms and conditions of the Agreement. Capitalized terms that are not otherwise defined herein shall have the meaning given to them in the Agreement.

1. SECURITY PROGRAM

While providing the Subscription Service, ServiceNow shall maintain a written information security program of policies, procedures and controls ("***Security Program***") governing the processing, storage, transmission and security of Customer Data. The Security Program includes industry standard practices designed to protect Customer Data from unauthorized access, acquisition, use, disclosure, or destruction. ServiceNow may periodically review and update the Security Program to address new and evolving security technologies, changes to industry standard practices, and changing security threats, provided that any such update does not materially reduce the commitments, protections or overall level of service provided to Customer as described herein.

2. CERTIFICATIONS AND ATTESTATIONS

2.1. Certifications and Attestations. ServiceNow shall establish and maintain sufficient controls to meet the objectives stated in ISO 27001 and SSAE 16 / SOC 1 and SOC 2 Type 2 (or equivalent standards) (collectively, the "***Standards***") for the information security management system supporting the Subscription Service. At least once per calendar year, ServiceNow shall perform an assessment against such Standards ("***Assessment***"). Upon Customer's written request, which shall be no more than once per calendar year, ServiceNow shall provide a summary of the Assessment(s) to Customer. Assessments shall be Confidential Information of ServiceNow.

2.2. Safe Harbor. ServiceNow shall maintain self-certified compliance under the U.S.-EU and U.S.-Swiss Safe Harbor Frameworks developed by the U.S. Department of Commerce regarding the collection, use and retention of Personal Data (defined in Section 6 below) from European Union member countries and Switzerland.

3. PHYSICAL, TECHNICAL AND ADMINISTRATIVE SECURITY MEASURES

The Security Program shall include the following physical, technical and administrative measures designed to protect Customer Data from unauthorized access, acquisition, use, disclosure, or destruction:

3.1. Physical Security Measures

(a) Data Center Facilities: (i) Physical access restrictions and monitoring that may include a combination of any of the following: multi-zone security, man-traps, appropriate perimeter deterrents (for example,

fencing, berms, guarded gates), on-site guards, biometric controls, CCTV, and secure cages; and (ii) fire detection and fire suppression systems both localized and throughout the data center floor.

(b) Systems, Machines and Devices: (i) Physical protection mechanisms; and (ii) entry controls to limit physical access.

(c) Media: (i) Industry standard destruction of sensitive materials before disposition of media; (ii) secure safe for storing damaged hard disks prior to physical destruction; and (iii) physical destruction of all decommissioned hard disks storing Customer Data.

3.2. Technical Security Measures

(a) Access Administration. Access to the Subscription Service by ServiceNow employees and contractors is protected by authentication and authorization mechanisms. User authentication is required to gain access to production and sub-production systems. Access privileges are based on job requirements and are revoked upon termination of employment or consulting relationship. Production infrastructure includes appropriate user account and password controls (for example, the required use of virtual private network connections, complex passwords with expiration dates, and a two-factored authenticated connection) and is accessible for administration.

(b) Logging and Monitoring. The production infrastructure log activities are centrally collected and are secured in an effort to prevent tampering and are monitored for anomalies by a trained security team.

(c) Firewall System. An industry-standard firewall is installed and managed to protect ServiceNow systems by residing on the network to inspect all ingress connections routed to the ServiceNow environment.

(d) Vulnerability Management. ServiceNow conducts periodic independent security risk evaluations to identify critical information assets, assess threats to such assets, determine potential vulnerabilities, and provide for remediation. When software vulnerabilities are revealed and addressed by a vendor patch, ServiceNow will obtain the patch from the applicable vendor and apply it within an appropriate timeframe in accordance with ServiceNow's then current vulnerability management and security patch management standard operating procedure and only after such patch is tested and determined to be safe for installation in all production systems.

(e) Antivirus. ServiceNow updates anti-virus, anti-malware, and anti-spyware software on regular intervals and centrally logs events for effectiveness of such software.

(f) Change Control. ServiceNow ensures that changes to platform, applications and production infrastructure are evaluated to minimize risk and are implemented following ServiceNow's standard operating procedure.

3.3. Administrative Security Measures

(a) Data Center Inspections. ServiceNow performs routine reviews at each data center to ensure that it continues to maintain the security controls necessary to comply with the Security Program.

(b) Personnel Security. ServiceNow performs background and drug screening on all employees and all contractors who have access to Customer Data in accordance with ServiceNow's then current applicable standard operating procedure and subject to applicable law.

(c) Security Awareness and Training. ServiceNow maintains a security awareness program that includes appropriate training of ServiceNow personnel on the Security Program. Training is conducted at time of hire and periodically throughout employment at ServiceNow.

(d) Vendor Risk Management. ServiceNow maintains a vendor risk management program that assesses all vendors that access, store, process or transmit Customer Data for appropriate security controls and business disciplines.

4. DATA PROTECTION AND SERVICE CONTINUITY

4.1. Data Centers; Data Backup. ServiceNow shall host Customer's instances in primary and secondary SSAE 16 Type II or ISO 27001 certified (or equivalent) data centers in the geographic regions specified on the Order Form for the Subscription Term. Each data center includes full redundancy (N+1) and fault tolerant infrastructure for electrical, cooling and network systems. The deployed servers are enterprise scale servers with redundant power to ensure maximum uptime and service availability. The production database servers are replicated in near real time to a mirrored data center in a different geographic region. Each customer instance is supported by a network configuration with multiple connections to the Internet. ServiceNow backs up all Customer Data in accordance with ServiceNow's standard operating procedure.

4.2. Personnel. In the event of an emergency that renders the customer support telephone system unavailable, all calls are routed to an answering service that will transfer to a ServiceNow telephone support representative, geographically located to ensure business continuity for support operations.

5. INCIDENT MANAGEMENT AND BREACH NOTIFICATION

5.1. Incident Monitoring and Management. ServiceNow shall monitor, analyze and respond to security incidents in a timely manner in accordance with ServiceNow's standard operating procedure. Depending on the nature of the incident, ServiceNow security group will escalate and engage response teams necessary to address an incident.

5.2. Breach Notification. Unless notification is delayed by the actions or demands of a law enforcement agency, ServiceNow shall report to Customer the unauthorized acquisition, access, use, disclosure or destruction of Customer Data (a "Breach") promptly following determination by ServiceNow that a Breach occurred. The initial report shall be made to Customer security contact(s) designated in ServiceNow's customer support portal. ServiceNow shall take reasonable measures to promptly mitigate the cause of the Breach and shall take reasonable corrective measures to prevent future Breaches. As information is collected or otherwise becomes available to ServiceNow and unless prohibited by law, ServiceNow shall provide information regarding the nature and consequences of the Breach that are reasonably requested to allow Customer to notify affected individuals, government agencies and/or credit bureaus. Customer is solely responsible for determining whether to notify impacted Data Subjects (defined in 6.1 below) and for providing such notice, and for determining if regulatory bodies or enforcement commissions applicable to Customer or Customer Data need to be notified of a Breach.

5.3. Customer Cooperation. Customer agrees to cooperate with ServiceNow in maintaining accurate contact information in the customer support portal and by providing any information that is reasonably requested to resolve any security incident, identify its root cause(s) and prevent a recurrence.

6. DATA PROCESSING GUIDELINES; COMPLIANCE WITH LAWS

6.1. Customer as Data Controller. Customer acknowledges that in relation to Personal Data supplied and/or processed under the Agreement it acts as Controller and it warrants that it will duly observe all of its obligations under all applicable laws and regulations of the European Union, the European Economic Area and their member states regarding the processing of Personal Data (collectively referred to as "Data Protection Laws") including, without limitation, obtaining and maintaining all necessary notifications and obtaining and maintaining all necessary Data Subject Consents. Customer shall (i) have sole responsibility for the accuracy, quality, integrity, legality and reliability of Personal Data and of the means by which it acquired Personal Data, (ii) ensure that data processing instructions given to ServiceNow comply with applicable Data Protection Laws, and (iii) comply with all applicable Data Protection Laws in collecting, compiling, storing, accessing and using Personal Data in connection with the Subscription Service. For the purposes of this Data Security Guide, "Personal Data", "Controller", "Data Subject" and "Data Subject Consent" shall have the meaning given to these terms in Directive 95/46/EC. For clarity, "process" or "processing" means any operation or set of operations performed upon Customer Data.

6.2. ServiceNow as Data Processor. ServiceNow shall process or otherwise use Personal Data (including possible onward transfers) on behalf of Customer solely for the purpose of providing the services

described in the Agreement and only in accordance with Customer's lawful instructions (limited to those instructions which ServiceNow can reasonably carry out in the provision of the Subscription Service), the terms of the Agreement, and this Data Security Guide. ServiceNow shall ensure that those employees to whom it grants access to such Personal Data are directed to keep such Personal Data confidential and are informed of any additional data protection obligations applicable to such Personal Data. ServiceNow shall, to the extent legally permitted, promptly notify Customer with respect to any request or communication ServiceNow receives from any regulatory authority in relation to any data processing activities ServiceNow conducts on behalf of Customer. In addition, ServiceNow will cooperate and assist Customer, at Customer's cost, in relation to any such request and to any response to any such communication. ServiceNow will pass on to the Customer any requests of a Data Subject to access, delete, correct, or block Personal Data processed under the Agreement. If ServiceNow is compelled by law to disclose Customer's information as part of a civil proceeding to which Customer is a party, and Customer is not contesting the disclosure, Customer will reimburse ServiceNow for its reasonable cost of compiling and providing secure access to that information.

6.3. Subcontractors. ServiceNow may engage subcontractors for processing Customer Data under the Agreement, provided ServiceNow shall ensure compliance by such subcontractor(s) with the requirements of this Section 6 by entering into written agreements with such subcontractors which provide that the subcontractor will apply the Safe Harbor principles to the processing of Personal Data. ServiceNow's use of any subcontractor will not relieve, waive or diminish any obligation ServiceNow has under the Agreement or this Data Security Guide.

7. PENETRATION TESTS

7.1. By a Third Party. ServiceNow contracts with third party vendors to perform an annual penetration test on the ServiceNow platform to identify risks and remediation that help increase security.

7.2. By Customer. No more than once per calendar year Customer may request to perform, at its own expense, an application penetration test of its instances of the Subscription Service. Customer shall notify ServiceNow in advance of any test by submitting a request using ServiceNow's online support portal and completing a penetration testing agreement. ServiceNow and Customer must agree upon a mutually acceptable time for the test; and Customer shall not perform a penetration test without ServiceNow's express written authorization. The test must be of reasonable duration, and must not interfere with ServiceNow's day-to-day operations. Promptly upon completion of the penetration test, Customer shall provide ServiceNow with the test results including any detected vulnerability. Upon such notice, ServiceNow shall, consistent with industry standard practices, use all commercially reasonable efforts to promptly make any necessary changes to improve the security of the Subscription Service. Customer shall treat the test results as Confidential Information of ServiceNow.

8. SHARING THE SECURITY RESPONSIBILITY

8.1. Product Capabilities. The Subscription Service has the capabilities to: (i) authenticate users before access; (ii) encrypt passwords; (iii) allow users to manage passwords; and (iv) prevent access by users with an inactive account. Customer manages each user's access to and use of the Subscription Service by assigning to each user a credential and user type that controls the level of access to the Subscription Service.

8.2. Customer Responsibilities. ServiceNow provides the cloud environment that permits Customer to use and process Customer Data in the Subscription Service. The architecture in the Subscription Service includes, without limitation, column level encryption functionality and the access control list engine. Customer shall be responsible for using the column level encryption functionality and access control list engine for protecting all Customer Data containing sensitive data, including without limitation, credit card numbers, social security numbers, financial and health information, and sensitive personal data. Customer is solely responsible for the results of its decision not to encrypt such sensitive data. ServiceNow protects all Customer Data in the ServiceNow cloud infrastructure equally in accordance with this Data Security Guide, regardless of the classification of the type of Customer Data. Customer shall be responsible for protecting the confidentiality of each user's login and password and shall manage each user's access to the Subscription Service.

8.3. Customer Cooperation. Customer shall promptly apply any application upgrade that ServiceNow determines is necessary to maintain the security, performance or availability of the Subscription Service.

8.4. Limitations. Notwithstanding anything to the contrary in the Agreement or this Data Security Guide, ServiceNow's obligations extend only to those systems, networks, network devices, facilities and components over which ServiceNow exercises control. This Data Security Guide does not apply to: (i) information shared with ServiceNow that is not data stored in its systems using the Subscription Service; (ii) data in Customer's virtual private network (VPN) or a third party network; or (iii) any data processed by Customer or its users in violation of the Agreement or this Data Security Guide.

servicenow

ServiceNow Product Overview

Effective Date: May 2, 2016

ServiceNow Applications	
Activity Designer	Enables a user to construct reusable activities that suit an organization's business needs. Requires Orchestration Core.
Activity Packs	A collection of related workflow activities that allow Orchestration Core to connect to, and automate work with, external systems. Some Activity Packs require Orchestration Core and others require Cloud Management.
Agile Development	Provides capabilities to manage the software development process in projects including enhancement requests, defect prioritization, definition of release content, and tasks.
Asset Management	Provides capabilities to track and manage the physical, contractual, and financial aspects of assets.
Audit Management	Provides a centralized process for Internal Audit teams to automate the complete audit lifecycle by providing the capability to plan, scope and execute integrated, risk-based audit plans.
Change Management	Allows repeatable methods and procedures to be used for introducing change into the IT infrastructure by providing capabilities for creating, assessing, approving, and executing changes.
Client Software Distribution	Allows administrators to distribute software from the service catalog using third party management systems. Requires Orchestration Core.
Cloud Management	Provides the capability to automate the provisioning and management lifecycle of public and private virtual servers. Requires Orchestration Core.
Configuration Automation	Provides the capability to manage the configuration settings of a physical or virtual server. Requires Orchestration Core.
Cost Management	Provides capabilities to track one-time and recurring costs of configuration items used by IT and allocate those costs to business units using allocation rules.
Cost Transparency	Provides insight for executives seeking to align spending to business goals. Users can classify general ledger records, define reporting structures and allocation rules, and view summary reports.
Customer Service Management	Includes the following key features: Omni–channel customer engagement across portal, chat, email, and phone (native telephony integration requires Notify); a robust customer data model for accounts, partners, and contacts; case management with advanced skills-based routing, real-time service level agreement (SLA), service contracts and service entitlements; pre-packaged service analytics using both real-time data as well as snapshots for trend analysis (trend analytics requires Performance Analytics use rights); and voice of customer feedback through online surveys and customer satisfaction reporting.

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.
ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

Demand Management	Consolidates IT requests through a service catalog and routes them in a workflow to stakeholders who gather additional information to prioritize investment decisions.
Discovery	Locates physical and virtual devices connected to an enterprise network. When Discovery locates a device, it explores its configuration, status, software, and relationships to other connected devices, and updates the Configuration Management Data Base (CMDB).
Edge Encryption	Resides on Customer-owned servers and encrypts and decrypts eligible data stored in their instance. Customer controls and manages the encryption keys for the eligible data in their instance.
Enterprise Service Portal - HR	In support of HR service delivery, provides employee self-service via an HR service catalog and provides HR the capability to assign tasks to employees. Uses prebuilt layouts, controls, and content. Requires HR Service Management.
Event Management	Aggregates events from monitoring tools used by Customer in its infrastructure, de-duplicates and correlates inputs from such events to CMDB, and provides the ability to filter and prioritize events to create incidents for remediation.
Facilities Service Management	Provides capabilities to manage the service delivery of a facilities department by offering a self-service catalog and assignment of requests based on fulfillment rules.
Field Service Management	Provides capabilities to create work order records for the repair and service of equipment. Requires Asset Management.
Financial Planning	Assists executives and budget owners in the automation of budget and forecast planning, helping to increase efficiency and simplify the planning process.
Finance Service Management	Enables the finance department to define its services and fulfill requests through workflow capabilities and knowledge management, and provides visibility into resource utilization and service delivery performance through dashboards.
HR Service Management	Provides capabilities to manage HR service delivery using case management to document the interactions between the employee and HR supported by the knowledge base.
Incident Management	Facilitates the process of restoring normal IT operations by providing capabilities to record, classify, distribute, and manage incidents through to resolution. Includes Performance Analytics limited to 15 key performance indicators (KPIs), one dashboard and 90 days of data captured by Incident Management.
Legal Service Management	Enables the legal department to define its services and fulfill requests through workflow capabilities and knowledge management, and provides visibility into resource utilization and service delivery performance through dashboards.
Marketing Service	Enables the marketing department to define its services and fulfill requests

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.
ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

Management	through workflow capabilities and knowledge management, and provides visibility into resource utilization and service delivery performance through dashboards.
Notify	Provides the capability to initiate notification from Customer's instance of the subscription service to a supported third-party platform for SMS, voice and other communications protocols. Customer is required to separately purchase any third-party service required to work with Notify.
Orchestration Core	Enables orchestration of activities outside Customer's instance of the subscription service. Allows Customer to automate discrete tasks or processes using graphical workflows that interact with external systems or services.
Password Reset	Provides the capability to reset User's passwords that are stored and pre-authenticated in a credential store outside Customer's instance of the subscription service, such as Active Directory and other supported credential stores. Requires Orchestration Core.
Performance Analytics	Provides advanced analytics and time series analysis for KPIs.
Platform Runtime	Allows customer to deploy applications developed on the ServiceNow Platform into production.
Policy and Compliance Management	Provides a centralized process for creating and managing policies, standards, and internal control procedures that are cross-mapped to external regulations and best practices. Additionally, the application provides structured workflows for the identification, assessment, and continuous monitoring of control activities.
Problem Management	Facilitates the process of identifying the root causes of errors in the IT infrastructure by providing capabilities to record, escalate, and manage problems through to resolution.
Project Portfolio Management	Provides capabilities to plan, organize, and manage projects and project portfolios including associated tasks and resources.
Release Management	Facilitates the planning, design, build, configuration, testing, and release of hardware and software into the IT infrastructure.
Request Management	Provides capabilities to approve and fulfill requests for goods and services defined and presented in the service catalog.
Resource Management	Provides a view of projects and the availability, allocation, and capacity of assigned resources.
Risk Management	Provides an executive view into risk to allow risk managers to quickly identify at-risk assets, perform assessments, and continuously monitor risk exposure.
Security Incident Response	Enables SOC/SIRT teams to enact response plans to address security-related activities, events or incidents. Enables response team collaboration, investigation of network and non-network related activities (i.e. intellectual property theft, criminal activities, etc.) and includes the capability for automated request assignment and remediation across IT and security teams.

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.
ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

Service Mapping	Discovers business services of the organization and builds a comprehensive map of all devices, applications, and configuration profiles used in these business services.
Test Management	Provides a user acceptance testing framework to help project teams and business users align on project deliverables, and provides visibility into the status of the project testing when used in conjunction with Project Portfolio Management and Agile Development. Project Portfolio Management and Agile Development are separately authorized.
Threat Intelligence	Provides the ability to support multiple threat intelligence feeds to enhance the context of a security incident by enabling analysts to see potential threats and related systems in an integrated view. Threat Intelligence also allows Customers to add their own custom feeds and to place confidence scores or weighting on each feed to accelerate the identification of legitimate security issues.
Vendor Performance Management	Enables Customer to manage, evaluate and compare vendors based on predefined criteria.
Vulnerability Response	Integrates with the National Vulnerability Database (NVD) and third-party solutions to generate a set of actionable reports of vulnerable assets in the Customer environment. Incident response tasks, change requests or problem tickets can easily be opened from vulnerabilities to allow security teams to perform further investigation or to allow IT to perform remediation.
ServiceNow Platform Services	
Business Service Maps	Graphically displays the configuration items related to a business service, and indicates the status of those configuration items.
Chat	Provides real-time communication capability via instant messaging between Users.
Coaching Loops	Provides the capability to monitor and provide feedback on a specific behavior of an individual or group.
Configuration Management (CMDB)	Provides capabilities to identify, record, and report on IT configuration items and their relationships.
Connect	Provides the capability to connect people, processes and information into a unique and centralized collaboration workspace to cut down on resolution times. Features include real-time chat, document delivery, active lists to see who is working and the ability to interact straight from the activity stream.
Content Management System	Provides the ability to create custom interfaces.
Form Designer	Allows creation of forms and tables with visual controls.

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.
ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

Google Maps	ServiceNow may make Google Maps available for use with the subscription service. If Customer uses Google Maps, Customer agrees to the following terms: (i) Customer shall limit its use to 60,000 map views on an annual basis and additional use shall be purchased from Google subject to Google's terms and conditions, to which ServiceNow is not a party; (ii) Customer agrees, and shall cause its end users to agree, to Google's Maps Terms (http://maps.google.com/help/terms_maps.html or a successor URL as provided by Google), the Legal Notices (http://www.maps.google.com/help/legalnotices_maps.html or a successor URL as provided by Google), and the Acceptable Use Policy (http://www.google.com/enterprise/earthmaps/legal/us/maps_AUP.html or a successor URL as provided by Google); and (iii) Customer agrees that Google may use Customer data in accordance with its privacy policy and that Google may provide its maps services to Customer. Google Maps may not be available to Customer due to location availability and may not be available during Customer's entire subscription term. ServiceNow support and warranty do not apply to Google Maps.
Graphical Workflow	Provides the capability to automate multi-step processes within Customer's instance of the subscription service. Each workflow can manage a sequence of activities, such as creating records or running scripts, and the condition-based transitions between them. Customer is required to purchase Orchestration Core to orchestrate activities using the Graphical Workflow that interact outside Customer's instance of the subscription service.
Knowledge Management	Provides role-based tools to create, store, and publish information. Provides mechanisms for version control and approvals of documents in the review process.
Live Feed	Provides a place to post and share content.
Mobile	Provides a customizable ServiceNow interface for mobile devices.
On-Call Scheduling	Enables creation of on-call schedules and escalation rosters.
OpenFrame	An interface technology that enables real-time communication channels such as telephone systems to be integrated into the ServiceNow Platform. OpenFrame consists of UI elements as well as a set of APIs that support exchange of events and data between ServiceNow and the communications system.
Reporting	Provides the capability to create and share reports and dashboards.
REST API	Provides the ability to integrate external systems through REST APIs using standard respond codes, header information, pagination support and streaming data on requests.
Service Catalog	Displays a listing of the goods and services that Customer provides within the enterprise to its employees and contractors.
Service Creator	Provides capabilities for building no-code service catalog items.

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.
ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

Service Level Management	Establishes and monitors status of service contracts and SLAs between the organization and its customers or third-party service providers.
Service Portal Designer	Provides the capability to build portals with a consumer-like experience using both ServiceNow out-of-the-box widgets and templates as well as Customer's own widgets and styles, while leveraging only HTML and CSS.
Skills Management	Assigns configured competencies to groups or users.
Studio	Integrated Development Environment (IDE) for professional and low-code (i.e., IT administration) application developers.
Survey Management	Allows for polling and collection of data, including configuration for specific events and/or conditions.
Time Cards	Records time worked on tasks either manually or automatically.
Visual Task Boards	Enables a Kanban-style workspace for either individual or team-based management of tasks.
Visualizations	Displays interactive 2-D and 3-D visual representations for any logical data relationships within an instance.

© 2016 ServiceNow, Inc. All rights reserved. ServiceNow Confidential.
ServiceNow and the ServiceNow logo are trademarks of ServiceNow, Inc. All other brand and product names are trademarks or registered trademarks of their respective holders.

GENERAL TERMS AND CONDITIONS

These General Terms and Conditions and any referenced documents form the agreement (the "***Agreement***") under which an Order Form is executed.

1. PROVISION OF SERVICES

ServiceNow will make the following purchased services available to Customer, subject to the terms and conditions of the Agreement and each ordering document signed by Customer and ServiceNow (each, an "***Order Form***") and the product overview attached thereto or referenced therein ("***Product Overview***"), including without limitation:

(a) use of the ServiceNow applications which are made available by ServiceNow as a software as a service (SaaS) ("***Subscription Service***"); and

(b) professional services and training services ("***Professional Services***").

An Order Form for Professional Services shall specify ServiceNow packaged professional services (each offering, a "***Packaged Service***"), as described in one or more service descriptions (if not attached to the Order Form, then as set forth on www.servicenow.com/be_schedules.do) ("***Service Description***") or other Professional Services described in one or more written statements of work ("***SOW***") signed by ServiceNow and Customer.

2. ORDERING

2.1 ORDERS AND PAYMENT. Upon execution by Customer and ServiceNow, each Order Form is non-cancellable and non-refundable except as provided in the Agreement. Prices stated in each Order Form are final. Except as expressly set forth in the applicable Order Form, Subscription Service fees are invoiced annually in advance. Each Subscription Term (as defined in Section 3.1) as set forth in the Order Form is a continuous and non-divisible commitment for the full duration of the Subscription Term regardless of the invoice schedule. Except as expressly set forth in the applicable Order Form or SOW or Service Description, Professional Services fees are invoiced on a time and materials basis monthly in arrears. Customer shall pay each invoice in full within thirty (30) days after the date of invoice. Customer may issue a purchase order consistent with the terms of the Order Form, but a purchase order is not required. If Customer issues a purchase order, then it shall be for the full amount of the Order Form, and any additional or conflicting terms appearing in a purchase order shall not amend the Order Form or the Agreement. Upon request, ServiceNow shall reference the purchase order number on its invoices (solely for administrative convenience) so long as Customer provides the purchase order at least fifteen (15) business days prior to the date of the invoice. Late payments shall accrue interest at a rate of one and one-half percent (1.5%) per month or the legal maximum interest rate, whichever is lower. If Customer is delinquent in payment of amounts for the services owed hereunder, ServiceNow may give notice to Customer of such delinquency and, in such case, Customer shall cure the delinquency within thirty (30) days from the date of ServiceNow's written notice. If Customer fails to cure the delinquency, ServiceNow may suspend Customer's use of the Subscription Service or terminate the Agreement for cause in accordance with Section 7 (Term and Termination), in addition to other rights and remedies available.

2.2 TAXES. All payments required by the Agreement are stated exclusive of all taxes, duties, levies, imposts, fines or similar governmental assessments including sales and use taxes, value-added taxes ("***VAT***"), goods and services taxes ("***GST***"), excise, business, service, and similar transactional taxes imposed by any jurisdiction and the interest and penalties thereon (collectively, "***Taxes***"). Customer shall be responsible for and bear Taxes associated with its purchase of, payment for, access to or use of the Subscription Service and Professional Services. Taxes shall not be deducted from the payments to ServiceNow, except as required by law, in which case Customer shall increase the amount payable as necessary so that after making all required deductions and withholdings, ServiceNow receives and retains (free from any Tax liability) an amount equal to the amount it would have received had no such deductions or withholdings been made. Each party is responsible for and shall bear taxes imposed on its net income. If Customer is a tax-exempt entity or claims exemption from any Taxes under the Agreement, Customer shall provide a tax exemption number on the Order Form and a certificate upon execution of the Order Form and, after receipt of valid evidence of exemption, ServiceNow shall not charge Customer any Taxes from which it is exempt. If ServiceNow is required to invoice or collect Taxes associated with Customer's purchase of, payment for, access to or use of the Subscription Service or Professional Services, ServiceNow will issue an invoice to Customer including the amount of those Taxes, itemized where required by law. Customer shall provide to ServiceNow its VAT or GST identification number(s) on the Order Form for (i) the country where Customer has established its business and/or (ii) any other country where Customer has a fixed establishment. Customer shall use the ordered Subscription Service and Professional Services for Customer's business use in the foregoing location(s) in accordance with the provided VAT or GST identification number(s). The parties' obligations under this Section shall survive the termination or expiration of the Agreement.

2.3 USE VERIFICATION. Customer may not use or otherwise access the Subscription Service in a manner that exceeds Customer's authorized use. ServiceNow may review Customer's use of the Subscription Service, and Customer shall provide any reasonable assistance to verify Customer's compliance with the Agreement. If ServiceNow determines that Customer has exceeded its permitted use of the Subscription Service then ServiceNow will notify Customer and within thirty (30) days thereafter Customer shall either: (i) disable any unpermitted use or (ii) purchase additional subscriptions. If Customer fails to regain compliance within such thirty (30) day period, ServiceNow may suspend Customer's use of the Subscription Service or terminate the Agreement for cause in accordance with Section 7 (Term and Termination), in addition to any other rights or remedies ServiceNow may have.

3. GRANT OF USE RIGHTS; OWNERSHIP; CUSTOMER RESTRICTIONS

3.1. SUBSCRIPTION SERVICE. Customer is authorized to use the Subscription Service limited by the purchased amount and subscription term ("***Subscription Term***") on the Order Form and the Product Overview.

3.2. DOCUMENTATION. ServiceNow grants to Customer a non-exclusive, non-transferable, worldwide right during the Subscription Term to access and use the documentation relating to the operation and use of the Subscription Service that is provided by ServiceNow to Customer under the Agreement, as updated by ServiceNow from time to time ("***Documentation***").

3.3. CUSTOMER DATA. Customer grants ServiceNow a non-exclusive, non-transferable, worldwide right to use the electronic data pertaining to Customer and/or its users that is processed using the Subscription Service (collectively "***Customer Data***") strictly for the limited purpose of providing the Subscription Service to Customer.

3.4. SOFTWARE. ServiceNow may provide ServiceNow software products ("***Software***") for use in connection with the Subscription Service. Any Software is licensed and not sold (even if for convenience ServiceNow makes reference to words such as "sale" or "purchase"). ServiceNow grants Customer a limited, personal, worldwide, non-sublicensable, non-transferable, non-exclusive license to install and execute the Software on machines operated by or for Customer solely to permit Customer to use the Subscription Service during the Subscription Term in accordance with the terms and conditions of the Agreement. The Software may include code that is licensed under third party license agreements, including open source made available or provided with the Software.

3.5. OWNERSHIP. As between ServiceNow and Customer, all rights, title, and interest in and to all intellectual property rights in the Subscription Service, Software and/or Documentation are owned exclusively by ServiceNow. Except as expressly provided in the Agreement, ServiceNow does not grant Customer (and expressly reserves) any rights, express or implied, or ownership in the Subscription Service, Software and/or Documentation. ServiceNow shall have a royalty-free, worldwide, non-exclusive, transferable, sub-licensable, irrevocable, perpetual right to make, use, sell, offer for sale, import, or otherwise incorporate into the Subscription Service, Software and/or Documentation, any suggestions, enhancements, recommendations or other feedback provided by Customer relating to the Subscription Service, Software and/or Documentation.

3.6. RESTRICTIONS. Customer shall not (and shall not permit others to) do the following with respect to the Subscription Service, Software or Documentation: (i) license, sub-license, sell, re-sell, rent, lease, transfer, distribute or time share or otherwise make any of them available for access by third parties; (ii) disassemble, reverse engineer, decompile or modify them or otherwise create derivative works thereof; (iii) access them for the purpose of developing products or services that compete with the Subscription Service; (iv) use them to operate more or different type of applications or platform not authorized under the Agreement; (v) use them to create, use, send, store or run viruses or other harmful computer code, files, scripts, agents or other programs or engage in any other malicious act; (vi) disrupt their security, integrity or operation; (vii) remove or modify a copyright or other proprietary rights notice in them; (viii) use them to reproduce, distribute, display, transmit or use material protected by copyright or other intellectual property right (including the rights of publicity or privacy) without first obtaining the permission of the owner; (ix) use them to damage the property of another; (x) use them in any manner which violates any law or regulation of the United States, any state thereof or other government authority; (xi) use them in any manner that disables, hacks or otherwise interferes with any security, digital signing, digital rights management, verification or authentication mechanisms or (xii) use them in a manner that temporarily or permanently alters, erases, removes, copies, modifies, halts or disables any ServiceNow or third party data, software or network.

4. WARRANTIES

4.1. LIMITED SUBSCRIPTION SERVICE WARRANTY. ServiceNow warrants that during the Subscription Term Customer's production instances of the Subscription Service shall materially conform to the Product Overview. To submit a warranty claim under this Section, Customer shall (1) reference this Section; and (2) submit a support request to resolve the non-conformity as provided in the Subscription Service Guide, which is set forth on www.servicenow.com/be_schedules.do. If the non-conformity persists without relief more than thirty (30) days after written notice of a warranty claim provided to

ServiceNow under this Section 4.1, then Customer may terminate the affected Subscription Service and ServiceNow shall refund to Customer any prepaid subscription fees covering the remainder of the Subscription Term of the affected Subscription Service after the date of termination. Notwithstanding the foregoing, this warranty shall not apply to any non-conformity due to a modification of or defect in the Subscription Service that is made or caused by any person other than ServiceNow or a person acting at ServiceNow's direction. THIS SECTION 4.1 SETS FORTH CUSTOMER'S EXCLUSIVE RIGHTS AND REMEDIES (AND SERVICENOW'S SOLE LIABILITY) IN CONNECTION WITH THIS WARRANTY.

4.2. LIMITED PROFESSIONAL SERVICES WARRANTY. ServiceNow warrants that the Professional Services will be performed in a competent and workmanlike manner in accordance with accepted industry standards and practices and all material requirements set forth in the SOW or Service Description. Customer shall notify ServiceNow in writing of any breach within thirty (30) days after performance of the non-conforming Professional Services. Upon receipt of such notice, ServiceNow, at its option, shall either use commercially reasonable efforts to re-perform the Professional Services in conformance with these warranty requirements or shall terminate the affected Professional Services and refund to Customer any amounts paid for the nonconforming Professional Services. THIS SECTION 4.2 SETS FORTH CUSTOMER'S EXCLUSIVE RIGHTS AND REMEDIES (AND SERVICENOW'S SOLE LIABILITY) IN CONNECTION WITH THIS WARRANTY.

4.3. DISCLAIMER OF WARRANTIES. EXCEPT FOR THE WARRANTIES EXPRESSLY STATED IN THE AGREEMENT, TO THE MAXIMUM EXTENT ALLOWED BY LAW, SERVICENOW DISCLAIMS ALL WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, ORAL OR WRITTEN, INCLUDING WARRANTIES ARISING UNDER STATUTE, WARRANTIES OF MERCHANTABILITY, ACCURACY, TITLE, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE OR ANY WARRANTIES ARISING FROM USAGE OF TRADE, COURSE OF DEALING OR COURSE OF PERFORMANCE. WITHOUT LIMITING THE GENERALITY OF THE FOREGOING, SERVICENOW SPECIFICALLY DOES NOT WARRANT THAT THE SUBSCRIPTION SERVICE, SOFTWARE, PROFESSIONAL SERVICES OR DOCUMENTATION WILL MEET THE REQUIREMENTS OF CUSTOMER OR OTHERS OR THAT THEY WILL BE ACCURATE OR OPERATE WITHOUT INTERRUPTION OR ERROR. CUSTOMER ACKNOWLEDGES THAT IN ENTERING THE AGREEMENT IT HAS NOT RELIED ON ANY PROMISE, WARRANTY OR REPRESENTATION NOT EXPRESSLY SET FORTH HEREIN.

5. CONFIDENTIALITY AND NON-USE RESTRICTIONS

5.1. CONFIDENTIAL INFORMATION. "***Confidential Information***" means all information disclosed by a party ("***Disclosing Party***") to the other party ("***Receiving Party***"), whether orally or in writing, that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information and the circumstances of the disclosure, including without limitation: each party's respective business plans and processes; financial and employee data; proprietary technology and product information and designs; the Subscription Service and Software and Customer Data. The terms of the Agreement and Order form(s) are Confidential Information of ServiceNow. Confidential Information excludes information that: (i) is or becomes generally known to the public; (ii) was known to the Receiving Party prior to its disclosure by the Disclosing Party without breach of any obligation to the Disclosing Party; (iii) is received from a third party without any obligation of confidentiality to a third party or breach of any obligation of confidentiality to the Disclosing Party; or (iv) was independently developed by the Receiving Party without reference to the Disclosing Party's Confidential Information.

5.2. PROTECTION. The Receiving Party shall: (i) at all times protect the confidentiality of the Disclosing Party's Confidential Information with the same degree of care that it uses to protect its own confidential information, and in no event using less than reasonable care; and (ii) not use Confidential Information of the Disclosing Party except to the extent necessary to exercise its rights or fulfill its obligations under the Agreement. To the extent necessary under the Agreement, the Receiving Party may disclose the Confidential Information of the Disclosing Party to the Receiving Party's employees or contractors who are bound by written obligations of confidentiality and non-use and non-disclosure restrictions at least as protective as those set forth herein. In the event of a court order or government regulation compelling disclosure of any Confidential Information, the Receiving Party shall provide the Disclosing Party with prompt written notice thereof, and shall reasonably cooperate with the Disclosing Party to seek confidential or other protective treatment. Each party's obligations set forth in this Section 5 shall remain in effect during the term and three (3) years after termination of the Agreement. The Receiving Party shall promptly return to the Disclosing Party or destroy (with certification of such destruction provided by the Receiving Party upon request) all Confidential Information of the Disclosing Party in its possession or control upon request from the Disclosing Party. Provisions for the return of Customer Data are set forth in Section 7.3 (Return of Customer Data).

6. LIMITATIONS OF LIABILITY AND DAMAGES

6.1. LIMITATIONS OF LIABILITY. TO THE EXTENT PERMITTED BY LAW, THE TOTAL, CUMULATIVE LIABILITY OF EACH PARTY ARISING OUT OF OR RELATED TO The AGREEMENT OR THE SERVICES PROVIDED HEREUNDER, WHETHER BASED ON CONTRACT, IN TORT OR ANY OTHER LEGAL OR EQUITABLE THEORY, SHALL BE LIMITED TO THE AMOUNTS PAID BY CUSTOMER FOR THE SERVICE GIVING RISE TO THE CLAIM DURING THE

TWELVE (12) MONTH PERIOD PRECEDING THE FIRST EVENT GIVING RISE TO LIABILITY. THE EXISTENCE OF MORE THAN ONE CLAIM SHALL NOT ENLARGE THIS LIMIT. THE FOREGOING LIMITATION OF LIABILITY SHALL NOT APPLY TO: (1) BODILY INJURY OR DEATH; (2) INFRINGEMENT BY A PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS; AND (3) CUSTOMER'S OBLIGATION TO PAY AMOUNTS OWED FOR SERVICES PROVIDED HEREUNDER.

6.2. EXCLUSION OF DAMAGES. TO THE EXTENT PERMITTED BY LAW, NEITHER SERVICENOW NOR CUSTOMER SHALL BE LIABLE TO THE OTHER OR ANY THIRD PARTY FOR LOST PROFITS (WHETHER DIRECT OR INDIRECT) OR LOSS OF USE OR DATA, COVER, SUBSTITUTE GOODS OR SERVICES, OR FOR INCIDENTAL, CONSEQUENTIAL, PUNITIVE, SPECIAL OR EXEMPLARY DAMAGES (INCLUDING DAMAGE TO BUSINESS, REPUTATION OR GOODWILL), OR INDIRECT DAMAGES OF ANY TYPE HOWEVER CAUSED, WHETHER BY BREACH OF WARRANTY, BREACH OF CONTRACT, IN TORT OR ANY OTHER LEGAL OR EQUITABLE CAUSE OF ACTION EVEN IF SUCH PARTY HAS BEEN ADVISED OF SUCH DAMAGES IN ADVANCE OR IF SUCH DAMAGES WERE FORESEEABLE. THE FOREGOING EXCLUSIONS SHALL NOT APPLY TO: (1) BODILY INJURY OR DEATH; AND (2) INFRINGEMENT BY A PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS.

7. TERM AND TERMINATION

7.1. TERM AND TERMINATION. The Agreement continues until terminated in accordance with its terms. Each party may terminate the Agreement in its entirety either: (i) upon thirty (30) days' prior written notice to the other party, if at the time such notice is served there are no Order Forms in effect; or (ii) upon written notice if the other party becomes the subject of a petition in bankruptcy or any proceeding related to its insolvency, receivership or liquidation, in any jurisdiction, that is not dismissed within sixty (60) days of its commencement or an assignment for the benefit of creditors. Either party may terminate a Subscription Service or Professional Services effective immediately upon written notice if the other party materially breaches a material obligation under the Agreement or the applicable Order Form for the affected service and does not cure the breach within thirty (30) days after receiving written notice thereof from the non-breaching party. Professional Services are separately ordered from the Subscription Service, and are not required for the Subscription Service. A breach by a party of its obligations with respect to Professional Services shall not by itself constitute a breach by that party of its obligations with respect to the Subscription Service even if the services are enumerated in the same Order Form.

7.2. EFFECT OF TERMINATION OF SERVICE. Upon expiration or other termination of the Subscription Service for any reason, Customer shall stop using, and ServiceNow shall stop providing, the terminated Subscription Service. (a) If the Subscription Service is terminated by Customer due to ServiceNow's breach, then ServiceNow shall refund to Customer, within thirty (30) days after the effective date of termination, all prepaid fees for the remaining portion of the Subscription Term for the terminated Subscription Service after the effective date of termination. (b) If Professional Service is terminated by Customer due to ServiceNow's breach, then ServiceNow shall refund to Customer, within thirty (30) days after the effective date of termination, any prepaid amounts for unperformed Professional Service. (c) If the Subscription Service is terminated by ServiceNow due to Customer's breach, then Customer shall pay to ServiceNow, within thirty (30) days after the effective date of termination, fees for the terminated Subscription Service that would have been payable for the remainder of the Subscription Term after the effective date of termination. (d) Upon expiration or other termination of the Subscription Service for any reason, Customer shall be eligible to request the return of Customer Data in accordance with Section 7.3 (Return of Customer Data).

7.3. RETURN OF CUSTOMER DATA. Following the end of the Subscription Term, where Customer has not renewed, Customer shall have forty-five (45) days to request a copy of the Customer Data from ServiceNow; and, if requested, ServiceNow shall use commercially reasonable efforts to provide a copy of that data within fifteen (15) days in a mutually agreed upon, commercially standard format at no cost to Customer unless ServiceNow determines in its reasonable discretion that the data output is not routine, in which case the parties shall mutually agree on a statement of work for professional services. After such forty-five (45) day period, ServiceNow shall have no obligation to maintain or provide any Customer Data and shall thereafter, unless legally prohibited, have the right to delete all Customer Data in its systems or otherwise in its possession or under its control and delete Customer's instances of the Subscription Service.

7.4. SURVIVAL. Upon termination of the Agreement for any reason, Customer shall pay all amounts owed hereunder. Sections 3.5 (Ownership), 3.6 (Restrictions), and 5 (Confidentiality and Non-Use Restrictions) through 8 (General Provisions) of these General Terms and Conditions, together with any other provision required for their construction or enforcement, shall survive termination of the Agreement for any reason.

8. GENERAL PROVISIONS

8.1. ASSIGNMENT. Neither party may assign its rights or obligations, whether by operation of law or otherwise, without the prior written consent of the other party. Notwithstanding the foregoing, either party may, upon notice and without the other party's consent: (i) in connection with a merger, reorganization or sale of all or substantially all of the assets or equity

of such party, assign the Agreement in its entirety to such party's successor; and (ii) assign the Agreement in its entirety to any company, partnership or other legal entity which from time to time directly or indirectly controls, is controlled by or is under the common control with such party. Any attempted or purported assignment in violation of this Section 8.1 will be null and void. Subject to the foregoing, the Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

8.2. NOTICE. Except as otherwise provided herein, all notices shall be in writing and deemed given upon: (i) personal delivery; (ii) when received by the addressee if sent by a nationally recognized overnight courier (receipt requested); (iii) the second business day after mailing; or (iv) the first business day after sending by email, except that email shall not be sufficient for notices regarding a Claim. Notices shall be sent to the parties as set forth on the Order Form or as otherwise agreed to by the parties in writing.

8.3. EXPORT COMPLIANCE. Each party shall comply with United States and foreign export control laws and regulations. Customer acknowledges that the Subscription Service, Professional Services, Software and Documentation are subject to the U.S. Export Administration Regulations (the "***EAR***") and that Customer shall comply with the EAR. Without limiting the foregoing, Customer represents and warrants that: (i) Customer is not located in, and shall not use the Subscription Service, Professional Services, Software and Documentation from, any country that is subject to U.S. export restrictions (currently including, but not necessarily limited to, Cuba, Iran, North Korea, Sudan and Syria); (ii) Customer shall not use the Subscription Service, Professional Services, Software and Documentation in the design, development or production of nuclear, chemical or biological weapons, or rocket systems, space launch vehicles, sounding rockets or unmanned air vehicle systems; and (iii) Customer is not prohibited from participating in the U.S. export transactions by any federal agency of the U.S. government. In addition, Customer is responsible for complying with any local laws which may impact Customer's right to import, export or use the Subscription Service, Professional Services, Software and Documentation.

8.4. FORCE MAJEURE. No party shall be liable or responsible to the other party, nor be deemed to have defaulted under or breached the Agreement, for any failure or delay in fulfilling or performing any term of the Agreement, when and to the extent such failure or delay is caused by or results from acts beyond the affected party's reasonable control, including without limitation: strikes, lock-outs or other industrial disputes (whether involving its own workforce or a third party's), trespassing, sabotage, theft or other criminal acts, failure of energy sources or transport network, acts of God, war, terrorism, riot, civil commotion, interference by civil or military authorities, national or international calamity, armed conflict, malicious damage, breakdown of plant or machinery, nuclear, chemical or biological contamination, explosions, collapse of building structures, fires, floods, storms, earthquakes, epidemics or similar events, natural disasters or extreme adverse weather conditions (each a "***Force Majeure Event***"). The party suffering a Force Majeure Event shall use reasonable efforts to mitigate against the effects of such Force Majeure Event.

8.5. US GOVERNMENT RIGHTS. All ServiceNow software is commercial computer software and all services are commercial items. "***Commercial computer software***" has the meaning set forth in Federal Acquisition Regulation ("***FAR***") 2.101 for civilian agency purchases and the Department of Defense ("***DOD***") FAR Supplement ("***DFARS***") 252.227-7014(a)(1) for defense agency purchases. If the software is licensed or the services are acquired by or on behalf of a civilian agency, ServiceNow provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as required in FAR 12.212 (Computer Software) and FAR 12.211 (Technical Data) and their successors. If the software is licensed or the services are acquired by or on behalf of any agency within the DOD, ServiceNow provides the commercial computer software and/or commercial computer software documentation and other technical data subject to the terms of the Agreement as specified in DFARS 227.7202-3 and its successors. Only if this is a DOD prime contract or DOD subcontract, the Government acquires additional rights in technical data as set forth in DFARS 252.227-7015. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFARS or other clause or provision that addresses Government rights in computer software or technical data.

8.6. ENTIRETY. Customer acknowledges that it has not relied on any statement, promise or representation made or given by or on behalf of ServiceNow which is not set out in the Agreement. Customer's order is not contingent on, and Customer has not relied on, the delivery of any future functionality regardless of any verbal or written communication about ServiceNow's future plans. The Agreement supersedes all prior or contemporaneous oral or written agreement, representations and negotiations, including, but not limited to, any terms contained in Customer's purchase order.

8.7. WAIVER AND AMENDMENT. A waiver of any right is only effective if it is in writing and only against the party who signed such writing and for the circumstances given. Any modification of the Agreement, an Order Form, the Product Overview, the Subscription Service Guide, a SOW or a Service Description must be in writing and signed by authorized representatives of both parties.

8.8. RELATIONSHIP OF THE PARTIES. The parties are independent contractors. Nothing in the Agreement shall be construed to create a partnership, joint venture or agency relationship. Neither party shall have any right or authority

to assume or create any obligation of any kind expressed or implied in the name of or on behalf of the other party. ServiceNow may at any time subcontract or delegate in any manner any or all of its obligations under the Agreement to any third party or agent.

8.9. GOVERNING LAW; VENUE; TIME FOR BRINGING ACTION. The Agreement shall be governed by, subject to, and interpreted in accordance with the laws of the state of California, United States of America, if Customer is located in Canada, United States or Mexico, and the laws of England if Customer is located elsewhere. If Customer is located in Canada, United State or Mexico, the parties hereby irrevocably consent to the nonexclusive jurisdiction of, and venue in, any federal or state court of competent jurisdiction located in San Diego, California, or New York, New York, for the purposes of adjudicating any action or proceeding to enforce the terms of the Agreement. If Customer is located elsewhere, then any dispute arising under the Agreement shall be finally settled by binding arbitration in London, England. Such arbitration shall be conducted in English in accordance with the rules of the International Chamber of Commerce by one (1) arbitrator appointed in accordance with such rules. The arbitrator shall allow such discovery as is appropriate in accomplishing a fair, speedy, and cost-effective resolution of the dispute, and shall be expressly empowered to issue appropriate injunctive relief. The award of arbitration shall be final and binding upon both parties, and judgment on the award rendered by the arbitrator may be entered in any court having jurisdiction thereof. Any monetary award shall be payable in United States dollars. To the extent permitted by law, choice of law rules and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. No cause of action arising hereunder or relating hereto may be brought more than one (1) year after it first accrues. The prevailing party in an action to enforce the Agreement shall be entitled to costs of bringing the claim and reasonable attorneys' and experts' fees and expenses. Notwithstanding the foregoing, either party may at any time seek and obtain appropriate legal or equitable relief in any court of competent jurisdiction for claims regarding such party's intellectual property rights.

8.10. CONSTRUCTION. The Subscription Service and Professional Services shall be provided in the English language unless agreed otherwise. The parties confirm that they have requested that the Agreement and all related documents be drafted in English at the express wishes of the parties. Les parties ont exigé que le présent contrat et ServiceNow les documents connexes soient rédigés en anglais selon la volonté expresse des parties. Capitalized terms not defined herein shall have the meaning set forth or referenced in the Subscription Service Guide. Section headings are for convenience only and are not to be used in interpreting the Agreement.

SUBSCRIPTION SERVICE GUIDE

Capitalized terms not defined herein shall have the meaning set forth in the Express General Terms and Conditions or Subscription Service Agreement.

1. CUSTOMER OPERATION OF SUBSCRIPTION SERVICE

1.1. PASSWORDS AND USER NAMES. Customer shall: (a) protect the names and passwords of users of the Subscription Service and prevent and notify ServiceNow of unauthorized use of the Subscription Service; (b) appoint up to five (5) designated support contacts for purposes of contacting ServiceNow support regarding questions and/or technical issues ("***Authorized Customer Support Contacts***") and ensure that the Authorized Customer Support Contacts' information is current in the ServiceNow support portal; (c) be responsible for the lawfulness of, and results obtained from, all Customer Data submitted by users to the Subscription Service and each user's acts and omissions; and (d) use the Subscription Service only in accordance with the Documentation.

1.2. ACCESS CONTROL. ServiceNow provides the technical architecture that permits Customer to use and process Customer Data in the Subscription Service. This architecture includes an access control list engine. Customer shall be responsible for using the access control list engine for protecting all Personal Data. Customer shall ensure that access to and use of Subscription Service is restricted to only users authorized by Customer. Customer shall be responsible for ensuring all such users maintain the security of any passwords, usernames and other forms of authentication to the Subscription Service. A username and password must be uniquely assigned to a specific person and may not be shared by multiple persons at any one time or transferred. "***Personal Data***" means information identifying a natural person; an identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, financial, cultural or social identity.

2. SECURITY PROGRAM; EXCEPTIONS

ServiceNow shall maintain a security program ("***Security Program***") that includes industry standard practices designed to protect Customer Data from unauthorized access, use, disclosure, alteration, distribution and destruction. Notwithstanding anything to the contrary in this Agreement, the Security Program apply only to those systems, networks, network devices, facilities and components over which ServiceNow exercises control. The Security Program does not apply to: (i) information shared with ServiceNow that is not Customer Data; (ii) Customer Data in transit over the Internet, Customer's virtual private network (VPN), or another third party network; (iii) any Customer Data processed by Customer or its users in violation of this Agreement; or (iv) any part of the Subscription Service that is not hosted by ServiceNow.

3. UPGRADES

3.1. UPGRADES. "***Upgrades***" are ServiceNow's releases of the Subscription Service for repairs, enhancements or new features applied by ServiceNow to Customer's instances of the Subscription Service at no additional fee during the Subscription Term. ServiceNow has the discretion to provide new functionality either: (i) as an Upgrade, or (ii) as different software or service for a separate fee. ServiceNow determines whether and when to develop, release and apply any Upgrade to Customer's instances of the Subscription Service.

3.2. MAINTENANCE. ServiceNow shall use reasonable efforts to give Customer ten (10) days' notice of any service maintenance to the infrastructure network, hardware or software used by ServiceNow to operate and deliver the Subscription Service if ServiceNow, in its reasonable judgment, believes that such cloud infrastructure maintenance will impact Customer's use of its production instances of the Subscription Service. ServiceNow will use reasonable efforts to limit the Maintenance Time (as defined below) to no more than two (2) hours per month. Notwithstanding the foregoing, ServiceNow may provide Customer with a shorter or no notice period of service maintenance if necessary, in the reasonable judgment of ServiceNow, to maintain the availability, security, stability or performance of the Subscription Service.

4. SUPPORT

During the Subscription Term, ServiceNow shall use reasonable efforts to resolve Defects in the Subscription Service ("***Support***").

A "***Defect***" means a problem causing the Subscription Service to not conform to the Product Overview. Customer may request Support for a Defect at the online portal https://hi.service-now.com/ or any successor site.

A Defect will be assigned a priority level as follows:

- A Priority Level 1 Defect is any Defect that causes Customer's instance(s) of the Subscription Service to be not Available (as defined below).
- A Priority Level 2 Defect is any Defect that causes a mission critical function of the Subscription Service to fail.
- A Priority Level 3 Defect is any Defect that significantly impedes work or progress.
- A Priority Level 4 Defect is any Defect that does not significantly impede work or progress.

Upon notification by Customer of a Defect, ServiceNow shall, in all instances, target an initial response (the "***Initial Response***") within the timeframes set forth in the Support Table, as measured from the time that Customer notifies ServiceNow. The initial response from ServiceNow shall include, as applicable and without limitation: (i) ServiceNow's acknowledgment or notification to Customer of such Defect, and (ii) the classification of such Defect as a Priority Level 1, 2, 3 or 4.

SUPPORT TABLE

Priority Level	Target Initial Response
1	30 minutes; at all times
2	2 hours; at all times
3	Within 1 business day
4	Varies

Support does not include: implementation services; configuration services; integration services; customization services or other custom software development; support for modifications of the Subscription Service by any person other than ServiceNow or a person acting at ServiceNow's direction; training or "how-to"; assistance with administrative functions; professional services; corrections of immaterial Defects or Defects that have a viable workaround; or corrections that will degrade the Subscription Service.

5. SERVICE LEVEL OBJECTIVE

5.1. DEFINITIONS.

(a) "***Available***" means that the Subscription Service can be accessed by authorized users.

(b) "***Excused Downtime***": means (i) Maintenance Time of up to two (2) hours per month; and (ii) any time the Subscription Service is not Available due to circumstances beyond ServiceNow's control, including without limitation modifications of the Subscription Service by any person other than ServiceNow or a person acting at ServiceNow's direction, a Force Majeure Event, general Internet outages, failure of Customer's infrastructure or connectivity (including without limitation, direct connectivity and virtual private network (VPN) connectivity to the Subscription Service), computer and telecommunications failures and delays not within ServiceNow's control, and network intrusions or denial-of-service or other criminal attacks.

(c) "***Maintenance Time***" means the time the Subscription Service is not Available due to service maintenance.

(d) "***Availability Service Level Objective***" means the percentage of total time during which Customer's production instances of the Subscription Service are Available during a calendar month, excluding Excused Downtime.

5.2. AVAILABLITY. ServiceNow shall use reasonable efforts to provide an Availability Service Level Objective of 99.8% over any calendar month. There is no service credit offered for a failure to meet this Availability Service Level Objective.

SCHEDULE A

TERMS AND CONDITIONS TO VIRTRU PRO SUBSCRIPTION AGREEMENT

1. DEFINITIONS

For purposes of this Agreement, the following terms shall have the following meanings:

1.1 "**Derivative Work**" shall mean a new or modified work that is based on or derived from a preexisting work, including, without limitation, a work that, in the absence of a license, would infringe the copyright in such preexisting work or that uses trade secrets or other proprietary information with respect to such preexisting work.

1.2 "**Materials**" shall mean the Virtru Pro software (including any object code, executable files, or browser plug-ins) or materials related thereto provided by Virtru to Customer hereunder, including, without limitation, any software downloaded from Virtru's website or from the Virtru Pro Services; any related materials and documentation therefor; and any modifications, error corrections, bug fixes, new releases, enhanced functionality (including platform integration features not generally available to non-commercial users of Virtru's software) or other updates thereto that may be provided hereunder by Virtru to Customer during the term of this Agreement.

1.3 "**Third Party Services**" shall mean any services used in connection with the Materials that are hosted by a party other than Virtru or Licensee.

1.4 "**Virtru Pro Services**" shall mean the Virtru hosted services made available by Virtru to Customer in connection with the Materials.

2. RIGHTS IN MATERIALS AND TO USE SERVICE

2.1 Grant of Rights. Subject to the terms and conditions of this Agreement, Virtru (a) hereby grants to Customer a restricted, non-exclusive, nontransferable, nonsublicensable, royalty-free (except as set forth in Section 2.3), revocable right to use, during the term of this Agreement and in accordance with the documentation provided by Virtru, the Materials (the "**License**"), and (b) Virtru will make the Virtru Pro Services available to Customer pursuant to this Agreement during the term of this Agreement. Except as set forth in this Section 2.1, no other right or license of any kind is granted by Virtru to Customer hereunder with respect to the Materials or the Virtru Pro Services. Customer acknowledges and agrees that, unless otherwise agreed in writing between the parties, Customer shall be solely responsible for procuring and complying with any license or right to use any Third Party Services, including those offered by Customer's email services provider.

2.2 Restrictions. Customer shall not, without the prior written consent of Virtru: (a) copy all or any portion of the Materials or Virtru Pro Services; (b) decompile, disassemble, scrape or otherwise reverse engineer the Materials, Virtru Pro Services or any portion thereof, or determine or attempt to determine any source code, algorithms, methods or techniques embodied in the Materials or used in the Virtru Pro Services or any portion thereof; (c) modify, translate or create any Derivative Works based upon the Materials or Virtru Pro Services; (d) distribute, disclose, market, rent, lease, assign, sublicense, pledge or otherwise transfer the Materials, in whole or in part, to any third party or export the Materials outside the United States; (e) remove or alter any copyright, trademark, trade name or other proprietary notices, legends, symbols or labels appearing on or in copies of the Materials or the Virtru Pro Services; (f) perform, or release the results of, benchmark tests or other comparisons of the Materials or Virtru Pro Services with other programs or services; (g) transfer the Materials to any computer other than a computer owned by Customer and used by Customer in Customer's operations; (h) permit the Materials or Virtru Pro Services to be used for processing the data of any third party; (i) incorporate the Materials, Virtru Pro Services or any portion thereof into any other program, product or service, or use the Materials or Virtru Pro Services to provide similar services or functionality to third parties; (j) provide any third party with access to the Virtru Pro Services other than as expressly permitted herein or by the Terms of Service (as defined below); (k) use the Materials or Virtru Pro Services for any unlawful or tortious purpose; or (l) use the Materials or Virtru Pro Services for any purpose other than in accordance with the terms and conditions of this Agreement or Virtru's then-current terms of service (available at https://www.virtru.com/terms-of-service) (the "**Terms of Service**"). Customer shall ensure that all Customer end users of the Virtru Pro Service and Materials comply with

the terms and conditions of this Agreement. Customer shall be responsible for compliance with this Agreement by each Customer end user and it shall monitor and manage all Customer users in connection with this Agreement.

2.3 Fees; Payment. In consideration of the Virtru's provision of the Virtru Pro Services and Materials, Customer shall make payments to Virtru in accordance with the terms set forth on the cover page of this Agreement. Sales and use tax, VAT, or GST are Customer's sole responsibility, and Customer acknowledges and agrees that all fees are exclusive of all such taxes.

2.4 Seats; Reporting. Customer shall initially be permitted to use the Materials and Virtru Pro Services with respect to the number of seats set forth on the cover page of this Agreement (the "**Baseline Seat Count**"). Each seat shall be used by one Customer user. During the term of this Agreement, Customer will report to Virtru the total number of users of the Materials and Virtru Pro Services on an annual basis. Such report will be submitted to sales@virtru.com and shall be due thirty (30) days prior to each anniversary of the date of this Agreement (each, a "**Reporting Date**") based on the actual number of users as of the date thirty (30) days prior to such Reporting Date (each, a "**Seat Count Date**"). If the actual number of Customer users as of any Seat Count Date is higher than the Baseline Seat Count, Customer will pay the "Subscription Fee per Seat" set forth on the cover page of this Agreement (the "**Subscription Fee**") for each such additional user for any Renewal Term.

2.5 Adjustment Events. In addition to the annual reporting required under Section 2.4 above, Customer shall report to Virtru any increase of ten percent (10%) or more in the aggregate number of Customer users in excess of the Baseline Seat Count that occurs between Reporting Dates (an "**Adjustment Event**") and agrees to pay Virtru, within thirty (30) days following any such Adjustment Event, a prorated Subscription Fee for each such additional user for the remaining portion of the applicable term and for any Renewal Term.

2.6 Seat Count Audit. At any time during the term of this Agreement, Virtru shall have the right to audit Customer's usage of the Virtru Pro Services and Materials (a "**Seat Count Audit**"). If the actual number of Customer users as of the date of any Seat Count Audit is higher than the Baseline Seat Count, Customer will pay the "Subscription Fee per Seat" set forth on the cover page of this Agreement for the remaining portion of the applicable term and for any Renewal Term.

3. SUPPORT

Virtru will provide support to Customer and its end users through Virtru's generally available online ticketing and support system. Except as expressly provided in Schedule B, which is incorporated herein by reference, in this Section 3 or as may otherwise be provided under a written support agreement entered into by Virtru and Customer, Virtru is under no obligation to support the Materials or Virtru Pro Services in any way, nor to provide any modification, error correction, bug fix, new release or other update (each an "**Update**") to or for the Materials or Virtru Pro Service. In the event Virtru, in its sole discretion, supplies or makes available any Update to Customer, such Update shall be deemed to be part of the Materials or Virtru Pro Services (as applicable) hereunder and shall be subject to the terms and conditions of this Agreement.

4. PROPRIETARY RIGHTS

4.1 General. As between Virtru and Customer, Virtru retains all right, title and interest, including, without limitation, all patent rights, copyrights, trademarks and trade secrets, in and to the Materials, Virtru Pro Services and any portion thereof, including, without limitation, any copy or Derivative Work of the Materials, Virtru Pro Services or any portion thereof and any Update thereto. Customer agrees to take any action reasonably requested by Virtru to evidence, maintain, enforce or defend the foregoing. Customer shall not take any action to jeopardize, limit or interfere in any manner with Virtru's ownership of and rights with respect to the Materials, Virtru Pro Services or any Derivative Work or Update. Customer shall have only those rights in or to the Materials, Virtru Pro Services and any Derivative Work or Update granted to it pursuant to this Agreement.

4.2 Feedback. Customer and its authorized users may provide suggestions, requests, recommendations and other feedback concerning Customer's use of the Materials and Virtru Pro Services (including, without limitation, any errors or difficulties discovered with respect thereto) (the "**Feedback**"). Customer agrees that all Feedback shall be the sole

property of Virtru and Virtru may use such Feedback at its discretion without the consent of Customer.

5. PROPRIETARY INFORMATION

5.1 Proprietary Information. Both parties acknowledge that, in the course of this Agreement each may obtain confidential or proprietary information of the other party ("**Proprietary Information**"). "Proprietary Information" will include, without limitation, (a) the existence of and terms of this Agreement, (b) trade secrets, know-how, inventions (whether or not patentable), techniques, processes, programs (whether in source code or object code form), ideas, algorithms, formulas, schematics, testing procedures, software design and architecture, computer code, documentation, design and functional specifications, product requirements, problem reports, performance information, software documents, hardware, devices, designs, drawings, unpublished patent applications, data, plans, strategies and forecasts, and (c) technical, engineering, manufacturing, product, marketing, servicing, financial, personnel and other information. Virtru's "Proprietary Information" will include, without limitation, the Materials (including all Derivative Works and Updates) and all confidential information related thereto provided by Virtru to Customer in connection with this Agreement. Virtru's Proprietary Information shall, as between Customer and Virtru, belong solely to Virtru, and Customer's Proprietary Information shall, as between Customer and Virtru, belong solely to Customer.

5.2 Use and Disclosure Restrictions. Each party agrees (a) to protect the other party's Proprietary Information from unauthorized dissemination and use; (b) to use the other party's Proprietary Information only for the performance of this Agreement and the exercise of any rights under this Agreement; (c) not to disclose any Proprietary Information, or any part or parts thereof, to any of its employees, agents, contractors or any other individuals except to its employees who are under confidentiality obligations no less restrictive than the requirements of this Section 5; (d) with respect to Customer, not to disclose or otherwise provide to any third party, without the prior written consent of Virtru or as otherwise set forth in a separate written agreement between the parties hereto entered into after the date hereof, as applicable, any of Virtru's Proprietary Information, materials or any data or other information produced, obtained or created by Customer in connection with Customer's use of the Materials, including, without limitation, the existence of this Agreement and the existence and possible applications of the Materials; (e) to undertake whatever action is necessary (or authorize the other party to do so in the name of such party) to prevent or remedy any breach of such party's confidentiality obligations herein set forth or any other unauthorized disclosure of any Proprietary Information by its current or former employees, agents or contractors; and (f) not to remove or destroy any proprietary or confidential legends or markings placed upon or contained within the Proprietary Information provided to such party by the other party.

5.3 Exclusions. The foregoing restrictions on disclosure and use shall not apply with respect to any Proprietary Information that: (a) is or becomes publicly known through no act or omission of the other party; (b) was rightfully known by the receiving party without confidential or proprietary restriction before receipt from the other party, as evidenced by the receiving party's contemporaneous written records; (c) becomes rightfully known to the receiving party without confidential or proprietary restriction from a source other than the disclosing party that does not owe a duty of confidentiality with respect to such Proprietary Information; or (d) is independently developed without the use of the Proprietary Information as evidenced by the receiving party's written records. In addition, a party may use or disclose Proprietary Information to the extent (i) approved in writing by the other party and (ii) a party is legally compelled to disclose such Proprietary Information, provided, however, that prior to any such compelled disclosure, such party shall cooperate fully with the other party in protecting against any such disclosure and/or obtaining a protective order narrowing the scope of such disclosure and/or use of the Proprietary Information. Further, each party may disclose the terms and conditions of this Agreement: (A) in confidence, to legal counsel; (B) in confidence, to accountants, banks, and financing sources and their advisors; and (C) in connection with the enforcement of this Agreement or any rights hereunder.

5.4 Equitable Relief. Each party agrees that, due to the unique nature of the other party's Proprietary Information, the unauthorized disclosure or use of the other party's Proprietary Information or any other breach of any provision of this Section 5 will cause irreparable harm and significant injury to the other party, the extent of which will be difficult to ascertain and for which there will be no adequate remedy at law. Accordingly, each party agrees that the other party, in addition to any other available remedies, shall have the right to seek an immediate injunction and other equitable relief enjoining any breach or threatened breach of this Section 6 without the necessity of posting any bond or other security. Each party shall notify the other party in writing immediately upon becoming aware of any such breach or threatened breach.

6. NO WARRANTY

THE MATERIALS AND VIRTRU PRO SERVICES ARE PROVIDED "AS IS" AND VIRTRU DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS, WHETHER EXPRESS OR IMPLIED, RELATING TO THE MATERIALS AND VIRTRU PRO SERVICES, INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OF DESIGN, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NONINFRINGEMENT OF THIRD PARTY RIGHTS, OR WARRANTIES ARISING FROM A COURSE OF DEALING, COURSE OF PERFORMANCE, USAGE OR TRADE PRACTICE. VIRTRU DOES NOT GUARANTEE THE ACCURACY OF THE INFORMATION INCLUDED IN, TRANSMITTED THROUGH OR MADE AVAILABLE BY THE MATERIALS OR VIRTRU PRO SERVICES, WHICH MAY INCLUDE INACCURACIES OR ERRORS. VIRTRU DOES NOT GUARANTEE THAT THE MATERIALS OR VIRTRU PRO SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE, THAT BUGS OR MALFUNCTIONS WILL BE CORRECTED OR THAT THE MATERIALS, VIRTRU PRO SERVICES OR VIRTRU'S SERVERS ARE FREE OF HARMFUL COMPONENTS. VIRTRU DOES NOT GUARANTEE THAT THE MATERIALS OR VIRTRU PRO SERVICES ARE ACCURATE, WITHOUT ERROR OR RELIABLE.

7. VIRTRU'S ENTIRE LIABILITY

TO THE EXTENT ALLOWED BY APPLICABLE LAW AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY: (a) IN NO EVENT SHALL VIRTRU OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES FOR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF USE OR DATA, INADVERTENT DISCLOSURE OF DATA, OR INTERRUPTION OF BUSINESS, OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES OF ANY KIND OR OTHER ECONOMIC LOSS ARISING FROM OR RELATING TO THIS AGREEMENT OR THE SUBJECT HEREOF, EVEN IF VIRTRU HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, HOWEVER CAUSED, AND (b) NOTWITHSTANDING ANYTHING IN THIS AGREEMENT TO THE CONTRARY, VIRTRU'S ENTIRE LIABILITY ARISING FROM OR RELATING TO THIS AGREEMENT OR THE SUBJECT HEREOF, UNDER ANY LEGAL THEORY (WHETHER IN CONTRACT, TORT, INDEMNITY OR OTHERWISE), IF ANY, SHALL NOT EXCEED ONE THOUSAND DOLLARS (US$1,000).

8. INDEMNIFICATION

Customer shall defend, indemnify and hold Virtru harmless against any loss, liability, damage or cost (including reasonable attorneys' fees) in connection with claims, actions, demands, suits, or proceedings made or brought against Virtru by a third party alleging (a) that any modification or addition to the Materials or Virtru Pro Services made by or for Customer (other than by Virtru) infringes a copyright, mask work right, trade secret, trademark right or patent of the third party; (b) in combination with any other product or service not provided, specified or recommended in writing by Virtru for use with the Materials or Virtru Pro Services; or (b) with respect to the development, manufacture, marketing, sales, distribution or use of any of the Materials or Virtru Pro Services, including, without limitation, a product liability claim or a claim for breach of any warranty or support obligations. In connection with a claim under this Section 9, Virtru shall: (i) provide Customer with prompt notice of the claim; (ii) permit Customer to control the defense and any settlement of the claim (provided that Customer may not settle any claim unless such settlement unconditionally releases Virtru of all liability in connection with such claim); and (iii) provide cooperation as reasonably requested by Customer (at Customer's expense).

9. TERM AND TERMINATION

9.1 Term. This Agreement shall commence on the Effective Date and, unless sooner terminated pursuant to the terms hereof, shall continue in full force and effect for one (1) year (the "**Initial Term**"). Thereafter, this Agreement shall automatically renew for successive one (1) year periods (each a "**Renewal Term**"), unless either party provides the other party with written notice of its intent not to renew at least thirty (30) days prior to the end of the then-current term. The automatic renewal of this Agreement will be for the Baseline Seat Count, as adjusted pursuant to Sections 2.4, 2.5 and/or 2.6, on the same payment terms as set forth on the cover page of this Agreement.

9.2 Termination. Either party may terminate this Agreement immediately upon written notice to the other party if the other party fails to perform any of its duties or obligations hereunder and, except with respect to Customer's breach of Section 2.1 or 2.2, which breach shall not be subject to any cure period, fails to cure such default within thirty (30) days following receipt of written notice from the non-defaulting party specifying the occurrence or existence of the default. Customer shall notify Virtru within twenty-four (24) hours of Customer becoming aware of any breach (other than by Virtru) of the terms and conditions of this Agreement, including, without limitation, Sections 2 and 5.

9.3 Effect of Termination. Upon the expiration or termination of this Agreement, the rights granted to Customer hereunder shall terminate, Customer will cease all use of the Materials, return to Virtru or destroy the Materials in its possession, and, upon Virtru's request, so certify such actions to Virtru. Any costs

incurred in returning or destroying the Materials upon termination shall be borne by Customer. The provisions of Sections 2.2, 4.2, 5, 6, 7, 8, 9.3, and 10 shall survive the expiration or any termination of this Agreement. Termination of this Agreement by either party shall not act as a waiver of any breach of this Agreement and shall not act as a release of either party from any liability for breach of such party's obligations under this Agreement. Neither party shall be liable to the other for damages of any kind solely as a result of terminating this Agreement in accordance with its terms, and termination of this Agreement by a party shall be without prejudice to any other right or remedy of such party under this Agreement or applicable law.

10. GENERAL PROVISIONS

10.1 Notices. Any notice, request, demand or other communication required or permitted hereunder shall be in writing, shall reference this Agreement and shall be deemed to be properly given: (a) when delivered personally; (b) seven (7) days after having been sent by registered or certified mail, return receipt requested, postage prepaid; or (c) two (2) business days after deposit with a private industry express courier, with written confirmation of receipt. All notices shall be sent to the address set forth on the cover page of this Agreement and to the notice of the person executing this Agreement (or to such other address as may be designated by a party by giving written notice to the other party pursuant to this Section 10.1).

10.2 Assignment. This Agreement may not be assigned, in whole or part, whether voluntarily, by operation of law or otherwise, by Customer without the prior written consent of Virtru. Subject to the preceding sentence, the rights and liabilities of the parties hereto shall bind, and inure to the benefit of, their respective assignees and successors and is binding on the parties and their successors and assigns. Any attempted assignment other than in accordance with this Section 10.2 shall be null and void.

10.3 Governing Law, Jurisdiction and Venue. This Agreement is to be construed in accordance with and governed by the internal laws of the Commonwealth of Virginia (but expressly excluding the Uniform Computer Information Transactions Act ("**UCITA**") as enacted in Virginia) without giving effect to any choice of law rule that would cause the application of the laws of any jurisdiction other than the internal laws of the Commonwealth of Virginia (excluding UCITA) to the rights and duties of the parties. Any legal suit, action or proceeding arising out of or relating to this Agreement shall be commenced in a federal court in the Eastern District of Virginia or in state courts with jurisdiction over Fairfax County, Virginia, and each party hereto irrevocably submits to the exclusive jurisdiction and venue of any such court in any such suit, action or proceeding.

10.4 Attorneys' Fees. If any legal action, including, without limitation, an action for arbitration or injunctive relief, is brought relating to this Agreement or the breach hereof, the prevailing party in any final judgment or arbitration award, or the non-dismissing party in the event of a dismissal without prejudice, shall be entitled to the full amount of all reasonable expenses, including all court costs, arbitration fees and actual attorneys' fees paid or incurred in good faith.

10.5 Waiver. The waiver by either party of a breach of or a default under any provision of this Agreement, shall be in writing and shall not be construed as a waiver of any subsequent breach of or default under the same or any other provision of this Agreement, nor shall any delay or omission on the part of either party to exercise or avail itself of any right or remedy that it has or may have hereunder operate as a waiver of any right or remedy.

10.6 Severability. If the application of any provision of this Agreement to any particular facts or circumstances shall be held to be invalid or unenforceable by an arbitration panel or a court of competent jurisdiction, then (a) the validity and enforceability of such provision as applied to any other particular facts or circumstances and the validity of other provisions of this Agreement shall not in any way be affected or impaired thereby and (b) such provision shall be enforced to the maximum extent possible so as to effect the intent of the parties and reformed without further action by the parties to the extent necessary to make such provision valid and enforceable.

10.7 Relationship of the Parties. Nothing contained in this Agreement shall be deemed or construed as creating a joint venture, partnership, agency, employment or fiduciary relationship between the parties. Neither party nor its agents have any authority of any kind to bind the other party in any respect whatsoever, and the relationship of the parties is, and at all times shall continue to be, that of independent contractors.

10.8 Restricted Rights. If Customer is an agency or instrumentality of the United States Government, the Materials are "commercial computer software" and "commercial computer software documentation," and, pursuant to FAR 12.212 or DFARS 227.7202, and their successors, as applicable, use reproduction and disclosure of the Materials are governed by the terms of this Agreement.

10.9 Reference. Customer agrees to serve as a "reference customer" that may be disclosed by Virtru to third parties (including by displaying Customer's name, logo and/or a link to Customer's web site on Virtru's web site) and, upon reasonable notice from Virtru, shall serve as a reference to potential customers, vendors, investors, or other third parties designated by Virtru; provided, however, that Virtru shall provide Customer with reasonable prior notice of its need to have Customer serve as a reference.

10.10 Entire Agreement. This Agreement, any Schedules and any Exhibits attached hereto and incorporated herein by reference, and the Terms of Service constitute the entire agreement between the parties concerning the subject matter hereof and supersede all prior or contemporaneous representations, discussions, proposals, negotiations, conditions, agreements and communications, whether oral or written, between the parties relating to the subject matter of this Agreement and all past courses of dealing or industry custom. No amendment or modification of any provision of this Agreement shall be effective unless in writing and signed by a duly authorized signatory of each of Virtru and Customer.

10.11 Counterparts and Electronic Signatures. The Parties may execute this Agreement in counterparts, each of which is deemed an original, but all of which together constitute one and the same agreement. This Agreement may be delivered electronically or by facsimile transmission, and the parties hereby agree that any electronic or facsimile signatures hereto are legal, valid and enforceable as originals.

SCHEDULE B

MAINTENANCE AND SUPPORT SERVICES SCHEDULE

1. DEFINITIONS

For purposes of this Schedule, the following term shall have the following meaning:

(a) "**Support Services**" means the delivery of front-end support to Customer's end users by telephone, email or other methods and the training of Customer's end users, in each case relating to the use of the Materials and Virtru Pro Services.

2. SUPPORT SERVICES.

Virtru will be responsible for providing Customer's end users with Support Services. Virtru will not be required to provide the Support Services if Customer has failed to pay any amount payable to Virtru under this Agreement and such amount is more than thirty (30) days overdue.

3. UPDATES.

Virtru will provide Customer with one copy of each Update made generally available by Virtru to its customers that pay for customer support and maintenance during the term of this Agreement.

4. SUPPORT HOURS.

Virtru will provide the Support Services during Virtru's normal business hours, Monday to Friday, except holidays. Virtru will respond to Customer support inquiries or requests within one business day.

vCloud Air (U.S. and Japan Data Centers)

TERMS OF SERVICE

Last updated: November 5, 2014

VMware vCloud Air is an infrastructure as a service offering. By accessing any service offered through VMware vCloud Air (the " **Service Offering**") you agree to be bound by these terms of service between you and VMware (" **Agreement**"). If you do not agree to this Agreement, you must not access the Service Offering. An individual accepting this Agreement on behalf of an organization represents and warrants having legal authority to bind that organization. " **You**" means the entity accepting this Agreement. " **VMware**," " **we**," or " **us**" means VMware, Inc., a Delaware corporation, to the extent that you are purchasing the Service Offering in the United States, VMware vCloud Service G.K., a company organized and existing under the laws of Japan, to the extent that you are purchasing the Service Offering in Japan, and VMware International Limited, a company organized and existing under the laws of Ireland, to the extent that you are purchasing the Service Offering elsewhere. Capitalized terms used in this Agreement are defined throughout this Agreement and in Section 14.

EVALUATION PROGRAM USE. When you access the Service Offering under a VMware evaluation program, you may use the Service Offering only for non-production computing activity. Notwithstanding any other provision in this Agreement, under a VMware evaluation program, we provide the Service Offering "AS-IS" without indemnification, support or warranty of any kind, expressed or implied, and we will not be liable for any damages. Upon termination of the evaluation, you will no longer have access to the Service Offering and Your Content.

1. The Service Offering.

1.1 Generally. This Agreement governs your access and use of the Service Offering. We may deliver the Service Offering to you with the assistance of our affiliates, licensors and providers. Service Level Agreements may apply to the Service Offering. You will comply with all laws, rules and regulations applicable to your use of the Service Offering, and with the Third Party Terms, the Service Description, the Privacy Addendum, and the Support Policy, all of which are incorporated herein by reference.

1.2 Access to the Service Offering. You may access and use the Service Offering solely for your own benefit and only in accordance with this Agreement. To access the Service Offering, you must register for the Service Offering and set up an authorized account with Login Credentials. You may monitor and manage your Service Offering account via the My VMware Portal available at www.vmware.com/accounts and through the Service Offering Portal available at http://vcloud.vmware.com. You must keep confidential your Login Credentials. If you set up an authorized account for an organization, you will require that all authorized users of that account (including anyone providing services to you) keep confidential their Login Credentials. You will keep your registration information accurate, complete and current as long as you use the Service Offering. You are responsible for any use that occurs under your Login Credentials, including any activities by you, or your employees, contractors or agents. If you believe an unauthorized user has gained access to your Login Credentials, you will notify us as soon as possible. Neither we nor our affiliates are responsible for any unauthorized access to or use of your account.

1.3 Verifying; Cooperation. We have the right to verify your compliance with this Agreement. If we

seek to verify that compliance, you will provide information or other materials reasonably requested by us to assist the verification. We monitor the overall performance and stability of the infrastructure of the Service Offering. You may not block or interfere with that monitoring. If we reasonably believe a problem with the Service Offering may be attributable to Your Content or your use of the Service Offering, you will cooperate with us to identify and resolve the source of that problem.

1.4 Additional Terms; Third Party Content. As part of your use of the Service Offering, you may receive access to additional data, content, software or applications subject to separate terms. If so, those separate terms will prevail over this Agreement as to your use of that data, content, software or applications. Third Party Content is available "AS IS" without indemnification or support, and we disclaim all express and implied warranties (including warranties of merchantability, fitness for a particular purpose, and non-infringement). You are responsible for reviewing, accepting, and complying with any third party terms of use or other restrictions applicable to the Third Party Content. Those terms will be available to you through a notification within the Service Offering or in a document available at https://www.vmware.com/files/pdf/support/vmware-vcloud-air-third-party-terms.pdf. It is your responsibility to check the Third Party Terms, which may be modified from time to time. We may provide billing and related services associated with the Third Party Content. We will not provide any support for the Third Party Content unless otherwise noted in the Third Party Terms. We reserve the right to suspend or terminate the Third Party Content at any time, but we will use commercially reasonable efforts to provide reasonable notice of that suspension or termination.

1.5 Early Evaluation/Beta Features. We may identify and make available on an early evaluation or beta basis certain features or functionality within the Service Offering. You must use these features or functionality only for evaluation purposes and for the period that we specify. We provide these features and functions "AS-IS," without indemnification or support and disclaim all express and implied warranties (including warranties of merchantability, fitness for a particular purpose, and non-infringement). Any early evaluation or beta features or functionality do not constitute an implied commitment to offer to you or anyone these features and functionality as part of the Service Offering on a generally available basis.

1.6 Open Source Software. You may receive open source software when you use the Service Offering and any open source software distributed to you is made available under the applicable open source license, which can be found at: http://www.vmware.com/download/open_source.html. You may obtain a copy of these licenses and any source code (and modifications) that we are required to make available under these licenses (the " **Source Files**") at http://www.vmware.com/download/open_source.html or by sending a written request, with your name and address to: VMware, Inc., 3401 Hillview Avenue, Palo Alto, CA 94304, United States of America. All written requests must clearly specify: Open Source Files Request, Attention: General Counsel. This offer to obtain a copy of the Source Files is valid for three years from the date you last received open source software as part of the Service Offering or last accessed the Service Offering.

2. Data Protection and Security.

2.1 Data Protection. We will process personal data contained in Your Content as set forth in the Privacy Addendum.

2.2 Your Content and Security. You are solely responsible for Your Content. You are responsible for protecting the security of Your Content, including any access you might provide to Your Content by your employees, customers or other third parties, and in transit to and from the Service Offering. The Service Offering provides you with certain software and functionality to help you protect Your Content from unauthorized access. You will take and maintain appropriate security, protection and backup of Your Content, which might include the use of encryption technology to protect Your Content from unauthorized access. You are responsible for providing any necessary notices to your

users and obtaining any legally-required consents from your users concerning their use of the Service Offering. You are solely responsible for complying with any laws or regulations that might apply to Your Content. You are responsible for any losses or other consequences arising from your failure to encrypt or back up Your Content.

3. Acceptable Use.

3.1 General Restrictions. You and those accessing the Service Offering through you may not: (a) resell or sublicense the Service Offering; or (b) use or access the Service Offering: (i) in a way prohibited by law, regulation, governmental order or decree; (ii) to violate any rights of others; (iii) to try to gain unauthorized access to, test the vulnerability of, or disrupt the Service Offering or any other service, device, data, account or network; (iv) to spam or distribute malware; (v) in a way that could harm the Service Offering or impair anyone else's use of it; (vi) in a way intended to work around the Service Offering's technical limitations, recurring fees or usage limits; or (vii) in any application or situation where failure of the Service Offering could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage. You must ensure that your users comply with the terms of this Agreement, and you agree that if you become aware of any violation by one of your users, you will terminate that user's access to Your Content immediately. If we have reason to believe that you or your users have breached this Agreement, we or our designated representative may review your use of the Service Offering, including your account, Your Content, and your records, to verify your compliance with this Agreement.

3.2 Content Restrictions. You will take steps to ensure that those accessing any service you provide with the Service Offering do not post content that: (a) may create a risk of harm, loss, physical or mental injury, emotional distress, death, disability, disfigurement, or physical or mental illness to anyone; (b) may create a risk of any other loss or damage to any person or property; (c) may constitute or contribute to a crime or tort; (d) contains any information or content that is illegal, unlawful, harmful, abusive, pornographic, racially or ethnically offensive, defamatory, infringing, invasive of personal privacy or publicity rights, harassing, humiliating to other people (publicly or otherwise), libelous, threatening, or otherwise objectionable; or (e) contains any information or content that you do not have a right to make available under any law or under contractual or fiduciary relationships. You are solely responsible for any software, product or service that a third party licenses, sells or makes available to you that you install or use with the Service Offering. Your use of that software, product or service is governed by separate terms between you and that third party. We are not a party to and are not bound by any of those separate terms. You represent and warrant that Your Content does not and will not violate any third-party rights, including any Intellectual Property Rights, and rights of publicity and privacy. You will ensure that your use of the Service Offering complies at all times with your privacy policies and all applicable laws and regulations, including any encryption requirements.

3.3 Violations of Acceptable Use. If you become aware that any of Your Content or your user's use of Your Content violates Section 3.1 or 3.2, you will take immediate action to remove the applicable part of Your Content or suspend the end user's access. If you fail to do so, we may ask you to do so. If you fail to comply with our request within twenty-four hours, we may suspend your account or disable access to Your Content until you comply with our request.

3.4 Notification of Infringement Concerns. If you believe that your copyrighted work has been copied and is accessible on our Service Offering in a way that constitutes copyright infringement, please send a notice to us as further detailed in Section 8 of the Community Terms of Use available at http://www.vmware.com/community_terms.html.

4. IP Ownership.

4.1 Ownership of Service Offering. We and our licensors own and retain all right, title and interest in and to the Service Offering and any related VMware Software, including all improvements, enhancements, modifications and derivative works thereof, and all Intellectual Property Rights therein. This includes any information that we collect and analyze in connection with the Service Offering, such as usage patterns, user feedback and other information to improve and evolve our software products and services offerings. Your rights to use the Service Offering are limited to those expressly granted in this Agreement. No other rights with respect to the Service Offering, any related VMware Software, or any related Intellectual Property Rights are implied.

4.2 Ownership of Your Content. You and your authorized users retain all right, title and interest in and to Your Content and all Intellectual Property Rights therein. Our rights to access and use Your Content are limited to those expressly granted in this Agreement. No other rights with respect to Your Content or any related Intellectual Property Rights are implied.

4.3. Feedback. We will be free to use for any purpose any feedback (such as comments or suggestions) that you provide to us regarding the Service Offering. You hereby grant to us a non-exclusive, perpetual, irrevocable, royalty-free, transferable, worldwide right and license, with the right to sublicense, to use, reproduce, perform, display, disclose, distribute, modify, prepare derivative works of and otherwise exploit the feedback without restriction in any manner now known or in the future conceived and to make, use, sell, offer to sell, import and export any product or service that incorporates the feedback.

5. Order, Delivery, Payment, and Taxes.

5.1 Generally. Sections 5.3 (Direct Orders), 5.4 (Delivery), 5.5 (Invoicing and Payment Terms) and 5.6 (Taxes) apply only to orders you place directly with, and the Service Offering you purchase directly from, VMware. When ordering through, or purchasing the Service Offering from, a VMware authorized reseller, the authorized reseller might specify similar terms.

5.2 Orders. All Orders issued to VMware are subject to the terms of this Agreement and are not binding until accepted by VMware. We are not required to provide any Service Offering to you until you provide all information we require for processing your Order.

5.3 Direct Orders. For orders placed directly with VMware, you must issue a purchase order to VMware for the initial Service Offering order, but a purchase order is not required for the monthly billings that occur after the initial Order billing. For subsequent billings, all fees (including subscription renewals, metered usage components, and other add-ons) will be paid in accordance with this Agreement. Your Order will be deemed accepted when we authorize the purchased Service Offering for your Login Credentials.

5.4 Delivery. When VMware accepts your Order for the Service Offering, we will deliver the corresponding Login Credentials to you by email to the address associated with your account. If VMware ships a physical object in connection with an add-on feature of the Service Offering, shipping and delivery terms are Ex Works VMware's regional fulfillment facility (INCOTERMS 2010).

5.5 Invoicing and Payment Terms. You will pay all fees for use of the Service Offering in the amount and currency specified in your invoice, within 30 days after the date of the invoice, and regardless of your usage level during a billing period. You will also be responsible for all additional fees for any subscription renewals and metered usage components consumed, and other subscriptions, features, products, services or add-ons that you purchase within the Service Offering. You will be billed in advance for the monthly or prepaid charges due to the subscription services purchased. Any metered usage components and any initial monthly fees will be billed in arrears. The applicable fees for subscriptions (including renewals), features and other available products and

services will be governed by the then-current applicable price list at the time the initial, renewal, or add-on order is submitted, or as otherwise agreed. We may increase or add new fees for the Service Offering by notifying you at least 30 days in advance.

5.6 Taxes. Service Offering fees are exclusive of taxes, and you shall pay or reimburse for all taxes arising out of transactions contemplated by this Agreement. If you are required to pay or withhold any tax for payments due under this Agreement, you shall gross your payments to us so we receive sums due in full and free of any deductions. You will provide documentation to us showing that taxes have been paid to the relevant taxing authority. " **Taxes**" means any sales, VAT, use, gross receipts, business and occupation, and other taxes (other than taxes on our income), export and import fees, customs duties and similar charges imposed by any government or other authority. You hereby confirm that we can rely on the name and address you provide to us when you agree to the Service Offering or in connection with your payment method as being the place of supply for sales tax and income tax purposes or as being the place of supply for VAT purposes where you have established your business.

6. Temporary Suspension.

6.1 Generally. Upon prior written notice to you, we may suspend your use of the Service Offering if we reasonably determine: (a) payment for the Service Offering is not received within 30 days from the date on which payment is due; (b) you or your use of the Service Offering is in breach of this Agreement; (c) you fail to address our request to take action as specified in Section 3.3; (d) your use of the Service Offering poses a security risk to the Service Offering or other users of the Service Offering; or (e) suspension is required pursuant to our receipt of a subpoena, court order, or other request by a law enforcement agency.

6.2 Effect of Suspension. You will remain responsible for all fees incurred before or during the suspension. You will not be entitled to any service credits under the Service Level Agreement that you might have otherwise accrued during the period of suspension.

7. Term and Termination.

7.1 Term of Agreement. This Agreement will be in effect through the Subscription Term, plus any renewals, unless terminated earlier as permitted under this Agreement or the Service Description. Upon the completion of the Subscription Term, the subscription will automatically renew as specified in the Service Description, unless terminated as permitted under the Service Description.

7.2 Termination for Cause. We may terminate this Agreement effective immediately upon sending you an email notice if: (a) you breach any provision in Sections 3.1 or 3.2; (b) you do not resolve the underlying cause resulting in a suspension of your account pursuant to Section 6.1 (other than suspension due to a subpoena, court order, or other request by a law enforcement agency) within 10 days after your account is suspended; or (c) you commit a material breach that cannot be cured.

7.3 Termination for Insolvency. We may terminate this Agreement effective immediately upon sending you an email notice if you: (a) terminate or suspend your business; (b) become insolvent, admit in writing your inability to pay your debts as they mature, make an assignment for the benefit of creditors; or (c) become subject to control of a trustee, receiver or similar authority or any bankruptcy or insolvency proceeding.

7.4 Effect of Termination. Upon the termination of this Agreement for any reason: (a) all rights granted to you under this Agreement, including your ability to access the Service Offering, will immediately terminate; and (b) you must promptly discontinue all use of the Service Offering and delete or destroy any of our Confidential Information. We will retain Your Content for a period of 30

days following the effective date of the termination, although you will cease to have access to the Service Offering or Your Content during this period. After the 30 days, Your Content will be deleted. Sections 1.6 (Open Source Software), 3 (Acceptable Use) 4 (IP Ownership), 5 (Order, Delivery, Payment and Taxes), 7 (Term and Termination), 9 (Disclaimer), 11 (Limitation of Liability), 12 (Confidential Information), 13 (General), and 14 (Definitions), will survive the termination of this Agreement. Termination of the Service Offering (except to the extent that the termination is permitted under Section 13.3 of this Agreement or Section 3.6 of the Service Description) will not entitle you to any refunds, credits, or exchanges, and you will be liable for all monthly billing fees for the remainder of the Subscription Term after termination, as well as all usage and other fees incurred up to the termination date.

8. Support and Subscription Services. When applicable, and subject to the terms of this Agreement, we will provide to you support for the Service Offering in accordance with the terms specified in the Support Policy. We will not provide support to any end users of Your Content.

9. Disclaimer. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, WE AND OUR LICENSORS AND SERVICE PROVIDERS DISCLAIM ALL WARRANTIES, WHETHER EXPRESS, IMPLIED, OR STATUTORY, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT AND ANY WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE REGARDING OR RELATING TO THE SERVICE OFFERING OR ANY MATERIALS OR SERVICES FURNISHED OR PROVIDED TO YOU UNDER THIS AGREEMENT. WE AND OUR LICENSORS AND SERVICE PROVIDERS DO NOT WARRANT THAT THE SERVICE OFFERING WILL BE UNINTERRUPTED OR FREE FROM DEFECTS, OR THAT THE SERVICE OFFERING WILL MEET (OR IS DESIGNED TO MEET) YOUR BUSINESS REQUIREMENTS.

10. Indemnification.

10.1 Indemnification by Customer. You will defend and indemnify us against any third party claim arising from or relating to: (a) Your Content; (b) any infringement or misappropriation of any Intellectual Property Rights by you, your customers, your end users or your suppliers; (c) violation of law by you; (d) your use of the Service Offering (including any activities under your account and any use by your employees, personnel or end users) in violation of this Agreement, or (e) your use of any Third Party Content. We will (a) provide you with notice of the claim within a reasonable period of time after learning of the claim; and (b) reasonably cooperate in response to your requests for assistance. You may not settle or compromise any indemnified claim without our prior written consent.

10.2 Defense and Indemnification. Subject to the remainder of this Section 10, we will defend you against an Infringement Claim and indemnify you from the resulting costs and damages finally awarded against you to that third party by a court of competent jurisdiction or agreed to in settlement. You will (a) provide us with notice of any Infringement Claim within a reasonable period of time after learning of it; (b) allow us sole control over the claim's defense and settlement; and (c) reasonably cooperate in response to our requests for assistance. You may not settle or compromise any Infringement Claim without our prior written consent.

10.3 Remedies. If the Service Offering becomes, or in our opinion is likely to become, the subject of an Infringement Claim, we will at our option and expense either: (a) procure the rights necessary for you to keep using the Service Offering; (b) modify or replace the Service Offering to make it non-infringing; or (c) terminate this Agreement and refund any pre-paid fees for the Service Offering pro-rated for its remaining Subscription Term.

10.4 Exclusions. We will have no obligation under this Section 10 or otherwise with respect to any

claim based on: (a) a combination of VMware Software with non-VMware products or content, including Your Content; (b) use of the Service Offering for a purpose or in a manner not specified in this Agreement or the Service Description; (c) any modification to the Service Offering made without our express written approval; or (d) any Service Offering provided on a no charge basis. This Section 10 states your exclusive remedy for any infringement actions or claims.

11. Limitation of Liability.

11.1 Generally. TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT WILL WE OR OUR LICENSORS OR SERVICE PROVIDERS BE LIABLE FOR ANY LOST PROFITS OR BUSINESS OPPORTUNITIES, LOSS OF USE OF THE SERVICE OFFERING, LOSS OF REVENUE, LOSS OF GOODWILL, BUSINESS INTERRUPTION, LOSS OF DATA, OR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES UNDER ANY THEORY OF LIABILITY, WHETHER BASED IN CONTRACT, TORT, NEGLIGENCE, PRODUCT LIABILITY, OR OTHERWISE. IN ADDITION, OUR AND OUR LICENSORS' AND SERVICE PROVIDERS' LIABILITY UNDER THIS AGREEMENT WILL NOT, IN ANY EVENT, REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE, EXCEED THE GREATER OF: (A) THE AGGREGATE FEES PAID OR PAYABLE TO US FOR YOUR ACCESS TO AND USE OF THE SERVICE OFFERING IN THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO YOUR CLAIM, OR (B) $5,000 USD (OR THE EQUIVALENT IN LOCAL CURRENCY). REGARDLESS OF WHETHER WE OR OUR LICENSORS OR SERVICE PROVIDERS HAVE BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES AND REGARDLESS OF WHETHER ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE. THESE LIMITATIONS OF LIABILITY IN THIS SECTION 11.1 WILL NOT APPLY TO (A) VMWARE'S INDEMNIFICATION OBLIGATIONS UNDER THIS AGREEMENT OR (B) ANY LIABILITY WHICH MAY NOT BE EXCLUDED BY APPLICABLE LAW.

11.2 Further Limitations. Our licensors and service providers will have no liability of any kind under this Agreement. You may not bring a claim under this Agreement more than eighteen (18) months after the cause of action arises.

12. Confidential Information.

12.1 Protection. A party may use Confidential Information of the other party solely to exercise its rights and perform its obligations under this Agreement or as otherwise permitted under this Agreement. Each party will disclose the Confidential Information of the other party only to the employees, service providers or contractors of the recipient party who have a need to know the Confidential Information for purposes of this Agreement and who are under a duty of confidentiality no less restrictive than each party's duty hereunder. Each party will use reasonable care to protect the confidentiality of the other party's Confidential Information.

12.2 Exceptions. The recipient's obligations under Section 12.1 with respect to any Confidential Information will terminate if the recipient can show by written records that the information: (a) was already known to the recipient at the time of disclosure by the other party; (b) was disclosed to the recipient by a third party who had the right to make the disclosure without any confidentiality restrictions; (c) is, or through no fault of the recipient has become, generally available to the public; or (d) was independently developed by the recipient without access to, or use of, discloser's Confidential Information. The recipient may disclose Confidential Information to the extent the disclosure is required by law or regulation. The recipient will provide the other party notice, when practicable, and will take reasonable steps to contest and limit the scope of any required disclosure.

13. General.

13.1 Assignment. You may not assign or transfer this Agreement, in whole or in part, by operation of law or otherwise, without our prior written consent. Any attempted assignment or transfer without that consent will be void. Subject to these limits, this Agreement will bind and inure to the benefit of the parties and their respective successors and assigns.

13.2 Notices. Any notice delivered by us to you under this Agreement will be delivered by email to the email address associated with your account or by posting on either the Service Offering Portal or the My VMware Portal, except as otherwise set forth in this Agreement. Please direct legal notices or other correspondence to VMware, Inc., 3401 Hillview Avenue, Palo Alto, California 94304, United States of America, Attention: Legal Department.

13.3 Modifications. We may change periodically the Service Offering, the terms of your access to the Service Offering, this Agreement, the Service Description, the Privacy Addendum, the Third Party Terms, the Service Level Agreement, or the Support Policy. It is your responsibility to regularly check the Service Offering console and the My VMware portal for updates. We will notify you of any material, detrimental change to this Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy. The modified Agreement, Service Description, Privacy Addendum, Service Level Agreement, or Support Policy, as applicable, will become effective as of the date stated in that notification. If we make a material, detrimental change to the Service Offering (other than the termination or modification of any beta feature or functionality), this Agreement, the Service Description, the Privacy Addendum, the Service Level Agreement, or the Support Policy, then you may terminate this Agreement within 30 days of the change to the Service Offering or within 30 days of the notification. In that event, the termination will be effective as of the date we receive your notification, unless you state an effective date in your notification that is within 45 days after we receive your notification. In the event of that termination, we will refund any prepaid fees, pro-rated for the remainder of your Subscription Term, and less any discounts that would then not be earned. Your continued use of the Service Offering after the effective date of any modification to the Agreement, the Service Description, the Privacy Addendum, the Third Party Terms, the Service Level Agreement, or the Support Policy will be deemed acceptance of the modified terms, as applicable.

13.4 Waiver. The waiver of a breach of any provision of this Agreement will not constitute a waiver of any other provision or any later breach.

13.5 Severability. If any provision of this Agreement is held to be invalid or unenforceable, the provision will be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remaining provisions of this Agreement will remain in force.

13.6 Compliance with Laws; Export Control. Each party will comply with all laws applicable to the actions contemplated by this Agreement. You acknowledge that the Service Offering is of United States origin, is provided subject to the U.S. Export Administration Regulations (including "deemed export" and "deemed re-export" regulations), and may be subject to the export control laws of the applicable territory. You represent and warrant that (a) you are not, and are not acting on behalf of, (1) any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States has prohibited export transactions; or (2) any person or entity listed on the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, or the U.S. Commerce Department Denied Persons List or Entity List; (b) you will not permit the Service Offering to be used for any purposes prohibited by law, including any prohibited development, design, manufacture or production of missiles or nuclear, chemical or biological weapons; (c) Your Content will not be classified or listed on the United States Munitions list, contain defense articles, defense services or contain ITAR-related data; (d) Your Content will not require an export license and is not restricted from export to any VMware global resource or personnel under applicable export control laws; and (e) you are not subject, either directly or indirectly, to any order

issued by any agency of the United States government, revoking or denying, in whole or in part, your United States export privileges. You will notify VMware immediately if you become subject to any such order.

13.7 Government Regulations. For purposes of sales to government entities in the U.S.: The Service Offering and its documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFARS Section 227.7202 and FAR Paragraph 12.212(b), as applicable. Any use, modification, reproduction, release, performing, displaying or disclosing of the Service Offering and documentation by or on behalf of the U.S. Government will be governed solely by the terms and conditions of this Agreement.

13.8 Force Majeure. We will not be liable for any delay or failure to perform any obligations under this Agreement due to any cause beyond our reasonable control, including acts of God, labor disputes or other industrial disturbances, systemic electrical, telecommunications or other utility failures, earthquakes, storms or other elements of nature, blockages, embargoes, riots, acts or orders of government, acts of terrorism or war.

13.9 Construction. The headings of sections of this Agreement are for convenience and are not for use in interpreting this Agreement. As used in this Agreement, the word 'including' means "including but not limited to."

13.10 Governing Law. This Agreement is governed by the laws of the State of California, United States of America (excluding its conflict of law rules), except as follows: To the extent that you choose a Japan data center Service Offering, then this Agreement is governed by the laws of Japan (excluding its conflict of law rules). The United Nations Convention for the International Sale of Goods does not apply.

13.11 Third Party Rights. Other than as expressly set out in this Agreement, this Agreement does not create any rights for any person who is not a party to it, and no person who is not a party to this Agreement may enforce any of its terms or rely on any exclusion or limitation contained in it.

13.12 Order of Precedence. The terms of this Agreement will supersede and control over any conflicting or additional terms and conditions of any other purchasing related document issued by you.

13.13 Entire Agreement. This Agreement, as may be revised by us, is the entire agreement of the parties regarding its subject matter. This Agreement supersedes all prior or contemporaneous communications, understandings and agreements, whether written or oral, between the parties regarding its subject matter.

14. Definitions.

14.1 "Confidential Information" means non-public technical, business or other information or materials disclosed or otherwise made available by one party that are in tangible form and labeled "confidential" or the like, or, information which is provided under circumstances reasonably indicating their confidentiality. Our Confidential Information includes: (1) Login Credentials; and (2) any information or materials relating to the Service Offering.

14.2 "Infringement Claim" means any third party claim that any VMware Software used to provide the Service Offering infringes any patent, trademark or copyright of the third party, or misappropriates a trade secret (but only to the extent that the misappropriation is not a result of your actions) under the laws of: (a) the United States; (b) Canada; (c) the European Economic Area; (d) Australia; (e) New Zealand; (f) Japan; or (g) the People's Republic of China, to the extent that those

countries are part of your places of use of the Service Offering.

14.3 "Intellectual Property Rights" means all worldwide intellectual property rights, including copyrights, trademarks, service marks, trade secrets, patents, patent applications, and moral rights, whether registered or unregistered.

14.4 "Login Credentials" mean any passwords, authentication keys or security credentials that enable your access to and management of the Service Offering.

14.5 "Order" means the internet order page, order document, purchase order, or purchase agreement issued to VMware that specifies your purchase of the Service Offering.

14.6 "Privacy Addendum" means the then-current version of the Service Offering Data Privacy Addendum document available at http://vcloud.vmware.com/legal, which we may modify from time to time.

14.7 "Service Description" means the then-current Service Offering Service Description document available at https://www.vmware.com/files/pdf/vcloud-air/vcloud-air-Service-Description.pdf, which contains technical and other information and which we may modify from time to time.

14.8 "Service Level Agreement" means the then-current Service Level Agreement document available at https://www.vmware.com/support/vcloud-air/sla.html, which we may modify from time to time.

14.9 "Subscription Term" means the time period of your access to the Service Offering, as specified by your Order.

14.10 "Support Policy" means the then-current version of the Service Offering Support Policy document available at http://www.vmware.com/support/services/iaas-production.html, which we may modify from time to time.

14.11 "Third Party Content" means third party data, service, content, software or applications, including open source software.

14.12 "Third Party Terms" means the then-current version of the third party license terms applicable to the Service Offering that are available at https://www.vmware.com/files/pdf/support/vmware-vcloud-air-third-party-terms.pdf, which we may modify from time to time.

14.14 "VMware Software" means the software programs listed in our commercial price list.

14.15 "Your Content" means any and all applications, files, information, data or other content uploaded to or published or displayed through the Service Offering by you, your users, us (acting upon your instructions as part of a service), or any third party users who access any service you provide with the Service Offering.

STATE OF UTAH COOPERATIVE CONTRACT AMENDMENT

AMENDMENT #: 4

CONTRACT #: AR2472

Starting Date: Unchanged

Expiration Date: Unchanged

TO BE ATTACHED AND MADE PART OF the specified contract by and between the State of Utah Division of Purchasing and Carahsoft Technology Corporation (Referred to as CONTRACTOR).

BOTH PARTIES AGREE TO AMEND THE CONTRACT AS FOLLOWS:

Attachment E in the master agreement is hereby amended as follows:

1. The "Exhibit A Product Passthrough Terms – Google Apps for Work (for Customers)" document is replaced with the "Passthrough Terms – G Suite HIPPA Business Associate Addendum" attached herein this Amendment 4.
2. The "Acquia Subscription and Services Agreement" attached herein this Amendment 4 is made a part of Attachment E.

Nothing within this amendment is to be construed to amend any term or condition provided outside of Attachment E.

Effective Date of Amendment: 6/16/2017

All other terms and conditions of the contract, including those previously modified, shall remain in full force and effect.
IN WITNESS WHEREOF, the parties sign and cause this contract to be executed.

CONTRACTOR

06/16/17

Contractor's Signature — Date

Ellen Lord

Contractor's Name (Print)

Contracts Manager

Title (Print)

STATE OF UTAH

6/19/17

Kent Beers Director
State of Utah Division of Purchasing — Date

Purchasing Agent	Phone #	e-mail	Contract #
Solomon Kingston	801-538-3228	skingston@utah.gov	AR2472

Passthrough Terms – G Suite HIPAA Business Associate Addendum

Customer has entered into a certain written agreement (the "Agreement"), including the applicable Product Passthrough Terms, pursuant to which Customer is entitled to access and use the Product: G Suite. This HIPAA Business Associate Addendum ("HIPAA BAA") is effective as of the date of the Product Passthrough Terms for the purpose of implementing the requirements of HIPAA (defined below) to support the compliance requirements thereunder. Together with the Product Passthrough Terms, this HIPAA BAA will be applicable to Protected Health Information (defined below).

1. **Definitions**. For purposes of this HIPAA BAA, any capitalized terms not otherwise defined herein will have the meaning given to them in the Product Passthrough Terms 6and under HIPAA.

   "HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the rules and the regulations thereunder, as amended (including with respect to the HITECH Act).

   "HIPAA Implementation Guide" means the informational guide that Google makes available describing how Customer can configure and use the Services to support HIPAA compliance. The HIPAA Implementation Guide is available for review at the following URL: https://static.googleusercontent.com/media/www.google.com/en/us/work/apps/terms/2015/1/hipaa_implementation_guide.pdf (as the content at such URL and the URL itself may be updated or modified from time to time).

   "HITECH Act" means the Health Information Technology for Economic and Clinical Health Act enacted in the United States Congress, which is Title XIII of the American Recovery & Reinvestment Act, and the regulations thereunder, as amended.

   "Included Functionality" means functionality within the Product as described at the following URL: www.google.com/work/apps/terms/2015/1/hipaa_functionality.html (as the content at that URL, or such other URL as may be provided, may be updated from time to time).

   "Product" means only the G Suite Core Services that Provider makes available to Customer under the applicable Product Passthrough Terms as further described at the following URL: http://www.google.com/apps/intl/en-in/terms/user_features.html (as the content at such URL and the URL itself may be updated or modified from time to time).

   "Protected Health Information" or "PHI" will have the meaning given to it under HIPAA to if provided as Customer Data in connection with Customer's permitted use of Included Functionality.

   "Provider" means the third party provider of the Product.

   "Security Rule" means 45 C.F.R., Part 164, Subpart C, under HIPAA.

2. **Applicability**.

   2.1. Parties. This HIPAA BAA applies to the extent Customer is acting as a Covered Entity or Business Associate, to create, receive, maintain or transmit PHI via the Included Functionality and where Provider, as a result, is deemed under HIPAA to be acting as a Business Associate of Customer.

   2.2. Services Scope. This HIPAA BAA is applicable only to the Included Functionality. The scope of Included Functionality may expand. If the scope of Included Functionality expands, then this HIPAA BAA will automatically apply to such additional new functionality and features as of the date the Included Functionality description is updated, or the date Provider has otherwise provided written communication regarding an update to the scope of Included Functionality to Customer's Notification Email Address (whichever date is earlier).

3. **Permitted Use and Disclosure.**

   3.1. By Provider. Provider may use and disclose PHI only as permitted under HIPAA as specified in the Product Passthrough Terms and under this HIPAA BAA. Provider may also use and disclose PHI for the proper management and administration of Provider's business, for provisioning the Product, and to carry out the legal responsibilities of Provider, provided that any disclosure of PHI for such purpose may

only occur if: (1) required by applicable law; or (2) Provider obtains written reasonable assurances from the person to whom PHI will be disclosed that it will be held in confidence, used only for the purpose for which it was disclosed, and that Provider will be notified of any Breach.

3.2. By Customer. Customer will not request Provider or the Product to use or disclose PHI in any manner that would not be permissible under HIPAA if done by a Covered Entity itself (unless otherwise expressly permitted under HIPAA for a Business Associate). In connection with Customer's management and administration of the Product to End Users, Customer is responsible for using the available controls within the Product to support its HIPAA compliance requirements, including reviewing the HIPAA Implementation Guide and enforcing appropriate controls to support Customer's HIPAA compliance. Customer will not use the Product to create, receive, maintain or transmit PHI to other products or services outside of the Included Functionality, except where Customer has expressly entered into a separate HIPAA business associate agreement for use of such other products or services. If Customer uses Included Functionality in connection with PHI, Customer will use controls available within the Product to ensure: (i) all other products or services not part of the Product are disabled for all End Users who use Included Functionality in connection with PHI (except those products or services where Customer already has an appropriate HIPAA business associate agreement in place); and (ii) it takes appropriate measures to limit its use of PHI in the Product to the minimum extent necessary for Customer to carry out its authorized use of such PHI. Customer agrees that Provider has no obligation to protect PHI under this HIPAA BAA to the extent Customer creates, receives, maintains, or transmits such PHI outside of the Included Functionality (including Customer's use of its offline or on-premise storage tools or third party applications).

4. **Appropriate Safeguards**. The Product is subject to appropriate safeguards designed to prevent against unauthorized use or disclosure of PHI, consistent with this HIPAA BAA, and as otherwise required under the Security Rule, with respect to the Included Functionality. Customer will use appropriate safeguards designed to prevent against unauthorized use or disclosure of PHI, consistent with this HIPAA BAA, and as otherwise required under the Security Rule, with respect to the Included Functionality.

5. **Reporting**. Customer will be promptly notify following the discovery of a Breach resulting in the unauthorized use or disclosure of PHI in violation of this HIPAA BAA in the most expedient time possible under the circumstances, consistent with the legitimate needs of applicable law enforcement and applicable laws, and after taking any measures necessary to determine the scope of the Breach and to restore the reasonable integrity of the Services system by using commercially reasonable efforts to mitigate any further harmful effects to the extent practicable. Customer will receive any applicable Breach notifications via the Notification Email Address (as such contact is designated in the Product by Customer) or via direct communication with the Customer. For clarity, Customer and not Provider, is responsible for managing whether its End Users are authorized to create, receive, maintain or transmit PHI within the Product and Provider does not have any obligations relating thereto. This Section 5 will be deemed as notice to Customer that Provider periodically receives unsuccessful attempts for unauthorized access, use, disclosure, modification or destruction of information or interference with the general operation of Provider's information systems and the Services and even if such events are defined as a Security Incident under HIPAA, Customer will not receive any further notice regarding such unsuccessful attempts.

6. **Agents and Subcontractors**. As related to the Product, appropriate measures are taken to ensure that any agents and subcontractors used by Provider to perform its obligations related to the provision of the Product that require access to PHI on behalf of Provider are bound by written obligations that provide the same material level of protection for PHI as this HIPAA BAA. To the extent Provider uses agents and subcontractors in its performance of obligations hereunder, Provider will remain responsible for their performance as if performed by Provider itself under the Product Passthrough Terms.

7. **Accounting Rights**. PHI will be made available to Customer via the Product so Customer may fulfill its obligation to give individuals their rights of access, amendment, and accounting in accordance with the requirements under HIPAA. Customer is responsible for managing its use of the Product to appropriately respond to such individual requests.

8. **Access to Records**. To the extent required by law, and subject to applicable attorney client privileges, Provider will make its internal practices, books, and records concerning the use and disclosure of PHI received from Customer, or created or received by Provider on behalf of Customer, available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for the purpose of the Secretary determining compliance with this HIPAA BAA.

9. **Return/Destruction of Information**. Upon termination of the Product Passthrough Terms or the Agreement, all PHI received from Customer, or created or received by Provider on behalf of Customer, which is still maintained in accordance with the section titled "Effects of Termination" (or as otherwise expressly agreed in writing) under the Product Passthrough Terms will be returned or destroyed; provided, however, that if such return or destruction is not feasible, the protections of this HIPAA BAA will extent to the PHI not returned or destroyed and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. In the event this HIPAA BAA is terminated earlier than the the Product Passthrough Terms or Agreement Customer may continue to use the Product in accordance with the the Product Passthrough Terms, but must delete any PHI it maintains in the Product and cease to create, receive, maintain or transmit such PHI to Provider or within the Product.

10. **Breach/Cure**. Customer may immediately terminate this HIPAA BAA and the Product Passthrough Terms upon 10 days written notice if Provider has materially breached this HIPAA BAA and such breach is not reasonably capable of being cured.

11. **Term**. This HIPAA BAA will expire upon the earlier of: (i) a permitted termination in accordance with this HIPAA BAA; (ii) the natural expiration or termination of the Product Passthrough Terms; (iii) the natural expiration or termination of the existing Agreement; or (iv) the execution of an updated HIPAA BAA that supersedes this HIPAA BAA.

12. **Interpretation**. It is the parties' intent that any ambiguity under this HIPAA BAA be interpreted consistently with the intent to comply with applicable laws.

13. **Effect of Addendum**. This HIPAA BAA supersedes in its entirety any pre-existing HIPAA BAA executed by the parties covering the same Product. To the extent of any conflict or inconsistency between the terms of this HIPAA BAA and the Product Passthrough Terms or the Agreement, the terms of this HIPAA BAA will govern. Except as expressly modified or amended under this HIPAA BAA, the terms of the Passthrough Terms and the Agreement remain in full force and effect.

Product Passthrough Terms – G Suite (for Customers)

Customer has entered into a certain written agreement (the "Agreement") pursuant to which Customer has purchased the right to access and use the Product. These Product Passthrough Terms set forth the terms and conditions under which Customer may access and use such Product.

1. **Product**.

1.1 Facilities and Data Transfer. All facilities used to store and process Customer Data will adhere to reasonable security standards no less protective than the security standards at facilities where Provider stores and processes its own information of a similar type. As part of providing the Product, Provider may transfer, store and process Customer Data in the United States or any other country in which Provider or its agents maintain facilities. By using the Product, Customer consents to this transfer, processing and storage of Customer Data.

1.2 No Ads. Notwithstanding any other term of the Product Passthrough Terms, Provider will not process Customer Data for Advertising purposes or serve Advertising in the Product.

1.3 New Features or Product. Provider may make new applications, features or functionality for the Product available from time to time, the use of which may be contingent upon Customer's Product Passthrough Terms to additional terms.

1.4 Modifications.

(a) Changes to Product. Provider may make commercially reasonable changes to the Product from time to time. If Provider makes a material change to the Product, Provider will inform Customer, by either sending an email to the Notification Email Address or alerting Customer through the Admin Console.

(b) Changes to URL Terms. Provider may make commercially reasonable changes to the URL Terms from time to time. If Provider makes a material change to the URL Terms, Provider will inform Customer by either sending an email to the Notification Email Address or alerting Customer through the Admin Console. If the change has a material adverse impact on Customer and the change is not a result of Provider complying with a court order or applicable law, Customer may notify Provider within thirty days after being informed of the change that Customer does not agree with the change. If Customer notifies Provider as required, then Customer will remain governed by the terms in effect immediately prior to the change until the earlier of: (i) the end of the then-current Term or (ii) 12 months after Provider informs Customer of the change, unless the modification to the URL Terms is in response to a court order or to comply with applicable law. If used of the Product renews, it will do so under the updated URL Terms.

(c) Discontinuance of Product. Subject to Section 1.4(d), Provider can discontinue any Product or any portion or feature for any reason at any time without liability to Customer.

(d) Deprecation Policy. Provider will notify Customer if it intends to make a Significant Deprecation. Provider will use commercially reasonable efforts to continue to provide the Product without a Significant Deprecation for at least one year after that notification, unless (as Provider determines in its reasonable good faith judgment): (i) otherwise required by law or by contract (including if there is a change in applicable law or contract), or (ii) doing so could create a security risk or a substantial economic or technical burden. This policy is the "Deprecation Policy."

1.5 Customer Domain Name Ownership. Prior to providing the Product, Provider may verify that Customer owns or controls the Customer Domain Names. If Customer does not own, or control, the Customer Domain Names, then Provider will have no obligation to provide Customer with the Product.

1.6 Google Vault - Retention. If Customer purchases Google Vault, Provider will have no obligation to retain any archived Customer Data beyond the retention period specified by Customer (other than for any legal holds). If Customer does not renew Google Vault, Provider will have no obligation to retain any archived Customer Data.

1.7 Federal Information Security Management Act (FISMA). The Provider's Product known as "G Suite Core Services" received a FISMA "Authorization to Operate" for a Moderate impact system. Provider will continue to maintain a System Security Plan (SSP) for the G Suite Core Services, based on NIST 800-53 Rev. 3, or a similarly applicable standard. If Provider does not maintain this SSP as stated, Customer's sole and exclusive remedy, and Provider's entire liability, will be Customer's ability to terminate use of the Product upon thirty days prior written notice.

2. **Customer Obligations**.

2.1 Compliance. Customer must ensure that all use of the Product by Customer and its End Users complies with this Product Passthrough Terms including the Acceptable Use Policy.

2.2 Additional Products. Provider may make Additional Products available to Customer and its End Users in accordance with the applicable product-specific Additional Product Terms. Additional Products are not subject to or governed by this Product Passthrough Terms. Customer can enable or disable Additional Products and is not required to use Additional Products in order to use the Product.

2.3 Customer Administration of the Product. Customer may specify one or more Administrators through the Admin Console who will have the rights to access Admin Account(s) and to administer the End User Accounts. Customer is responsible for: (a) maintaining the confidentiality of the password and Admin Account(s); (b) designating those individuals who are authorized to access the Admin Account(s); and (c) ensuring that all activities that occur in connection with the Admin Account(s) comply with the Product Passthrough Terms. Customer agrees that Provider's responsibilities do not extend to the internal management or administration of the Product for Customer and that Provider is merely a data-processor.

2.4 Administrator Access; End User Consent.

(a) Administrator Access. Administrators will have the ability to access all Customer's End User Accounts, including the ability to access, monitor, use, modify, withhold, or disclose any data available to End Users associated with their End User Accounts.

(b) Reseller as Administrator. If Customer orders Product via Reseller, Reseller may have Administrator access to Customer's Account and Customer's End User Accounts. As between Provider and Customer, Customer is solely responsible for: (i) any access by Reseller to Customer's Account or Customer's End User Accounts; and (ii) defining in the Reseller Product Passthrough Terms any rights or obligations as between Reseller and Customer with respect to the Product.

(c) End User Consent. Customer will obtain and maintain all required consents from End Users to allow: (i) Administrators to have the access described in these Product Passthrough Terms; and (ii) Provider's provision of the Product to Administrators and End Users.

2.5 Unauthorized Use. Customer will use commercially reasonable efforts to prevent unauthorized use of the Product and to terminate any unauthorized use. Customer will promptly notify Provider of any unauthorized use of, or access to, the Product of which it becomes aware.

2.6 Restrictions on Use. Unless Provider specifically agrees in writing, Customer will not, and will use commercially reasonable efforts to make sure a third party does not: (a) sell, resell, lease, or the functional equivalent, the Product to a third party (unless expressly authorized in this Product Passthrough Terms); (b) attempt to reverse engineer the Product or any component; (c) attempt to create a substitute or similar service through use of, or access to, the Product; (d) use the Product for High Risk Activities; (e) use the Product to store or transfer any Customer Data that is controlled for export under Export Control Laws; or (f) use the Product on behalf of or for the benefit of any entity or person who is prohibited from using the Product by United States laws or regulations. Customer is solely responsible for any applicable compliance with HIPAA.

2.7 Support. Customer will, at its own expense, respond to questions and complaints from End Users or third parties relating to Customer's or End Users' use of the Product. Customer will use commercially reasonable efforts to resolve support issues before escalating them to Provider.

2.8 Aliases. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names but Provider may monitor emails sent to these aliases for Customer Domain Names to allow Provider to identify Product abuse.

3. **Intentionally Omitted.**

4. **Technical Support Services**. Provider will provide TSS to Customer during the Term in accordance with the TSS Guidelines subject to payment of support Fees, if applicable.

5. **Suspension**.

5.1 Of End User Accounts by Provider. If Provider becomes aware of an End User's violation of the Product Passthrough Terms, then Provider may specifically request that Customer Suspend the applicable End User Account. If Customer fails to comply with Provider's request to Suspend an End User Account, then Provider may do so. The duration of any Suspension by Provider will be until the applicable End User has cured the breach which caused the Suspension.

5.2 Emergency Security Issues. Notwithstanding the foregoing, if there is an Emergency Security Issue, then Provider may automatically Suspend the offending use. Suspension will be to the minimum extent and of the minimum duration required to prevent or terminate the Emergency Security Issue. If Provider Suspends an End User Account for any reason without prior notice to Customer, at Customer's request, Provider will provide Customer the reason for the Suspension as soon as is reasonably possible.

5.3 Suspension for Non-Payment and Delinquent Payment. As of the first date Customer becomes delinquent on Fees owed, Customer's Account may be Suspended until all delinquent Fees have been paid.

5.4 Suspension to Comply with Laws. Provider may at its sole discretion Suspend the provision of any Product at any time if required to comply with any applicable law.

6. **Confidential Information.**

6.1 Obligations. Subject to Section 6.2 (Disclosure of Confidential Information), the recipient will not disclose the discloser's Confidential Information, except to employees, Affiliates, agents, or professional advisors ("Delegates") who need to know it and who have a legal obligation to keep it confidential. The recipient will use the Confidential Information only to exercise rights and fulfill obligations under these Product Passthrough Terms, while using reasonable care. The recipient will ensure that its Delegates are also subject to the same non-disclosure and use obligations.

6.2 Disclosure of Confidential Information.

(a) General. Subject to Section 6.2(b), the recipient may disclose the discloser's Confidential Information (i) in accordance with a Legal Process or (ii) with the discloser's written consent.

(b) Notification. Before the recipient discloses the discloser's Confidential Information in accordance with a Legal Process, the recipient will use commercially reasonable efforts to promptly notify the discloser Provider will give notice via the Notification Email Address. The recipient does not need to provide notice before disclosure if the recipient is informed that (i) it is legally prohibited from giving notice or (ii) the Legal Process relates to exceptional circumstances involving danger of death or serious physical injury to any person.

(c) Opposition. Recipient will comply with the other party's reasonable requests opposing disclosure of its Confidential Information.

7. **Intellectual Property Rights; Brand Features**.

7.1 Intellectual Property Rights. Except as expressly set forth herein, these Product Passthrough Terms does not grant either party any rights, implied or otherwise, to the other's content or any of the other's intellectual property. As between the parties, Customer owns all Intellectual Property Rights in Customer Data and Provider owns all Intellectual Property Rights in the Product.

7.2 Display of Brand Features. Provider may display only those Customer Brand Features authorized by Customer (such authorization is provided by Customer uploading its Brand Features into the Product) within designated areas of the Service Pages. Customer may specify the nature of this use using the Admin Console. Provider may also display Provider Brand Features on the Service Pages to indicate that the Product are provided by Provider. Neither party may display or use the other party's Brand Features beyond what is allowed in these Product Passthrough Terms without the other party's prior written consent.

7.3 Brand Features Limitation. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights in those Brand Features. A party may revoke the other party's right to use its Brand Features pursuant to these Product Passthrough Terms with written notice to the other and a reasonable period to stop the use.

8. **Publicity**. In connection with Customer's use of the Product, (a) Customer may state publicly that it is a Provider customer and display Provider Brand Features consistent with the Trademark Guidelines and (b) Provider may (i) orally state that Customer is a Provider customer and (ii) include Customer's name or Customer Brand Features in a list of Provider customers in Provider's online or offline promotional materials. Neither party needs approval if it is using the other party's name or Brand Features in a manner that is substantially similar to a previously approved manner. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights to those Brand Features. A party may revoke the other party's right to use its Brand Features under this Section with written notice to the other party and a reasonable period to stop the use.

9. **Representations, Warranties and Disclaimers**.

9.1 Representations and Warranties. Each party represents that (a) it has full power and authority to enter into the Product Passthrough Terms; and (b) it will comply with all laws and regulations applicable to its provision, or use, of the Product, as applicable. Provider warrants that it will provide the Product in accordance with the applicable SLA.

9.2 Disclaimers. EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS PRODUCT PASSTHROUGH TERMS, TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, (A) NEITHER PARTY NOR ITS SUPPLIERS MAKES ANY OTHER WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT; AND (B) NEITHER PROVIDER NOR ITS SUPPLIERS WARRANTS THAT OPERATION OF THE SOFTWARE OR THE PRODUCT WILL BE ERROR-FREE OR UNINTERRUPTED. NEITHER THE SOFTWARE NOR THE PRODUCT ARE DESIGNED, MANUFACTURED, OR INTENDED FOR HIGH RISK ACTIVITIES. EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS PRODUCT PASSTHROUGH TERMS, TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, PROVIDER MAKES NO REPRESENTATIONS ABOUT ANY CONTENT OR INFORMATION MADE ACCESSIBLE BY OR THROUGH THE PRODUCT. CUSTOMER ACKNOWLEDGES THAT THE PRODUCT ARE NOT A TELEPHONY SERVICE AND THAT THE PRODUCT ARE NOT CAPABLE OF PLACING OR RECEIVING ANY CALLS, INCLUDING EMERGENCY SERVICES CALLS, OVER PUBLICLY SWITCHED TELEPHONE NETWORKS.

10. **Term**. These Product Passthrough Terms will remain in effect for the Term.

11. **Termination**.

11.1 Termination for Cause. Either party may suspend performance or terminate these Product Passthrough Terms if: (i) the other party is in material breach of the Product Passthrough Terms and fails to cure that breach within thirty days after receipt of written notice; (ii) the other party ceases its business operations or becomes subject to insolvency proceedings and the proceedings are not dismissed within ninety days; or (iii) the other party is in material breach of these Product Passthrough Terms more than two times notwithstanding any cure of such breaches.

11.2 Effects of Termination. If these Product Passthrough Terms terminates or expires, then: (i) the rights granted by one party to the other will cease immediately (except as set forth in Section 11.2 and Section 14.12 (Survival)); (ii) Customer will not have access to, or the ability to export, the Customer Data after the effective date of termination or expiry of the Product Passthrough Terms; (iii) all Fees owed by Customer to Provider are immediately due upon receipt of the final invoice; (d) Customer will delete the Customer Data in a manner consistent with the functionality of the Product and in accordance with the terms of the Product Passthrough Terms; (e) Provider will delete Customer Data in accordance with the

terms of the Product Passthrough Terms; and (f) upon request each party will promptly use reasonable efforts to return or destroy any remaining Confidential Information of the other party.

12. Miscellaneous.

12.1 Product Development. The Product was developed solely at private expense and is commercial computer software and related documentation within the meaning of the applicable civilian and military federal acquisition regulations and any supplements thereto.

12.2 Force Majeure. Neither party will be liable for inadequate performance to the extent caused by a condition (for example, natural disaster, act of war or terrorism, riot, labor condition, governmental action, and Internet disturbance) that was beyond the party's reasonable control.

12.3 No Waiver. Failure to enforce any provision of this Product Passthrough Terms will not constitute a waiver.

12.4 Severability. If any provision of this Product Passthrough Terms is found unenforceable, the balance of the Product Passthrough Terms will remain in full force and effect.

12.5 No Agency. The parties are independent contractors, and this Product Passthrough Terms does not create an agency, partnership or joint venture.

12.6 No Third-Party Beneficiaries. There are no third-party beneficiaries to this Product Passthrough Terms.

12.7 Survival. The following sections will survive expiration or termination of this Product Passthrough Terms: Section 3 (Payment), 6 (Confidential Information), 7.1 (Intellectual Property Rights), 11.2 (Effects of Termination), 12 (Defense and Indemnity), 13 (Limitation of Liability), 14 (Miscellaneous) and 15 (Definitions).

12.8 Entire Product Passthrough Terms. This Product Passthrough Terms, and all documents referenced herein, is the parties' entire Product Passthrough Terms relating to its subject and supersedes any prior or contemporaneous Product Passthrough Termss on that subject. The terms located at a URL and referenced in this Product Passthrough Terms are hereby incorporated by this reference.

12.9 Interpretation of Conflicting Terms. If there is a conflict between the documents that make up this Product Passthrough Terms, the documents will control in the following order: the Order Form, the Product Passthrough Terms, and the terms located at any URL.

13. Definitions.

"Acceptable Use Policy" means the acceptable use policy for the Product available at https://gsuite.Provider.com/terms/use_policy.html or such other URL as may be provided by Provider.

"Account" means Customer's Provider account credentials and correlating access to the Product under this Product Passthrough Terms.

"Account Manager" means the Provider business person working with Customer regarding Customer's purchase of the Product.

"Additional Products" means products, Product and applications that are not part of the Product but that may be accessible, via the Admin Console or otherwise, for use with the Product.

"Admin Account(s)" means the administrative account(s) provided to Customer by Provider for the purpose of administering the Product. The use of the Admin Account(s) requires a password, which Provider will provide to Customer.

"Admin Console" means the online tool provided by Provider to Customer for use in reporting and certain other administration functions.

"Administrators" mean the Customer-designated technical personnel who administer the Product to End Users on Customer's behalf.

"Advertising" means online advertisements displayed by Provider to End Users, excluding any advertisements Customer expressly chooses to have Provider or any Provider Affiliate display in connection with the Product under a separate Product Passthrough Terms (for example, Provider AdSense advertisements implemented by Customer on a website created by Customer using the "Provider Sites" functionality within the Product).

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with a party.

"Annual Charge" means the annual charge for the Product set forth in the Order Form.

"Billing Start Date" means the date upon which Customer will begin paying Provider for the Product.

"Brand Features" means the trade names, trademarks, service marks, logos, domain names, and other distinctive brand features of each party, respectively, as secured by such party from time to time.

"Confidential Information" means information that one party (or Affiliate) discloses to the other party under this Product Passthrough Terms, and that is marked as confidential or would normally be considered confidential information under the circumstances. It does not include information that is independently developed by the recipient, is rightfully given to the recipient by a third party without confidentiality obligations, or becomes public through no fault of the recipient. Subject to the preceding sentence, Customer Data is Customer's Confidential Information.

"Customer Data" means data, including email, provided, generated, transmitted or displayed via the Product by Customer or End Users.

"Customer Domain Names" mean the domain names owned or controlled by Customer, which will be used in connection with the Product and specified in the Order Form.

"Effective Date" means the date this Product Passthrough Terms is countersigned.

"Emergency Security Issue" means either: (a) Customer's or End Users' use of the Product in violation of the Acceptable Use Policy, in a way that disrupts: (i) the Product; (ii) other customers' use of the Product; or (iii) the Provider network or servers used to provide the Product; or (b) to prevent unauthorized third party access to the Product or data within the Product.

"End Users" means the individuals Customer permits to use the Product.

"End User Account" means a Provider-hosted account established by Customer through the Product for an End User.

"Export Control Laws" means all applicable export and reexport control laws and regulations, including trade and economic sanctions maintained by the Treasury Department's Office of Foreign Assets Control, and the International Traffic in Arms Regulations ("ITAR") maintained by the Department of State, but excluding the Export Administration Regulations ("EAR") maintained by the U.S. Department of Commerce.

"Fees" means the amounts invoiced to Customer by Provider, or Reseller, if applicable, for the Product as described in this Product Passthrough Terms.

"G Suite Core Services" means the Product specified in the Order Form which are more fully described here: https://gsuite.Provider.com/terms/user_features.html or other such URL as Provider may provide.

"Help Center" means the Provider help center accessible at http://www.Provider.com/support/, or other such URL as Provider may provide.

"High Risk Activities" means uses such as the operation of nuclear facilities, air traffic control, or life support systems, where the use or failure of the Product could lead to death, personal injury, or environmental damage.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as may be amended from time to time, and any regulations issued thereunder.

"Initial Term" means the term for the applicable Product beginning on the Service Commencement Date and continuing for the "Current Term" set forth in the Order Form from the Billing Start Date.

"Initial Term Charge" means the charge for the Product for the Initial Term (excluding any applicable one time fees), as set forth in the Order Form.

"Intellectual Property Rights" means current and future worldwide rights under patent law, copyright law, trade secret law, trademark law, moral rights law, and other similar rights.

"Legal Process" means a data disclosure request made under law, governmental regulation, court order, subpoena, warrant, governmental regulatory or agency request, or other valid legal authority, legal procedure, or similar process.

"Notification Email Address" means the email address(es) designated by Customer in the Admin Console to receive certain notifications from Provider. It is Customer's responsibility to keep the Notification Email Address(es) valid and current.

"Order Form" means an order form, which is the written document provided to Customer by Provider or by a Reseller specifying the Product Customer will use under the Product Passthrough Terms.

"Product" means, as applicable, the G Suite Core Services set forth in the Order Form.

"Product Passthrough Terms" means the combination of the Order Form and this G Suite Product Passthrough Terms.

"Provider" means the third party provider of the Product.

"Purchase Order" means a Customer issued purchase order.

"Reseller" means, if applicable, the authorized reseller that sells or supplies the Product to Customer.

"Service Commencement Date" is the date upon which Provider makes the Product available to Customer, and will be within one week of Provider's receipt of the applicable Order Form signed by Customer, unless otherwise agreed by the parties.

"Service Pages" mean the web pages displaying the Product to End Users.

"Significant Deprecation" means to discontinue or to make backwards incompatible changes to the Product that results in Provider no longer providing to its enterprise-customer base the ability to: (1) to send and receive e-mail messages; (2) schedule and manage events; (3) create, share, store and sync files; (4) communicate with other end users in real time; or (5) search, archive, and export email messages.

"SLA" means the Service Level Product Passthrough Terms located here for applicable Product: https://gsuite.Provider.com/terms/sla.html or such other URL as Provider may provide.

"Suspend" means the immediate disabling of access to the Product, or components of the Product, as applicable, to prevent further use of the Product.

"Term" means the Initial Term and all renewal terms for the applicable Product.

"TSS" means the technical support services provided by Provider to the Administrators under the TSS Guidelines.

"TSS Guidelines" means Provider's technical support services guidelines then in effect for the Product. TSS Guidelines are at the following URL: https://gsuite.Provider.com/terms/tssg.html or such other URL as Provider may provide.

"URL Terms" means the Acceptable Use Policy, the SLA, and the TSS Guidelines.

Pass-through Terms of Service for Google Professional Services

The following Terms of Service govern Google's performance and delivery of certain services and deliverables as described below.

1. **Definitions**.

"**Affiliate**" means any entity that directly or indirectly controls, is controlled by, or is under common control with, a party.

"**Background IP**" means all Intellectual Property owned or licensed by a party (a) before the provision of any Professional Services; or (b) independent of the Professional Services.

"**Brand Features**" means each party's trade names, trademarks, logos, domain names, and other distinctive brand features.

"**Confidential Information**" means information that one party (or an Affiliate) discloses to the other party under the Terms of Service, and that is marked as confidential or would normally be considered confidential information under the circumstances. It does not include information that is independently developed by the recipient, is rightfully given to the recipient by a third party without confidentiality obligations, or becomes public through no fault of the recipient.

"**Deliverables**" means any tangible or intangible work product (including third party materials) specific to the Customer to be provided by Google to Customer in connection with the Professional Services.

"**Developed IP**" means any Intellectual Property (other than Background IP) created or discovered by or on behalf of either party in connection with the Terms of Service.

"**Fees**" means the applicable fees for the Professional Services, including any reimbursable expenses (if applicable). The Fees for the Professional Services are stated in the applicable Ordering Document or other Partner document.

"**Google Product**" means any Google services or products made available to Customer under a separate agreement.

"**Including**" or "**including**" means "including but not limited to," and any examples listed are illustrative and not the sole examples of a particular concept.

"**Indemnified Liabilities**" means any (a) settlement amounts approved by the indemnifying party; and (b) damages and costs in a final judgment awarded against the indemnified part(ies) by a competent court.

"**Intellectual Property**" or "**IP**" means anything protectable by an Intellectual Property Right.

"**Intellectual Property Rights**" means all patent rights, copyrights, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, and any other intellectual property rights (registered or unregistered) throughout the world.

"**Ordering Document**" means an order form or statement of work issued by a Partner, referencing the Terms of Service and signed by Customer and Partner (as applicable). An Ordering Document will describe, at a minimum, the following: (a) details of the Google Professional Services being ordered; (b) the Fees; and (c) the applicable form of payment.

"**Partner**" means a third party entity authorized by Google to resell the Professional Services.

"**Personnel**" means a party's directors, officers, employees, agents, other staff and subcontractors.

"**Product Agreement**" means the separate agreement (if any) entered into between Google and Customer with respect to a Google Product, as amended from time to time in accordance with its terms.

"**Professional Services**" means Google professional services ordered by Customer subject to the Terms of Service, as more fully described in the datasheet associated with the applicable SKU referenced in an applicable Ordering Document.

"**Third-Party Legal Proceeding**" means any formal legal proceeding filed by an unaffiliated third party before a court or government tribunal (including any civil, administrative, investigative or appellate proceeding).

"**Trademark Guidelines**" means Google's guidelines for third party use of Google's Brand Features, located at: http://www.google.com/permissions/guidelines.html.

2. **Professional Services.**

2.1 Professional Services. Google will provide Professional Services and Deliverables to Customer in accordance with the Terms of Service, subject to Customer fulfilling its obligations under Section 2.2 (Customer Cooperation). The scope of the Google Professional Services will be detailed in the Ordering Document.

2.2 Customer Cooperation. Time will not be of the essence for performance of the Professional Services or delivery of the Deliverables. Customer will provide reasonable and timely cooperation in connection with Google's performance of the Professional Services and delivery of the Deliverables. Customer will fulfill any responsibility described in the Ordering Document. Customer will also provide any information that Google needs to provide Professional Services or that is necessary for a Deliverable. If necessary, Customer will provide access to customer controlled facilities and locations. All information that Customer provides Google will be accurate in all material respects. If Customer's failure to comply with the foregoing causes any delay in Google's performance of the Professional Services or delivery of the Deliverables, neither Google nor Partner will be liable for such delay. Partner may charge additional reasonable fees or cancel any uncompleted Professional Services or Deliverables by notifying Customer in writing (email permitted).

2.3 Personnel. Google will determine its Personnel assigned to perform the Professional Services. If Customer has a reasonable basis for requesting a change of such Personnel, Google will reasonably consider the request and use reasonable efforts to replace the assigned Personnel with alternative Google Personnel.

3. **Payments.** If Customer orders Professional Services from a Partner: (a) Customer will pay Partner for the Professional Services; (b) all payment terms are to be decided upon between Customer and Partner; (c) there will not be an Ordering Document between Google and Customer; (d) Google will provide to Partner any refunds or credits that may be due to Customer; and (e) any obligation on the part of Partner to provide any such refunds or credits to Customer will depend on the terms decided upon between Customer and Partner.

4. **Intellectual Property.**

4.1 Background IP. Except for the license rights under Section 5 (Licenses), neither party will own or acquire any right, title, or interest in or to the other party's Background IP under the Terms of Service.

4.2 Deliverables and Developed IP.

(a) Title to Deliverables. Subject to Sections 4.1 (Background IP) and 4.2(b) (Ownership of Developed IP), title to the Deliverables will transfer to Customer upon delivery.

(b) Ownership of Developed IP. As between the parties, and subject to Section 5.3 (License to Developed IP):

(i) Google owns any Developed IP; and

(ii) to the extent that Customer or any of its Personnel owns any rights in the Developed IP, Customer assigns to Google (or agrees to procure the assignment to Google of) all rights (including Intellectual Property Rights), title, and interest in or to the Developed IP, provided

however that if applicable law prevents future assignments, Customer will assign (or will procure the assignment of) such rights as these are created.

(c) Moral Rights. Customer will not assert, and to the extent permitted by applicable law, otherwise waives, any moral rights in the Developed IP. Customer will ensure that its Personnel and other third parties in its control who have moral rights in the Developed IP will also not assert, and to the extent permitted by applicable law, will waive, those moral rights.

5. Licenses.

5.1 Google IP. Subject to Customer's payment of applicable Fees, Google grants a limited, non-exclusive, royalty-free, fully-paid, worldwide license (with the right to sublicense to Affiliates only) to Customer to do the following for Customer's internal business purposes:

(a) use the Developed IP solely in connection with the Deliverables; and

(b) use any Google Background IP included in the Deliverables solely in connection with the Deliverables.

5.2 Customer Background IP. Customer grants to Google and its Personnel a limited, non-exclusive, non-transferable, royalty-free, fully-paid, worldwide license (with the right to sublicense) to reproduce, maintain, prepare derivative works of, distribute and use Customer Background IP solely in connection with Google's performance of Professional Services and creation and delivery of the Deliverables under the Terms of Service.

5.3 License to Developed IP. If applicable law prevents Customer from assigning ownership to Google of any Developed IP, Customer grants Google a perpetual, irrevocable, exclusive, royalty-free, fully-paid, transferable, worldwide license (with the right to sublicense) to:

(a) reproduce, prepare derivative works of, distribute, publicly perform, publicly display and otherwise use such Developed IP; and

(b) make, use, sell, offer for sale, import, export any component of and otherwise dispose of such Developed IP.

6. Confidentiality. The recipient will not disclose the Confidential Information, except to its Personnel, Affiliates, or professional advisors ("Delegates") who need to know it and who have a legal obligation to keep it confidential. The recipient will use the Confidential Information only to exercise rights and fulfill obligations under the Terms of Service, while using reasonable care. The recipient will ensure that its Delegates are also subject to the same non-disclosure and use obligations. The recipient may disclose Confidential Information when required by law after giving reasonable notice to the discloser, if permitted by law. Except for the limited use rights under the Terms of Service, neither party acquires any right, title, or interest in the other party's Confidential Information.

7. **Publicity**. Unless Customer agrees to different terms with the Reseller, then in connection with Customer's purchase and receipt of the Professional Services, (a) Customer may state publicly that it is a Google customer and display Google Brand Features consistent with the Trademark Guidelines, and (b) Google may (i) orally state that Customer is a Google customer and (ii) include Customer's name or Customer Brand Features in a list of Google customers (whether in Google's online or offline promotional materials). Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights to those Brand Features. A party may revoke the other party's right to use its Brand Features under this Section with written notice to the other party and a reasonable period to stop the use.

8. **Warranties and Disclaimers**.

8.1 Google Warranties.

(a) Quality. Google will perform the Professional Services in a professional and workmanlike manner, with reasonable skill and care, in accordance with generally-accepted industry standards. All of Google's Personnel performing the Professional Services have the requisite skills, experience, and qualifications.

(b) No Conflicts. There are no actual or potential conflicts of interest concerning the provision of the Services.

(c) Compliance with Customer's Onsite Policies and Procedures. If Google's Personnel perform Professional Services onsite at Customer's facilities, they will comply with Customer's reasonable procedures and policies made known to Google in writing in advance.

8.2 Remedies. Google's entire liability and Customer's sole remedy for failure to provide Professional Services or Deliverables that conform with Section 8.1(a) (Quality) will be for Google to use reasonable efforts to re-perform the applicable Professional Services or to terminate the applicable Ordering Document, and refund any applicable Fees received for the nonconforming Professional Services.

8.3 Disclaimers. TO THE FULLEST EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT AS EXPRESSLY PROVIDED FOR IN THIS SECTION 8, GOOGLE DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR USE AND NONINFRINGEMENT. GOOGLE MAKES NO REPRESENTATIONS ABOUT ANY GOOGLE PRODUCTS OR ANY CONTENT OR INFORMATION MADE ACCESSIBLE OR AVAILABLE BY OR THROUGH THE PROFESSIONAL SERVICES.

9. **Termination**.

9.1 Effects of Termination.

(a) Effects of Termination on Professional Services and Deliverables. If there is a termination of the agreement between the Customer and Partner, Google will immediately stop work on any Professional Services and Deliverables that remain incomplete as of the effective date of termination.

(c) Survival. Sections 1 (Definitions), 3 (Payment), 4 (Intellectual Property), 5.3 (License to Developed IP), 6 (Confidentiality), 8.2 (Remedies), 8.3 (Disclaimers), 9.1 (Effects of Termination), 10 (Defense and Indemnity), and 11 (General) will survive expiry or termination of the Terms of Service.

10. **Defense and Indemnity.**

10.1 Google Indemnification Obligations. Subject to Section 10.4 (Conditions), Google will defend and indemnify Customer against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that Customer's use in accordance with the Terms of Service of any of the following (collectively, the "Google Indemnified Materials") infringes the third party's Intellectual Property Rights: (a) Deliverables including Developed IP and Google Background IP (in each case, excluding any open source software and any Developed IP licensed by Customer to Google); or (b) Google's Brand Features.

10.2 Customer Indemnification Obligations. Subject to Section 10.4 (Conditions), Customer will defend Google, its Personnel, and its Affiliates ("Google Indemnified Parties"), and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that Google Indemnified Parties' use in accordance with the Terms of Service of any of the following (collectively, the "Customer Indemnified Materials") infringes the third party's Intellectual Property Rights: (a) Customer Background IP, any Developed IP licensed to Google by Customer and any other information, materials or technology provided to Google by Customer in connection with the Professional Services (in each case, excluding any open source software); or (b) Customer's Brand Features. If Customer is a U.S. (federal, state, or local) government agency, then Customer's indemnification obligations will apply to the extent permitted by law.

10.3 Exclusions. This Section 10 will not apply to the extent the underlying allegation arises from:

(a) modifications to the Google Indemnified Materials or Customer Indemnified Materials (as applicable) by anyone other than the indemnifying party;

(b) combination of the Google Indemnified Materials or Customer Indemnified Materials (as applicable) with materials not provided by the indemnifying party; or

(c) compliance with the indemnified party's instructions, design or request for customized features.

10.4 Conditions. Obligations under Sections 10.1 (Google Indemnification Obligations) and 10.2 (Customer's Indemnification Obligations) are conditioned on the following:

(a) The indemnified party must have promptly notified the indemnifying party in writing of any allegation(s) that preceded the Third-Party Legal Proceeding and must cooperate reasonably with the indemnifying party to resolve the allegation(s) and Third-Party Legal Proceeding. If breach of this Section 10.4(a) prejudices the defense of the Third-Party Legal Proceeding, the indemnifying party's obligations under Section 10.1 or 10.2 (as applicable) will be reduced in proportion to the prejudice.

(b) The indemnified party must tender sole control of the indemnified portion of the Third-Party Legal Proceeding to the indemnifying party, subject to the following: (i) the indemnified party may appoint its own non-controlling counsel, at its own expense; and (ii) any settlement requiring the indemnified party to admit liability, pay money, or take (or refrain from taking) any action, will require the indemnified party's prior written consent, not to be unreasonably withheld, conditioned, or delayed.

10.5 Infringement Remedies.

(a) If Google reasonably believes the Professional Services or Deliverables (including the Developed IP and Google Background IP) might infringe a third party's Intellectual Property Rights, then Google may, at its sole option and expense: (i) procure the right for Google to provide the Professional Services or for Customer to use the Deliverables including the Developed IP and Google Background IP (as applicable) in accordance with the Terms of Service; (ii) modify the Professional Services or Deliverables to make them non-infringing without materially reducing their functionality; or (iii) replace the Professional Services or Deliverables with a non-infringing, functionally equivalent alternative.

(b) If Google notifies Customer that Google does not consider the remedies in Section 10.5(a) to be commercially reasonable in the circumstances, or if such remedies are not provided within ninety (90) days of an injunction:

(i) either party may terminate the work described in the Ordering Document immediately on written notice; or

(ii) Google may, with prior written notice, suspend or terminate Customer's use of the impacted Deliverables and provide a pro-rated refund of any Fees paid for such Professional Services to Partner for return to Customer.

10.6 Sole Rights and Obligations. Without affecting either party's termination rights , this Section 10 states the parties' only rights and obligations under the Terms of Service for any third party's Intellectual Property Rights allegations and Third-Party Legal Proceedings.

11. **Miscellaneous.**

11.1 Independent Development. Nothing in the Terms of Service will be construed to limit or restrict either party from independently developing, providing, or acquiring any materials, services, products, programs or technology that are similar to the subject of the Terms of Service t, provided that the party does not violate its obligations under the Terms of Service.

11.2 Force Majeure. Neither party will be liable for failure or delay in performance to the extent caused by circumstances beyond its reasonable control.

11.3 Severability. If any term (or part of a term) in the Terms of Service is invalid, illegal or unenforceable, the rest of the terms will remain in effect.

11.4 No Third-Party Beneficiaries. The Terms of Service do not confer any benefits on any third party unless it expressly states that it does.

11.5 Interpretation of Conflicting Terms. Unless stated otherwise in the applicable Ordering Document, if there is a conflict between any term of the Terms of Service and a term of an Ordering Document, the Terms of Service will govern.

Acquia

SUBSCRIPTION AND SERVICES AGREEMENT

This subscription and services agreement (the **"Agreement"**), the relevant terms of the Guide, and any executed Orders and/or SOWs between the parties, are incorporated herein and shall govern the provision of the Services. Customer and its Affiliates may place orders under this Agreement by submitting separate Order(s) and SOW(s), pursuant to which an Affiliate will be considered the Customer as forth herein. This Agreement shall commence on the Effective Date of Customer's first executed Order or SOW (**"Effective Date"**) and will continue until otherwise terminated in accordance with Section 12 below.

1. DEFINITIONS.

"Affiliate" means any entity that directly or indirectly controls, is controlled by, or is under common control with the subject entity. "Control," for purposes hereof, means direct or indirect ownership or control of more than 50% of the voting interests of the subject entity.

"Authorized Contractors" means independent contractors, licensors or subcontractors that assist Acquia in the delivery of the Services.

"Customer Applications" means all software programs, including Drupal, that Customer uses on the Platform as a Service. Subscription Services do not fall within the meaning of Customer Applications.

"Customer Data" means all data, records, files, images, graphics, audio, video, photographs, reports, forms and other content and material, in any format, that are submitted, stored, posted, displayed, transmitted or otherwise used with the Subscription Services and includes Regulated Data for which the applicable Subscription Services have been subscribed by Customer.

"Data Center Region" refers to the geographic region in which the Platform environment is physically located and the Customer Data is housed.

"Deliverable" means any work product, deliverables, programs, interfaces, modifications, configurations, reports, or documentation developed or delivered in the performance of Professional Services.

"Documentation" means the Guide as updated from time to time.

"Guide" means the documented descriptions of the products and services that are applicable to the Services under Customer's Order and is made accessible via the URL at https://docs.acquia.com/guide. The Guide is subject to change at Acquia's discretion to reflect changes in technology, industry practices and patterns of system use; however, Acquia's changes to the Guide will not result in a material reduction in the level of performance or availability of the applicable Services provided to Customer for the duration of the Subscription Term.

"Order Form" or **"Order"** means each ordering document for Services purchased from Acquia hereunder executed by Acquia and Customer from time to time. Customer Affiliates may purchase Services subject to this Agreement by executing Order Forms hereunder.

"PaaS", "Platform as a Service", or "Platform" means the cloud platform ordered by Customer under an Order Form and made available by Acquia to Customer as a managed service.

"Professional Services" means fee-based migration, implementation, training or consulting services that Acquia performs as described in an Order Form or SOW, but excluding Support Services.

"Regulated Data" means individual personal data to which Acquia is exposed during the provision of Services that is regulated by various acts, legislations and directives relating to privacy and security requirements for its protection and processing, both in the United States and elsewhere in world.

"Services" means the Subscription Services and Professional Services that Customer may purchases under an Order Form or SOW.

"Statement of Work" or "SOW" means a statement of work entered into and executed by the parties describing Professional Services to be provided by Acquia to Customer.

"Subscription Services" means SaaS, PaaS, and associated Support Services, as applicable.

"SaaS" or "Software as a Service" means the software ordered by Customer under an Order Form and made available by Acquia to Customer online via the applicable customer logins.

"Support Services" means the level of support services purchased by Customer pursuant to an Order Form.

"Third Party Marketplace" means any non-Acquia products or services made available as an accommodation on Acquia's website, which are subject to change during the Subscription Term.

2. SUBSCRIPTION SERVICES

2.1. Provision of Subscription Services. Acquia will make the Subscription Services available to Customer pursuant to this Agreement, the Guide and the relevant Order Form during the subscription term as set forth in the Order Form (the **"Subscription Term"**). Acquia, its Affiliates and its Authorized Contractors may perform certain aspects of the Subscription Services, such as service administration and Support Services, as well as other Services (including Professional Services and disaster recovery), from locations and/or through the use of Authorized Contractors, worldwide. The Order shall also set forth any Regulated Data to be provided by Customer and the relevant Subscription Services. Customer's use of the Subscription Services includes the right to access all functionality available in the purchased Subscription Services during the Subscription Term and any renewals thereto. Subsequent updates, upgrades, enhancements to the Subscription Services made generally available to all subscribing customers will be made available to Customer at no additional charge, but the purchase of Subscription Services is not contingent on the delivery of any future functionality or features. New features, functionality or enhancements to the Subscription Services may be marketed separately by Acquia and may require the payment of additional fees. Acquia will determine, in its sole discretion, whether access to such new features, functionality or enhancements will require an additional fee.

2.2 Trial Services. From time to time Acquia may invite Customer to try, at no charge, Acquia products or services not generally available to Acquia customers (**"Trial Services"**). Customer may accept or decline any such trial in Customer's sole discretion. Any Trial Services will be clearly designated as trial, beta, pilot, limited release, or by a similar description on the applicable Order. Unless otherwise set forth in an Order, Trial Services are provided for evaluation purposes and not for production use. Acquia may provide Customer with product, support, engineering and/or technical services on an "as needed" basis as determined by Acquia in its sole discretion. Such services may include, for example, but without limitation, reviewing Customer's goals and objectives; assessing the current state of Customer's infrastructure, files, and databases; and planning implementation of the Trial Services. Acquia shall be under no obligation to provide such services, or to make any tests, fixes, workarounds, revisions, or repairs to the Trial Services, to maintain the Trial Services at any Customer-desired level of performance, to keep to keep the Trial Services in operating condition, or to market or license the Trial Services. Trial Services may contain bugs or errors, and may be subject to additional terms. TRIAL SERVICES ARE NOT CONSIDERED "SERVICES" HEREUNDER AND ARE PROVIDED "AS IS" WITH NO EXPRESS OR IMPLIED WARRANTY. Customer shall have sole responsibility and Acquia assumes no liability for any Customer Data or Regulated Data that Customer may choose to upload on the Trial Services. Acquia may, in its sole discretion, discontinue Trial Services at any time.

2.3. Third Party Marketplace. As part of the Subscription Services, Acquia may provide access to the Third Party Marketplace solely as an accommodation to Customer. Customer may choose to use any, all or none of such Third Party Marketplace at its sole discretion. Customer's use of the Third Party Marketplace is subject to such provider's terms and conditions and any such terms and conditions associated with such use are solely between Customer and such third party provider. Acquia does not provide any Support Services for Third Party Marketplace products and services.

3. SECURITY AND DATA PRIVACY

3.1. Security. Acquia shall maintain a security framework of policies, procedures and controls that includes administrative, physical and technical safeguards for the protection of the security and integrity of the Subscription Services, and of the Customer Data contained within the Subscription Services ("Safeguards") using the capabilities of currently available technologies and in accordance with prevailing industry practices and standards, such Safeguards shall be materially consistent with Acquia's implementation of NIST 800-53 which forms the basis of Acquia's current FedRAMP certification. Those safeguards will include, but will not be limited to, measures for preventing access, use, modification or disclosure of Customer Data by Acquia personnel except (a) to provide the Subscription Services and prevent or address service or technical problems, (b) as compelled by law, or (c) as Customer expressly permits in writing.

3.2 Internal Controls. The internal controls of the Subscription Services are subject to periodic testing by independent third party audit organizations with Service Organization Controls 1 (SOC 1), SOC 2 audits and ISO 27001 certification or surveillance audits performed annually. Such audits and certifications may be based on the Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organization, the International Standard on Assurance Engagements (ISAE) No. 3402, Assurance Reports on Controls at a Service Organization, the Trust Services Principles, specifically Security and Availability respectively, or ISO/IEC 27001:2013 (ISO 27001). Customer may, upon prior written request, request a copy of the current published audit report available for the Subscription Services. Such audit reports, and the information they contain, are Acquia Confidential Information, and must be handled by Customer accordingly. Such reports may be used solely by Customer to evaluate the design and operating effectiveness of defined controls applicable to Subscription Services and are provided without any warranty.

3.3. Data Privacy. In performing Subscription Services, Acquia will comply with the Acquia Privacy Policy available at https://www.acquia.com/about-us/legal/privacy-policy and incorporated herein by reference. The Acquia Privacy Policy is subject to change at Acquia's discretion; however, Acquia policy changes will not result in a material reduction in the level of protection provided for Customer Data during the Subscription Term.

3.4 Data Center Region. Customer may select the Data Center Region in which the PaaS environment will reside and may identify such region in the Order Form. Acquia will not move the selected Data Center Region without Customer's written consent or unless required to comply with the law or requests of a governmental or regulatory body (including subpoenas or court orders). Customer consents to Acquia's collection, use and disclosure of information associated with the Subscription Services to the processing of Customer Data in, and transfer of Customer Data into, the Data Center Region Customer selects.

4. CUSTOMER OBLIGATIONS

4.1. Responsibilities. Customer shall (i) access and use the Services in accordance with this Agreement, applicable laws and government regulations and Acquia's Acceptable Use Policy available at https://www.acquia.com/about-us/legal/acquia-acceptable-use-policy; (ii) be responsible for the accuracy, quality and legality of Customer Data and the means by which Customer acquired Customer Data; (iii) not cause, or otherwise request that Acquia create, receive, maintain or transmit Regulated Data for Customer or on Customer's behalf in connection with the Services without first subscribing to the required applicable Subscription Services; (iv) use commercially reasonable efforts to prevent unauthorized access to or use of the Services, and notify Acquia promptly of any such unauthorized access or use, (v) take commercially reasonable steps necessary to ensure the security and compliance of the Customer Applications; and (vi) be responsible for obtaining and maintaining all telephone, computer hardware, Internet access services and other equipment or services needed to access and use the Services and all costs and fees associated therewith.

4.2. Regulated Data. Customer is responsible for its legal and regulatory compliance in its use of any Subscription Services and shall make Acquia aware of any technical requirements that result from its regulatory obligations prior to contract execution. If available, Customer may order Subscription Services from Acquia designed to address particular data protection requirements applicable for the processing of Regulated Data within the Subscription Services environment. Where Customer's use of the Subscription Services includes the processing of personal data subject to the EU Data Protection Directive 95/46/EC, Acquia will provide Customer with an Acquia data protection agreement with the EU Standard Contractual Clauses, which upon the parties' mutual execution, will form part of this Agreement.

4.3 Restrictions. Customer shall not (a) license, sublicense, sell, resell, rent, lease, transfer, distribute or otherwise similarly exploit the Subscription Services; (b) use or permit others to use any security testing tools in order to probe, scan or attempt to penetrate or ascertain the security of the Subscription Services; (c) copy, create a derivative work of, reverse engineer, reverse assemble, disassemble, or decompile the Subscription Services or any part thereof or otherwise attempt to discover any source code or modify the Subscription Services; or (d) disclose any benchmark or performance tests of the Services.

4.4. Compliance. Acquia monitors the Subscription Services for any unauthorized conduct (including any violation of this Agreement, Acquia's Acceptable Use Policy, any applicable law or third party right) and may suspend access to the Subscription Services and any publicly facing Customer Applications to the extent and for the duration of any such violation if Customer is engaged in, or Acquia in good faith believes Customer is engaged in, such violation. Acquia will attempt to contact Customer prior to or contemporaneously with such suspension; provided, however, that Acquia's exercise of the suspension rights herein shall not be conditioned upon Customer's receipt of any notification. A suspension may take effect for Customer's entire account and Customer understands that such suspension would therefore include Affiliate and/or user sub-accounts. Customer agrees that Acquia will not be liable to Customer or to any Affiliate or user or any other third party if Acquia exercises its suspension rights as permitted by this Section.

5. PROFESSIONAL SERVICES

5.1. Standard Professional Services. A description of Acquia's standard Professional Services offerings, including training, and workshops, may be found in the Guide. Standard Professional Services may be identified in an Order Form without the need for issuance of an SOW.

5.2. Other Professional Services. For any non-standard Professional Services, Acquia will provide Customer with Professional Services as set forth in the applicable SOW. Each SOW will include, at a minimum: (i) a description of the Professional Services and any Deliverable to be delivered to Customer; (ii) the scope of Professional Services; (iii) the schedule for the provision of such Professional Services; and (iv) the applicable fees and payment terms for such Professional Services, if not specified elsewhere.

5.3. Change Orders. Changes to an SOW or Order Form will require, and shall become effective only when, fully documented in a written change order (each a "Change Order") signed by duly authorized representatives of the parties prior to implementation of the changes. Such changes may include, for example, changes to the scope of work and any corresponding changes to the estimated fees and schedule. Change Orders shall be deemed part of, and subject to, this Agreement.

5.4. Staffing, Designated Contact and Cooperation. Acquia shall have sole discretion in staffing the Services and may use Authorized Contractors to assist in the delivery of the Professional Services, provided that Acquia shall remain liable for the actions or omissions of such Authorized Contractors. Each party will designate in each SOW an individual who will be the primary point of contact between the parties for all matters relating to the Professional Services to be performed thereunder. Customer will cooperate with Acquia, will provide Acquia with accurate and complete information, will provide Acquia with such assistance and access as Acquia may reasonably request, and will fulfill its responsibilities as set forth in this Agreement and the applicable SOW. If Acquia personnel are required to be present on a Customer site, Customer will provide adequate workspace and may provide reasonable worksite safety and security rules to which such personnel are to conform.

6. FEES AND PAYMENT

6.1. Fees. Customer shall pay all fees specified in each Order Form and SOW. Except as otherwise specified herein or in an Order Form or SOW, (i) fees are quoted and payable in United States dollars, (ii) fees are based on Services purchased, regardless of usage, (iii) payment obligations are non-cancelable and fees paid are non-refundable, (iv) all Services shall be deemed accepted upon delivery, and (v) the Subscription Services purchased cannot be decreased during the relevant Subscription Term. Customer shall reimburse Acquia for out-of-pocket expenses incurred by Acquia in connection with its performance of Services. Acquia will provide Customer with reasonably detailed invoices for such expenses. All amounts payable under this Agreement will be made without setoff or counterclaim, and without any deduction or withholding.

6.2. Invoicing and Payment. All fees for Subscription Services will be invoiced in advance and, unless otherwise set forth in an SOW, all fees and expenses for Professional Services will be invoiced monthly in arrears on a time and materials basis. Except as otherwise stated in the applicable Order Form or SOW, Customer agrees to pay all invoiced amounts within thirty (30) days of invoice date.

6.3. Overdue Charges. If Acquia does not receive fees by the due date, then, at Acquia's discretion, such fees may accrue late interest at the rate of 1.5% of the outstanding balance per month, or the maximum rate permitted by law, whichever is lower, from the date such payment was due until the date paid.

6.4. Payment Disputes. Acquia agrees that it will not exercise its rights under Section 6.3 (Overdue Charges) if Customer is disputing the applicable charges reasonably and in good faith and is cooperating diligently to resolve the dispute.

6.5. Taxes. Fees for Services exclude all sales, value added and other taxes and duties imposed with respect to the sale, delivery, or use of any product or Services covered hereby. Customer is responsible for payment of all taxes, levies, duties, assessments, including but not limited to value-added, sales, use or withholding taxes, assessed or collected by any governmental body (collectively, "**Taxes**") arising from Acquia's provision of the Services hereunder, except any taxes assessed on Acquia's net income. If Acquia is required to directly pay or collect Taxes related to Customer's use or receipt of the Services hereunder, Customer agrees to promptly reimburse Acquia for any amounts paid by Acquia.

7. PROPRIETARY RIGHTS

7.1. Subscription Services. Acquia, its licensors and its service providers own all right, title and interest in and to the Subscription Services, including all related intellectual property rights. Acquia reserves all rights in and to the Subscription Services not expressly granted to Customer under this Agreement. Customer will not delete or in any manner alter the copyright, trademark, and other proprietary notices of Acquia.

7.2. Customer Data and Customer Applications. To enable Acquia to provide Customer with the Subscription Services, Customer hereby grants Acquia, its Affiliates and sublicensees (including Authorized Contractors whose technologies and services interface with the Subscription Services that include the Customer Data and Customer Applications) a worldwide, royalty-free, non-exclusive, limited term license to use, process, store, display and transmit Customer Data and Customer Applications solely as necessary for Acquia to provide the Services in accordance with this Agreement. Subject to the limited licenses granted herein, Acquia acquires no right, title or interest from Customer or Customer licensors hereunder in or to Customer Data and Customer Applications, including any intellectual property rights therein.

7.3. Deliverables. Excluding any property that constitutes Outside Property, any Deliverables shall be the sole property of Customer upon Customer's payment in full of all associated Professional Services fees. Acquia shall execute and, at Customer's written request, require its personnel to execute any document that may be necessary or desirable to establish or perfect Customer's rights to the ownership of such Deliverables. For purposes of this Agreement, "Outside Property" means any and all technology and information, methodologies, data, designs, ideas, concepts, know-how, techniques, user-interfaces, templates, documentation, software, hardware, modules, development tools and other tangible or intangible technical material or information that Acquia possesses or owns prior to the commencement of Professional Services or which it develops independent of any activities governed by this Agreement, and any derivatives, modifications or enhancements made to any such property. Outside Property shall also include any enhancements, modifications or derivatives made by Acquia to the Outside Property while performing Professional Services hereunder, and any software, modules, routines or algorithms which are developed by Acquia during the term in providing the Professional Services to Customer, provided such software, modules, routines or algorithms have general application to work performed by Acquia for its other customers and do not include any content that is specific to Customer or which, directly or indirectly, incorporate or disclose Customer's Confidential Information.

7.4 Outside Property License. To the extent that Acquia incorporates any Outside Property into any Deliverables, then Acquia hereby grants Customer a limited, royalty-free, non-exclusive, non-transferable (subject to Section 14.11) license to use such Outside Property delivered to Customer solely as necessary for and in conjunction with Customer 's use of the Deliverables.

8. CONFIDENTIALITY

8.1. Definition of Confidential Information. "**Confidential Information**" means all confidential or proprietary information of a party (**"Disclosing Party"**) disclosed to the other party (**"Receiving Party"**), whether orally or in writing, that is designated as confidential or reasonably should be understood to be confidential given the nature of information and the circumstances of disclosure. Without limiting the coverage of these confidentiality obligations, the parties acknowledge and agree that Confidential Information of each party shall include the terms and conditions of this Agreement (including pricing and other terms set forth in all Order Forms and/or SOWs hereunder), related benchmark or similar test results, other technology and technical information, security information, security audit reports, and business and marketing plans, except that Acquia may reference and use Customer's name, logos and the nature of the Services provided hereunder in Acquia's business development and marketing efforts.

8.2. Exceptions. Confidential Information shall not include information that (i) is or becomes publicly available without a breach of any obligation owed to the Disclosing Party, (ii) is already known to the Receiving Party at the time of its disclosure by the Disclosing Party, without a breach of any obligation owed to the Disclosing Party, (iii) following its disclosure to the Receiving Party, is received by the Receiving Party from a third party without breach of any obligation owed to Disclosing Party, or (iv) is independently developed by Receiving Party without reference to or use of the Disclosing Party's Confidential Information.

8.3. Protection of Confidential Information. The Receiving Party shall use the same degree of care used to protect the confidentiality of its own

Confidential Information of like kind (but in no event less than reasonable care), and, except with Disclosing Party's written consent, shall (i) not use any Confidential Information of Disclosing Party for any purpose outside the scope of this Agreement and (ii) limit access to Confidential Information of Disclosing Party to those of its and its Affiliates' employees, contractors and agents who need such access for purposes consistent with this Agreement and who have a duty or obligation of confidentiality no less stringent than that set forth herein.

8.4. Compelled Disclosure. The Receiving Party may disclose Confidential Information of the Disclosing Party to the extent required by applicable law, regulation or legal process, provided that the Receiving Party (i) provides prompt written notice to the extent legally permitted, (ii) provides reasonable assistance, at Disclosing Party's cost, in the event the Disclosing Party wishes to oppose the disclosure, and (iii) limits disclosure to that required by law, regulation or legal process.

9. REPRESENTATIONS, WARRANTIES AND DISCLAIMERS

9.1. Acquia Representations & Warranties. Acquia represents and warrants that (i) Acquia has the legal authority to enter into this Agreement, (ii) the Subscription Services will materially conform with the relevant Documentation, (iii) the functionality and security of the Subscription Services will not be materially decreased during a Subscription Term, and (iv) Professional Services will be performed in a competent and workmanlike manner consistent with generally accepted industry standards.

9.2. Remedies. For any failure of any Subscription Services or Professional Services, as applicable, to conform to their respective warranties, Acquia's liability and Customer's sole and exclusive remedy shall be for Acquia, in the case of a breach of the warranty set forth in Section 9.1 (ii), (iii), and/or (iv), to use commercially reasonable efforts to correct such failure; or, in the case of a breach of the warranty set forth in Section 9.1 (iv) to re-perform the affected Professional Services. If the foregoing remedies are not commercially practicable, Acquia may, in its sole discretion, terminate the applicable Order Form or SOW upon providing Customer with written notice thereof, and, as Customer's sole and exclusive remedy, refund to Customer: (a) in the case of breach of the warranty set forth in Section 9.1(ii), any Subscription Services fees paid by Customer with respect to the unexpired portion of the current Subscription Term for the non-conforming Subscription Services; or (b) in the case of breach of the warranty set forth in Section 9.1(iv), any fees paid by Customer for the portion of Professional Services giving rise to the breach.

9.3. Customer Representations & Warranties. Customer represents and warrants that (i) it has the legal authority to enter into this Agreement, and (ii) it will use the Services in accordance with the terms and conditions set forth in this Agreement and in compliance with all applicable laws, rules and regulations.

9.4. Disclaimer. EXCEPT AS EXPRESSLY PROVIDED HEREIN, ACQUIA MAKES NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, ORAL OR WRITTEN, STATUTORY OR OTHERWISE, AND ACQUIA HEREBY DISCLAIMS ALL IMPLIED WARRANTIES AND CONDITIONS, INCLUDING, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY WITH RESPECT TO THE QUALITY, PERFORMANCE, ACCURACY OR FUNCTIONALITY OF THE SERVICES OR THAT THE SERVICES ARE OR WILL BE ERROR FREE OR WILL ACCOMPLISH ANY PARTICULAR RESULT.

10. MUTUAL INDEMNIFICATION

10.1. Indemnification by Acquia. Acquia shall indemnify, defend and hold Customer harmless from and against any judgments, settlements, costs and fees reasonably incurred (including reasonable attorney's fees) resulting from any claim, demand, suit, or proceeding made or brought against Customer by a third party alleging that the use of the Subscription Services hereunder infringes or misappropriates the valid intellectual property rights of a third party (a **"Claim Against Customer"**); provided that Customer (a) promptly gives Acquia written notice of the Claim Against Customer; (b) gives Acquia sole control of the defense and settlement of the Claim Against Customer (provided that Acquia may not settle any Claim Against Customer unless the settlement unconditionally releases Customer of all liability); and (c) provides to Acquia all reasonable assistance, at Acquia's expense. In the event of a Claim Against Customer, or if Acquia reasonably believes the Subscription Services may infringe or misappropriate, Acquia may in Acquia's sole discretion and at no cost to Customer (i) modify the Subscription Services so that they no longer infringe or misappropriate, without breaching Acquia's warranties hereunder, (ii) obtain a license for Customer's continued use of Subscription Services in accordance with this Agreement, or (iii) terminate Customer's subscriptions for such Subscription Services and refund to Customer any prepaid fees covering the remainder of the term of such subscriptions after the effective date of termination. Notwithstanding the foregoing, Acquia shall have no obligation to indemnify, defend, or hold Customer harmless from any Claim Against Customer to the extent it arises from Customer Data or Customer Applications, use by Customer after notice by Acquia to discontinue use of all or a portion of the Subscription Services or Customer's breach of this Agreement.

10.2. Indemnification by Customer. Customer shall indemnify, defend and hold Acquia harmless from and against any judgments, settlements, costs and fees reasonably incurred (including reasonable attorney's fees) resulting from any claim, demand, suit or proceeding made or brought against Acquia by a third party alleging that Customer Data or Customer Applications infringes or misappropriates the intellectual property rights of a third party, violates applicable law or causes tortious harm to a third party (a **"Claim Against Acquia"**); provided that Acquia (a) promptly gives Customer written notice of the Claim Against Acquia; (b) gives Customer sole control of the defense and settlement of the Claim Against Acquia (provided that Customer may not settle any Claim Against Acquia unless the settlement unconditionally releases Acquia of all liability); and (c) provides to Customer all reasonable assistance, at Customer's expense.

10.3. Exclusive Remedy. This Section 10 states the indemnifying party's sole liability to, and the indemnified party's exclusive remedy against, the other party for any type of claim described in this Section.

11. LIMITATION OF LIABILITY

11.1. Limitation of Liability. OTHER THAN EACH PARTY'S OBLIGATIONS SET FORTH IN SECTION 10 (MUTUAL INDEMNIFICATION), NEITHER PARTY'S TOTAL AGGREGATE LIABILITY RELATING TO THIS AGREEMENT (WHETHER IN CONTRACT OR TORT OR UNDER ANY OTHER THEORY OF LIABILITY) SHALL EXCEED THE AMOUNT PAID OR PAYABLE BY CUSTOMER HEREUNDER IN THE 12 MONTHS PRECEDING THE APPLICABLE INCIDENT.

11.2. Exclusion of Consequential and Related Damages. NEITHER PARTY SHALL HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY LOST PROFITS OR REVENUES OR FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER OR PUNITIVE DAMAGES HOWEVER CAUSED, WHETHER IN CONTRACT, TORT OR UNDER ANY OTHER THEORY OF LIABILITY, AND WHETHER OR NOT THE PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE FOREGOING DISCLAIMER WILL NOT APPLY TO THE EXTENT PROHIBITED BY LAW.

12. TERM AND TERMINATION

12.1. Term of Agreement. This Agreement commences on the Effective Date and continues until otherwise terminated, by written agreement of the parties, in accordance with Section 12.3 or upon the expiration of the last Subscription Term or renewal thereof.

12.2. Term of Subscription Services. Subscription Services purchased by Customer commence on the start date specified in the applicable Order Form and continue for the subscription term specified therein (each, a **"Subscription Term"**). Except as otherwise specified in such Order Form, the Subscription Services shall automatically renew for successive one-year periods, unless and until terminated by either party in accordance herewith or either party provides written notice of non-renewal to the other party at

least 30 days prior to the end of the then-current Subscription Term. Acquia may adjust the pricing applicable to any renewal of any then-current Subscription Term, by providing Customer with written notice thereof at least 30 days prior to the end of such term.

12.3. Termination for Cause. A party may terminate this Agreement (or, at such party's option, the individual Order Forms or SOWs affected by the applicable breach), for cause (i) upon 30 days written notice to the other party of a material breach if such breach remains uncured at the expiration of such same 30 day period, or (ii) automatically if the other party becomes the subject of a petition in bankruptcy or other proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors.

12.4. Refund upon Termination. Upon termination for cause by Customer and upon Customer's written request, Acquia shall refund to Customer the prepaid fees covering the remainder of the applicable Subscription Term after the effective date of termination. Upon termination for cause by Acquia, Customer shall pay the unpaid fees covering the remainder of the Subscription Term of the Order Forms after the effective date of termination. In no event shall any termination relieve Customer of the obligation to pay all fees payable to Acquia for the period prior to the effective date of termination.

12.5. Data Portability and Deletion. Upon written request made by Customer within 30 days of termination or expiration of the Subscription Services, Acquia will make Customer Data and Customer Applications available to Customer for export or download as provided in the Documentation. At the end of such 30 day period, Acquia will delete or otherwise render inaccessible any Customer Data and Customer Applications, unless legally prohibited. Acquia has no obligation to retain the Customer Data for Customer purposes after this 30 day post termination period.

12.6. Survival. Section 7 (Proprietary Rights), 8 (Confidentiality), 9.4 (Disclaimer), 10 (Mutual Indemnification), 11 (Limitation of Liability), 12.4 (Refund upon Termination), 13 (Notices, Governing Law and Jurisdiction) and 14 (General Provisions) and any other rights and obligations of the parties hereunder that by their nature are reasonably intended to survive termination or expiration, shall survive any termination or expiration of this Agreement.

13. NOTICES, GOVERNING LAW AND JURISDICTION

13.1. Manner of Giving Notice. Except as otherwise specified in this Agreement, all notices, permissions and approvals hereunder shall be in writing and shall be deemed to have been given upon (i) personal delivery, (ii) the fifth business day after being sent by certified mail return receipt requested, or (iii) the first business day after sending by a generally recognized international guaranteed overnight delivery service. Each party shall send all notices, demands, requests or other communications which may be or are required to be given hereunder to the other party at the address set forth in the applicable Order Form or SOW, as such party may update such information from time to time, with, in the case of notices sent by Customer, a copy sent to the Acquia Legal Department at the address first set forth above.

13.2. Governing Law and Jurisdiction. If Customer is entering into this Agreement from a European Union member country, then this Agreement is governed by the laws of England and subject to the exclusive jurisdiction of the courts of England and Wales. If Customer is entering into this Agreement from Australia, then this Agreement is governed by the laws of New South Wales and subject to the exclusive jurisdiction of the courts of Sydney. Otherwise, this Agreement shall be governed and construed in accordance with the laws of the Commonwealth of Massachusetts, excluding its conflicts of law rules. Any civil action or legal proceeding arising out of or relating to this Agreement shall be brought in the courts of record of the Commonwealth of Massachusetts in Suffolk County or the United States District Court, Eastern District of Massachusetts. Each party consents to the jurisdiction of such court in any such civil action or legal proceeding and waives any objection to the laying of venue of any such civil action or legal proceeding in such court. Notwithstanding the foregoing, the parties acknowledge that any unauthorized disclosure of Confidential Information or any actual or alleged infringement of such party's or third party's intellectual property rights might cause the other party to suffer irreparable harm for which damages would be an inadequate remedy and that, in such event, the aggrieved party may seek, in addition to any other available remedies, injunctive and other equitable relief in any state, federal, or national court of competent jurisdiction, without bond and without the necessity of showing actual monetary damages. The United Nations Convention on Contracts for the International Sale of Goods and the Uniform Computer Information Transactions Act do not apply to the Agreement.

13.3. Waiver of Jury Trial. Each party hereby waives any right to jury trial in connection with any action or litigation in any way arising out of or related to this Agreement.

14. GENERAL PROVISIONS

14.1. Import and Export Compliance. Each party shall comply with all applicable import, re-import, export and re-export control laws, treaties, agreements, and regulations. Export controls may include, but are not limited to, those of the Export Administration Regulations of the U.S. Department of Commerce (EAR), the Department of State International Traffic in Arms Regulations (ITAR), and country-specific economic sanctions programs implemented by the Office of Foreign Assets Control (OFAC), which may restrict or require licenses for the export of items from the United States and their re-export from other countries. Each party represents that it is not named on any U.S. government denied-party list. Customer shall not permit users to access or use Services in a U.S.-embargoed country or in violation of any U.S. export law or regulation.

14.2. Anti-Corruption. Neither party has received or been offered any illegal or improper bribe, kickback, payment, gift, or thing of value from any of the other party's employees or agents in connection with this Agreement. If a party learns of any violation of the above restriction, such party will use reasonable efforts to promptly notify the other party.

14.3. Federal Government End Use Provisions. If the Services are being or have been acquired with U.S. Federal Government funds, or Customer is an agency, department, or other entity of the United States Government ("Government"), the use, duplication, reproduction, release, modification, disclosure or transfer of the Services, or any related documentation of any kind, including technical data, manuals or Acquia Property is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995), as applicable. Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire the software and Services with only those rights set forth in this Agreement and any amendment hereto.

14.4. Subscription Service Analyses. Acquia may (i) compile statistical and other information related to the performance, operation and use of the Subscription Services, and (ii) use, and share data from the Subscription Services environment in aggregated form for security and operations management, to create statistical analyses, and for research and development purposes (clauses i and ii are collectively referred to as 'Subscription Service Analyses"). Subscription Service Analyses will not incorporate any information in a form that could serve to identify Customer or an individual. Acquia retains all intellectual property rights in Subscription Service Analyses.

14.5. Relationship of the Parties. The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary or employment relationship between the parties.

14.6. Non-Solicitation. Customer agrees that during the term of each Order Form and/or SOW and for twelve (12) months thereafter, it will not recruit or otherwise solicit for employment any person employed by Acquia who

participated in the performance of Services under the applicable Order Form and/or SOW. Nothing in this clause shall be construed to prohibit individual Acquia employees from responding to public employment advertisements, postings or job fairs of Customer, provided such response is not prompted by Customer intentionally circumventing the restrictions of this Section.

14.7. No Third-Party Beneficiaries. There are no third-party beneficiaries to this Agreement.

14.8. Waiver. No failure or delay by either party in exercising any right under this Agreement shall constitute a waiver of that right.

14.9. Force Majeure. Neither party shall be liable under this Agreement for delays, failures to perform, damages, losses or destruction, or malfunction of any equipment, or any consequence thereof, caused or occasioned by, or due to fire, earthquake, flood, water, the elements, labor disputes or shortages, utility curtailments, power failures, explosions, civil disturbances, governmental actions, shortages of equipment or supplies, unavailability of transportation, acts or omissions of third parties, or any other cause beyond its reasonable control. This Section does not excuse either party's obligation to take reasonable steps to follow its normal disaster recovery procedures or Customer's obligation to pay for the Services. If the force majeure event continues for more than thirty (30) calendar days, then either party may terminate the Agreement upon written notice to the other party.

14.10. Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be contrary to law, the provision shall be modified by the court and interpreted so as best to accomplish the objectives of the original provision to the fullest extent permitted by law, and the remaining provisions of this Agreement shall remain in effect.

14.11. Assignment. Neither party may assign its rights and obligations hereunder, either in whole or in part, whether by operation of law or otherwise, without the prior written consent of the other party. Notwithstanding the foregoing, either party may assign this Agreement in its entirety (including all Order Forms and SOWs), without consent of the other party, to its Affiliate or in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets not involving a direct competitor of the other party. Subject to the foregoing, this Agreement shall bind and inure to the benefit of the parties, their respective successors and permitted assigns.

14.12. Entire Agreement. This Agreement constitutes the entire agreement between the parties as it relates to the subject matter and supersedes all prior and contemporaneous agreements, proposals or representations, written or oral, concerning relating to the same. No modification, amendment, or waiver of any provision of this Agreement shall be effective unless in writing and signed by both parties with the exception that Acquia may, from time to time, modify the terms of the Guide in its sole discretion. To the extent of any conflict or inconsistency between the provisions of this Agreement, the Guide, any Order Form or SOW, the terms of such Order Form or SOW shall prevail. Notwithstanding any language to the contrary therein, no terms or conditions stated in a Customer purchase order or other order documentation (excluding Order Forms and/or SOWs) shall be incorporated into or form any part of this Agreement, and all such terms or conditions shall be null and void.

Google Cloud Master Agreement – Public Sector (Partner)

This Google Cloud Master Agreement is comprised of the Google Cloud Master Agreement General Terms ("General Terms"), and all Services Schedules that are incorporated by reference into the Google Cloud Master Agreement (collectively, the "Agreement").

Google Cloud Master Agreement General Terms

1. Services. After the Customer and Reseller and/or Distributor complete and execute an Order Form incorporating this Agreement, Google will provide the Services specified in the Order Form in accordance with the Agreement, including the SLAs, and Customer and its End Users may use the Services in accordance with the Services Schedule.

2. Customer Obligations.

2.1. Consents. Customer is responsible for any consents and notices required to permit (a) Customer's use and receipt of the Services and (b) Google's accessing, storing, and processing of data provided by Customer (including Customer Data, if applicable) under the Agreement.

2.2. Compliance. Customer will (a) ensure that Customer and its End Users' use of the Services complies with the Agreement, (b) use commercially reasonable efforts to prevent and terminate any unauthorized access or use of the Services, and (c) promptly notify Google of any unauthorized use of, or access to, the Services of which Customer becomes aware.

2.3. Use Restrictions. Customer will not, and will not allow End Users to, (a) copy, modify, create a derivative work of, reverse engineer, decompile, translate, disassemble, or otherwise attempt to extract any of the source code of, the Services (except to the extent such restriction is expressly prohibited by applicable law); (b) sell, resell, sublicense, transfer, or distribute the Services; or (c) access or use the Services (i) for High Risk Activities; (ii) in a manner intended to avoid incurring Fees; (iii) for materials or activities that are subject to the International Traffic in Arms Regulations (ITAR) maintained by the United States Department of State; (iv) in a manner that breaches, or causes the breach of, Export Control Laws; or (v) to transmit, store, or process health information subject to United States HIPAA regulations except as permitted by an executed HIPAA BAA with Google (if approved), or an executed HIPAA BAA with Google's Reseller or Distributor.

3. RESERVED

4. Intellectual Property.

4.1. Intellectual Property Rights. Except as expressly described in the Agreement, the Agreement does not grant either party any rights, implied or otherwise, to the other's content or Intellectual Property. As between the parties, Customer retains all Intellectual Property Rights in Customer Data and Customer Applications, and Google retains all Intellectual Property Rights in the Services and Software.

4.2. Feedback. At its option, Customer may provide feedback and suggestions about the Services to Google ("Feedback"). If Customer provides Feedback, then Google and its Affiliates may use that Feedback without restriction and without obligation to Customer.

5. Confidentiality.

5.1. Use and Disclosure of Confidential Information. The Recipient will only use the Disclosing Party's Confidential Information to exercise its rights and fulfill its obligations under the Agreement, and will use reasonable care to protect against the disclosure of the Disclosing Party's Confidential Information. Notwithstanding any other provision in the Agreement, the Recipient may disclose the Disclosing

Party's Confidential Information (a) to its Delegates who have a need to know and who are bound by confidentiality obligations at least as protective as those in this Section 5 (Confidentiality); (b) with the Disclosing Party's written consent; or (c) subject to Section 5.2 (Legal Process), as strictly necessary to comply with Legal Process.

5.2. Legal Process. If the Recipient receives Legal Process for the Disclosing Party's Confidential Information, the Recipient will: (a) promptly notify the Disclosing Party prior to such disclosure unless the Recipient is legally prohibited from doing so; (b) attempt to redirect the third party to request it from the Disclosing Party directly; (c) comply with the Disclosing Party's reasonable requests to oppose disclosure of its Confidential Information; and (d) use commercially reasonable efforts to object to, or limit or modify, any Legal Process that the Recipient reasonably determines is overbroad, disproportionate, incompatible with applicable law, or otherwise unlawful. To facilitate the request in (b), the Recipient may provide the Disclosing Party's basic contact information to the third party. Google acknowledges that the Customer may be subject to and must comply with the Freedom of Information Act (FOIA) or similar Open Records/Sunshine law.

6. Marketing and Publicity. Customer may state publicly that it is a Google customer and display Google Brand Features in accordance with the Trademark Guidelines. Google may use Customer's name and Brand Features in online or offline promotional materials of the Services. Each party may use the other party's Brand Features only as permitted in the Agreement. Any use of a party's Brand Features will inure to the benefit of the party holding Intellectual Property Rights to those Brand Features.

7. RESERVED.

8. Disclaimer. Except as expressly provided for in the Agreement, to the fullest extent permitted by applicable law, Google (a) does not make any warranties of any kind, whether express, implied, statutory, or otherwise, including warranties of merchantability, fitness for a particular use, noninfringement, or error-free or uninterrupted use of the Services or Software and (b) makes no representation about content or information accessible through the Services.

9. Indemnification.

9.1. Google Indemnification Obligations. Google will defend Customer and its Covered Affiliates, and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from an allegation that the Google Indemnified Materials used in accordance with the Agreement infringe the third party's Intellectual Property Rights.

9.2. Customer Indemnification Obligations. Subject to applicable federal or state law, and without waiving sovereign immunity, Customer will defend Google and its Affiliates providing the Services and indemnify them against Indemnified Liabilities in any Third-Party Legal Proceeding to the extent arising from (a) any Customer Indemnified Materials or (b) Customer's or an End User's use of the Services in breach of the AUP or the Use Restrictions. This section will not apply if the Customer is prohibited from agreeing to any vendor indemnification requirement.

9.3. Indemnification Exclusions. Sections 9.1 (Google Indemnification Obligations) and 9.2 (Customer Indemnification Obligations) will not apply to the extent the underlying allegation arises from (a) the indemnified party's breach of the Agreement or (b) a combination of the Google Indemnified Materials or Customer Indemnified Materials (as applicable) with materials not provided by the indemnifying party under the Agreement, unless the combination is required by the Agreement.

9.4. Indemnification Conditions. Sections 9.1 (Google Indemnification Obligations) and 9.2 (Customer Indemnification Obligations) are conditioned on the following:

(a) Any indemnified party must promptly notify the indemnifying party in writing of any allegation(s) that preceded the Third-Party Legal Proceeding and cooperate reasonably with the indemnifying party to resolve the allegation(s) and Third-Party Legal Proceeding. If breach of this Section 9.4(a) prejudices the defense of the Third-Party Legal Proceeding, the indemnifying party's obligations under Section 9.1 (Google Indemnification Obligations) or 9.2 (Customer Indemnification Obligations) (as applicable) will be reduced in proportion to the prejudice.

(b) Any indemnified party must tender sole control of the indemnified portion of the Third-Party Legal Proceeding to the indemnifying party, subject to the following: (i) the indemnified party may appoint its own non-controlling counsel, at its own expense; and (ii) any settlement requiring the indemnified party to admit liability, pay money, or take (or refrain from taking) any action, will require the indemnified party's prior written consent, not to be unreasonably withheld, conditioned, or delayed.

9.5 Remedies.

(a) If Google reasonably believes the Services might infringe a third party's Intellectual Property Rights, then Google may, at its sole option and expense, (i) procure the right for Customer to continue using the Services, (ii) modify the Services to make them non-infringing without materially reducing their functionality, or (iii) replace the Services with a non-infringing, functionally equivalent alternative.

(b) If Google does not believe the remedies in Section 9.5(a) are commercially reasonable, then Google may Suspend or terminate the impacted Services. If Google terminates Services under this Section 9.5 (Remedies), then upon Customer request (i) Google will refund to Customer any unused prepaid Fees that Customer paid to Google for use of the terminated Services, and (ii) if Customer has made financial commitments in an Order Form or addendum to the Agreement, then Google will agree to amend such commitments proportional to Customer's spend on the terminated Services in the year preceding the termination of the Services. For Federal Customers, if Google does not believe the remedies in Section 9.5(a) are commercially reasonable, the parties recognize that the provisions of 28 U.S.C.§ 1498 will apply to the resolution of any patent or copyright claim made by the patent or copyright owner.

9.6 Sole Rights and Obligations. Without affecting either party's termination or Suspension rights, this Section 9 (Indemnification) states the parties' sole and exclusive remedy under the Agreement for any third-party allegations of Intellectual Property Rights infringement covered by this Section 9 (Indemnification).

10. Liability.

10.1 Limited Liabilities.

(a) To the extent permitted by applicable law and subject to Section 10.2 (Unlimited Liabilities), neither party will have any Liability arising out of or relating to the Agreement for any
(i) indirect, consequential, special, incidental, or punitive damages or
(ii) lost revenues, profits, savings, or goodwill.

(b) Each party's total aggregate Liability for damages arising out of or relating to the Agreement is limited to the Fees Customer paid under the applicable Services Schedule during the 12 month period before the event giving rise to Liability.

10.2 Unlimited Liabilities. Nothing in the Agreement excludes or limits either party's Liability for:

(a) death, personal injury, or tangible personal property damage resulting from its negligence or the negligence of its employees or agents;

(b) its fraud or fraudulent misrepresentation;
(c) its obligations under Section 9 (Indemnification);
(d) its infringement of the other party's Intellectual Property Rights;
(e) its payment obligations under the Agreement; or
(f) matters for which liability cannot be excluded or limited under applicable law.

11. Term and Termination.

11.1 Agreement Term. The Agreement, unless it expires or terminates according to the Reseller Agreement or Distributor Agreement, will remain in effect for the contract period as described in the applicable Reseller Agreement or Distributor Agreement (the "Term").

11.2 Termination for Convenience. Subject to any financial commitments in an Order Form or addendum to the Agreement, Customer may terminate the Agreement or an Order Form for convenience with 30 days' prior written notice to Reseller or Distributor.

11.3 RESERVED.

11.4 Effects of Termination. If the Agreement terminates, then all Services Schedules and Order Forms also terminate. If an Order Form terminates or expires, then after that Order Form's termination or expiration effective date, (a) all rights and access to the Services under that Order Form will terminate (including access to Customer Data, if applicable), unless otherwise described in the applicable Services Schedule, and (b) Reseller or Distributor will send Customer a final invoice (if applicable) for payment obligations under that Order Form. Termination or expiration of one Order Form will not affect other Order Forms.

11.5 Survival. The following Sections will survive expiration or termination of the Agreement: Section 4 (Intellectual Property), Section 5 (Confidentiality), Section 8 (Disclaimer), Section 9 (Indemnification), Section 10 (Liability), Section 11 (Term and Termination), Section 12 (Miscellaneous), Section 13 (Definitions), and any additional sections specified in the applicable Services Schedule.

12. Miscellaneous.

12.1 Notices. Under the Agreement, notices to Customer must be sent to the Notification Email Address and notices to Google must be sent to legal-notices@google.com. Notice will be treated as received when the email is sent. Customer is responsible for keeping its Notification Email Address current throughout the Term.

12.2 Emails. The parties may use emails to satisfy written approval and consent requirements under the Agreement.

12.3 RESERVED.

12.4 RESERVED.

12.5 Force Majeure. Neither party will be liable for failure or delay in performance of its obligations to the extent caused by circumstances beyond its reasonable control, including acts of God, natural disasters, terrorism, riots, or war.

12.6 Subcontracting. Google may subcontract obligations under the Agreement but will remain liable to Customer for any subcontracted obligations.

12.7 No Agency. The Agreement does not create any agency, partnership, or joint venture between the parties.

12.8 No Waiver. Neither party will be treated as having waived any rights by not exercising (or delaying the exercise of) any rights under the Agreement.

12.9 Severability. If any part of the Agreement is invalid, illegal, or unenforceable, the rest of the Agreement will remain in effect.

12.10 No Third-Party Beneficiaries. The Agreement does not confer any rights or benefits to any third party unless it expressly states that it does.

12.11 Equitable Relief. Nothing in the Agreement will limit either party's ability to seek equitable relief.

12.12 RESERVED.

12.13 Amendments. Except as specifically described otherwise in the Agreement, any amendment to the Agreement must be in writing, expressly state that it is amending the Agreement, and be signed by Customer and Reseller.

12.14 Independent Development. Nothing in the Agreement will be construed to limit or restrict either party from independently developing, providing, or acquiring any materials, services, products, programs, or technology that are similar to the subject of the Agreement, provided that the party does not breach its obligations under the Agreement in doing so.

12.15 URL Terms. The URL Terms are incorporated by reference into the Agreement.

12.16 Conflicting Terms. If there is a conflict among the documents that make up the Agreement, then the documents will control in the following order (of decreasing precedence): the Data Processing Addendum, the applicable Services Schedule, the General Terms, and the other URL Terms.

12.17 Conflicting Languages. If the Agreement is translated into any other language, and there is a discrepancy between the English text and the translated text, the English text will control.

12.18 RESERVED.

12.19 RESERVED.

12.20 Headers. Headings and captions used in the Agreement are for reference purposes only and will not have any effect on the interpretation of the Agreement.

12.21 Federal Customers. The Services were developed solely at private expense and are "commercial services," "commercial items," "commercial computer software," and "commercial computer software documentation," as those terms are defined within Section 2.101 of the Federal Acquisition Regulation ("FAR") and any applicable agency supplements to the FAR.

13. Definitions.

"Affiliate" means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party.

"AUP" means Google's acceptable use policy as defined in the applicable Services Schedule (if applicable).

"BAA" or "Business Associate Agreement" is an amendment to the Customer's Reseller Agreement or Distributor Agreement, or an executed HIPAA BAA with Google (if approved) covering the handling of Protected Health Information (as defined in HIPAA).

"Brand Features" means each party's trade names, trademarks, logos, domain names, and other distinctive brand features.

"Confidential Information" means information that one party or its Affiliate ("Disclosing Party") discloses to the other party ("Recipient") under the Agreement, and that is marked as confidential or would normally be considered confidential information under the circumstances. Customer Data is Customer's Confidential Information. Confidential Information does not include information that is independently developed by the Recipient, is shared with the Recipient by a third party without confidentiality obligations, or is or becomes public through no fault of the Recipient.

"Control" means control of greater than 50% of the voting rights or equity interests of a party.

"Covered Affiliate" has the meaning described in the Services Schedule (if applicable).

"Customer" means the party executing an Order Form with a Reseller for Google Services as described in the Agreement.

"Customer Application" has the meaning described in the Services Schedule (if applicable).

"Customer Data" has the meaning described in the Services Schedule (if applicable).

"Customer Indemnified Materials" has the meaning described in the applicable Services Schedule.

"Delegates" means the Recipient's employees, Affiliates, agents, or professional advisors.

"Distributor" means an entity authorized by Google to distribute the Services to a Reseller for resale to federal, state, or local government entities of the United States (or representatives of such entities).

"Distributor Agreement" means, if applicable, the separate agreement between Customer and Distributor regarding the Services. The Distributor Agreement is independent of and outside the scope of these Terms.

"Effective Date" means the date of the last party's signature of the General Terms (or other applicable ordering document that incorporates the General Terms).

"End User" or "Customer End User" has the meaning described in the Services Schedule (if applicable).

"Export Control Laws" means all applicable export and re-export control laws and regulations, including (a) the Export Administration Regulations ("EAR") maintained by the U.S. Department of Commerce, (b) trade and economic sanctions maintained by the U.S. Treasury Department's Office of Foreign Assets Control, and (c) the International Traffic in Arms Regulations ("ITAR") maintained by the U.S. Department of State.

"Fees" means the product of the amount of Services or Software used or ordered by Customer multiplied by the Prices, plus any applicable Taxes. Fees will be described in the Customer's Reseller Agreement or Distributor Agreement.

"Google" means Google LLC and its Affiliates, including Google Public Sector LLC.

"Google Indemnified Materials" has the meaning described in the applicable Services Schedule.

"High Risk Activities" means activities where the use or failure of the Services would reasonably be expected to result in death, serious personal injury, or severe environmental or property damage (such as the creation or operation of weaponry).

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 as it may be amended from time to time, and any regulations issued under it.

"including" means including but not limited to.

"Indemnified Liabilities" means any (a) settlement amounts approved by the indemnifying party, and (b) damages and costs finally awarded against the indemnified party by a court of competent jurisdiction.

"Intellectual Property" or "IP" means anything protectable by an Intellectual Property Right.

"Intellectual Property Right(s)" means all patent rights, copyrights, trademark rights, rights in trade secrets (if any), design rights, database rights, domain name rights, moral rights, and any other intellectual property rights (registered or unregistered) throughout the world.

"Legal Process" means an information disclosure request made under law, governmental regulation, court order, subpoena, warrant, or other valid legal authority, legal procedure, or similar process.

"Liability" means any liability, whether under contract, tort (including negligence), or otherwise, regardless of whether foreseeable or contemplated by the parties.

"Notification Email Address" has the meaning described in the applicable Services Schedule.

"Order Form" has the meaning described in the applicable Services Schedule.

"Order Term" means the period of time starting on the Services Start Date for the Services and continuing for the period indicated on the Order Form unless terminated in accordance with the Agreement.

"Prices" has the meaning described in the applicable Reseller Agreement or Distributor Agreement.

"Reseller Agreement" means the separate agreement between Customer and Reseller regarding the Services. The Reseller Agreement is independent of and outside the scope of This Agreement.

"Reseller" means, if applicable, the authorized non-Affiliate third party reseller that sells Google Services to Customer.

"Service Level Agreement" or "SLA" has the meaning described in the Services Schedule (if applicable).

"Services" has the meaning described in the applicable Services Schedule.

"Services Schedule(s)" means a schedule to the Agreement with terms that apply only to the services and software (if applicable) described in that schedule.

"Services Start Date" means either the start date described in the Order Form or, in the absence of any such date, the date Google makes the Services available to Customer.

"Software" has the meaning described in the Services Schedule (if applicable).

"Suspend" or "Suspension" means disabling or limiting access to or use of the Services or components of the Services.

"Taxes" means all government-imposed taxes, except for taxes based on Google's net income, net worth, asset value, property value, or employment.

"Third-Party Legal Proceeding" means any formal legal proceeding filed by an unaffiliated third party before a court or government tribunal (including any appellate proceeding).

"Trademark Guidelines" means Google's Brand Terms and Conditions described at https://www.google.com/permissions/trademark/brand-terms.html.

"URL" means a uniform resource locator address to a site on the internet.

"URL Terms" has the meaning described in the Services Schedule (if applicable).

"Use Restrictions" means the restrictions in Section 2.3 (Use Restrictions) of these General Terms and any additional restrictions on the use of Services described in a section entitled "Additional Use Restrictions" in the applicable Services Schedule.

Google Cloud Master Agreement
Google Cloud Platform Services Schedule

This Google Cloud Platform Services Schedule (the "Services Schedule") supplements and is incorporated by reference into the Google Cloud Master Agreement. This Services Schedule applies solely to the services and software described in this Services Schedule and is effective for the Term of the Agreement. Terms defined in the General Terms apply to this Services Schedule.

1. Using the Services.

1.1 Admin Console. Google (or Reseller or Distributor) will provide Customer an Account to access the Admin Console through which Customer may manage its use of the Services. Customer is responsible for (a) maintaining the confidentiality and security of the Account and associated passwords and (b) any use of the Account.

1.2 Ceasing Services Use. Customer may stop using the Services at any time.

1.3 Customer Applications. Customer may enable End Users to access its Customer Applications.

1.4 Additional Use Restrictions. Unless otherwise permitted in the GCP Service Specific Terms, Customer will not (a) use, and will not allow End Users to use, the Services to operate or enable any telecommunications service, or to place or receive calls from any public switched telephone network, including as part of a Customer Application; or (b) use the Services to provide a hosting, outsourced, or managed services solution to unaffiliated third parties, except as part of a Customer Application that provides value distinct from the Services.

2. Data Processing and Security.

2.1 Protection of Customer Data. Google will only access or use Customer Data to provide the Services and TSS ordered by Customer and will not use it for any other Google products, services, or advertising. Google has implemented and will maintain administrative, physical, and technical safeguards to protect Customer Data, as further described in the Data Processing Addendum.

2.2 Data Processing Addendum. The Data Processing Addendum is incorporated by reference into this Services Schedule.

3. Additional Payment Terms.

3.1 Usage and Invoicing. Customer will pay all Fees for the Services and GCP Technical Support Services. Google's measurement tools will be used to determine Customer's usage of the Services. Each invoice, which may be generated by Reseller or Distributor, will include data in sufficient detail to allow Customer to validate the Services purchased and associated Fees.

3.2 RESERVED.

3.3 RESERVED.

4. Updates to Services and Terms.

4.1 Changes to Services.

(a) Limitations on Changes. Google may update the Services, provided the updates do not result in a material reduction of the functionality, performance, availability, or security of the Services.

(b) Discontinuance. Google will notify Customer at least 12 months before discontinuing any Service

(or associated material functionality), and at least 36 months for any Key Service (or associated material functionality), in each case unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality.

(c) Support. Google will continue to provide product and security updates, and GCP Technical Support Services, until the conclusion of the applicable notice period under subsection (b) (Discontinuance).

(d) Backwards Incompatible Changes. Google will notify Customer at least 12 months before significantly modifying a Customer-facing Google API in a backwards-incompatible manner.

4.2 Changes to Terms. Google may update the URL Terms, provided the updates do not (a) result in a material reduction of the security of the Services, (b) expand the scope of or remove any restrictions on Google's processing of Customer Data as described in the Data Processing Addendum, or (c) have a material adverse impact on Customer's rights under the URL Terms. Google will notify Customer of any material updates to URL Terms.

4.3 Permitted Changes. Sections 4.1 (Changes to Services) and 4.2 (Changes to Terms) do not limit Google's ability to make changes required to comply with applicable law or address a material security risk, or that are applicable to new or pre-general availability Services, offerings, or functionality.

5. Temporary Suspension.

5.1 Services Suspension. Google may Suspend Services if (a) necessary to comply with law or protect the Services or Google's infrastructure supporting the Services or (b) Customer or any End User's use of the Services does not comply with the AUP, and it is not cured following notice from Google.

5.2 Limitations on Services Suspensions. If Google Suspends Services under Section 5.1 (Services Suspension), then (a) Google will provide Customer notice of the cause for Suspension without undue delay, to the extent legally permitted, and (b) the Suspension will be to the minimum extent and for the shortest duration required to resolve the cause for Suspension.

6. Technical Support. Google will provide GCP Technical Support Services to Customer during the Order Term in accordance with the GCP Technical Support Services Guidelines. Customer is responsible for the technical support of its Customer Applications and Projects.

7. Copyright. Google provides information to help copyright holders manage their intellectual property online, but Google cannot determine whether something is being used legally without input from the copyright holders. Google will respond to notices of alleged copyright infringement and may terminate repeat infringers in appropriate circumstances as required to maintain safe harbor for online service providers under the U.S. Digital Millennium Copyright Act. If Customer believes a person or entity is infringing Customer's or its End User's copyrights and would like to notify Google, Customer can find information about submitting notices, and Google's policy about responding to notices, at http://www.google.com/dmca.html.

8. Software.

8.1 Provision of Software. Google may make Software available to Customer, including third-party software. Customer's use of any Software is subject to the applicable provisions in the GCP Service Specific Terms.

8.2 Ceasing Software Use. If the Agreement or the Google Cloud Platform Order Form terminates or expires, then Customer will stop using the Software.

9. Survival. The following Sections of this Services Schedule will survive expiration or termination of this Services Schedule: Section 11 (Additional Definitions).

10. **Termination of Previous Agreements.** If Google and Customer have previously entered into a Google Cloud Platform License Agreement, then that agreement will terminate on the Services Start Date, and the Agreement will govern the provision and use of the Services going forward.

11. **Additional Definitions.**

"Account" means Customer's Google Cloud Platform account.

"Admin Console" means the online console(s) or dashboard provided by Google to Customer for administering the Services.

"AUP" means the then-current acceptable use policy for the Services described at https://cloud.google.com/terms/aup.

"Covered Affiliate" means an Affiliate using the Services under Customer's Account.

"Customer Application" means a software program that Customer creates or hosts using the Services.

"Customer Data" means data provided to Google by Customer or End Users through the Services under the Account, and data that Customer or End Users derive from that data through their use of the Services.

"Customer Indemnified Materials" means Customer Data, Customer Brand Features, Customer Applications, and Projects.

"Data Processing Addendum" means the then-current terms describing data processing and security obligations with respect to Customer Data, as described at https://cloud.google.com/terms/data-processing-terms.

"End User" or "Customer End User" means an individual that Customer permits to use the Services or a Customer Application. For clarity, End Users may include employees of Customer Affiliates and other authorized third parties.

"GCP Service Specific Terms" means the then-current terms specific to one or more Services or Software described at https://cloud.google.com/cloud/terms/service-terms.

"GCP Technical Support Services" or "TSS" means the then-current technical support service provided by Google to Customer under the GCP Technical Support Services Guidelines.

"GCP Technical Support Services Guidelines" or "TSS Guidelines" means the then-current Google Cloud Platform support service guidelines described at https://cloud.google.com/terms/tssg/.

"Google API" means any application programming interface provided by Google as part of the Services.

"Google Indemnified Materials" means the Services and Google's Brand Features.

"Key Services" means the then-current list of Services described at https://cloud.google.com/terms/key-services. Google may not remove a Service from this URL unless that Service is discontinued in accordance with Section 4.1(b) (Discontinuance).

"Notification Email Address" means the email address(es) designated by Customer in the Admin Console.

"Order Form" means an order form issued by Google, Reseller or Distributor and executed by Customer and issuer specifying the Services Google will provide to Customer under this Services Schedule.

"Prices" means the applicable prices described in the applicable Reseller Agreement or Distributor Agreement.

"Project" means a collection of Google Cloud Platform resources configured by Customer via the Services.

"Services" means the then-current services described at https://cloud.google.com/terms/services, excluding any Third-Party Offerings.

"SLA" means the then-current service level agreements described at https://cloud.google.com/terms/sla/.

"Software" means any downloadable tools, software development kits, or other such computer software provided by Google for use in connection with the Services, and any updates Google may make to such Software from time to time, excluding any Third-Party Offerings.

"Third-Party Offerings" means (a) third-party services, software, products, and other offerings that are not incorporated into the Services or Software and (b) offerings identified in the "Third-Party Terms" section of the Service Specific Terms.

"URL Terms" means the AUP, Data Processing Addendum, GCP Service Specific Terms, GCP Technical Support Services Guidelines, and SLAs.

Google Cloud Master Agreement
Google Workspace Services Schedule

This Google Workspace Services Schedule (the "Services Schedule") supplements and is incorporated by reference into the Google Cloud Master Agreement. This Services Schedule applies solely to the services described in this Services Schedule and is effective for the Term of the Agreement. Terms defined in the General Terms apply to this Services Schedule.

1. Using the Services.

1.1 Admin Console. Google will provide Customer access to the Admin Console through which Customer may manage its use of the Services. Customer may specify one or more Administrators through the Admin Console who will have the right to access Admin Accounts. Customer is responsible for (a) maintaining the confidentiality and security of the End User Accounts and associated passwords and (b) any use of the End User Accounts. Customer agrees that Google's responsibilities do not extend to the internal management or administration of the Services for Customer.

1.2 Additional Use Restrictions. Unless otherwise permitted in the Google Workspace Service Specific Terms, Customer will not use, and will not allow End Users to use, the Services to place or receive emergency services calls.

1.3 Adding End User Accounts During Order Term. Customer may purchase additional End User Accounts during an Order Term by means of an additional Order Form or Reseller Order or by ordering via the Admin Console. Such additional End User Accounts will have a pro-rated term ending on the last day of the applicable Order Term.

2. Data Processing and Security.

2.1 Data Processing Addendum. The Data Processing Addendum is incorporated by reference into this Services Schedule.

3. Additional Payment Terms.

3.1 Usage and Invoicing. Customer will pay all Fees for the Services and such payment will be made pursuant to the Reseller Agreement or Distributor Agreement. Google's measurement tools will be used to determine Customer's usage of the Services. Unless otherwise provided in the Agreement or required by law, Fees for Services are nonrefundable.

3.2 RESERVED.

4. Updates to Services and Terms.

4.1 Changes to Services.

(a) Limitations on Changes. Google may update the Services, provided the updates do not result in a material reduction of the performance or security of the Services.

(b) Discontinuance. Google will notify Customer at least 12 months before discontinuing any Core Service (or associated material functionality), and at least 36 months for any Key Service (or associated material functionality), in each case unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality.

(c) Support. Google will continue to provide product and security updates, and Technical Support Services, until the conclusion of the applicable notice period under subsection (b) (Discontinuance).

4.2 Changes to Terms. Google may update the URL Terms, provided the updates do not (a) result in a material reduction of the security of the Services, (b) expand the scope of or remove any restrictions on Google's processing of Customer Data as described in the Data Processing Addendum, or (c) have a material adverse impact on Customer's rights under the URL Terms. Google will notify Customer of any material updates to URL Terms.

4.3 Permitted Changes. Sections 4.1 (Changes to Services) and 4.2 (Changes to Terms) do not limit Google's ability to make changes required to comply with applicable law or address a material security risk, or that are applicable to new or pre-general availability Services, offerings, or functionality.

5. Temporary Suspension.

5.1 Services Suspension. Google may Suspend Services if (a) necessary to comply with law or protect the Services or Google's infrastructure supporting the Services or (b) Customer or any End User's use of the Services does not comply with the AUP, and it is not cured following notice from Google. For Suspensions of End User Accounts, Google will provide Customer's Administrator the ability to restore End User Accounts in certain circumstances.

5.2 Limitations on Services Suspensions. If Google Suspends Services, then (a) Google will provide Customer notice of the cause for Suspension without undue delay, to the extent legally permitted, and (b) the Suspension will be to the minimum extent and for the shortest duration required to resolve the cause for Suspension.

6. Technical Support. Google will provide Google Workspace Technical Support Services to Customer during the Order Term in accordance with the Google Workspace Technical Support Services Guidelines.

7. Additional Customer Responsibilities.

7.1 Customer Domain Name Ownership. Customer is responsible for obtaining and maintaining any rights necessary for Customer's and Google's use of the Customer Domain Names under the Agreement. Before providing the Services, Google may require that Customer verify that Customer owns or controls the Customer Domain Names. If Customer does not own or control the Customer Domain Names, then Google will have no obligation to provide the Services to Customer.

7.2 Abuse Monitoring. Customer is solely responsible for monitoring, responding to, and otherwise processing emails sent to the "abuse" and "postmaster" aliases for Customer Domain Names, but Google may monitor emails sent to these aliases to allow Google to identify Services abuse.

8. Using Brand Features Within the Services. Google will display only those Customer Brand Features that Customer authorizes Google to display by uploading them into the Services. Google will display those Customer Brand Features within designated areas of the web pages displaying the Services to End Users. Customer may specify the nature of this use in the Admin Console. Google may also display Google Brand Features on such web pages to indicate that the Services are provided by Google.

9. Additional Products. Google makes optional Additional Products available to Customer and its End Users. Customer's use of Additional Products is subject to the Additional Product Terms.

10. RESERVED.

11. Termination of Previous Agreements. If Google and Customer have previously entered into another agreement under which Customer uses the Services, then that agreement will terminate on the

Services Start Date, and the Agreement will govern the provision and use of the Services going forward.

12. Additional Definitions.

"Additional Products" means products, services, and applications that are not part of the Services but may be accessible for use in conjunction with the Services.

"Additional Product Terms" means the then-current terms at https://workspace.google.com/intl/en/terms/additional_services.html.

"Admin Account" means a type of End User Account that Customer (or Reseller, if applicable) may use to administer the Services.

"Admin Console" means the online console(s) or dashboard provided by Google to Customer for administering (a) the Services and (b) the services set out in a Complementary Product Services Summary (if applicable).

"Administrator" means Customer-designated personnel who administer the Services to End Users on Customer's behalf, and have the ability to access Customer End User Accounts. Such access includes the ability to access, monitor, use, modify, withhold, or disclose any data available to End Users associated with their End User Accounts.

"AUP" means the then-current acceptable use policy for the Services described at https://workspace.google.com/terms/use_policy.html.

"Complementary Product Services Summary" has the meaning given in the Data Processing Addendum.

"Core Services" means the then-current "Core Services" as described in the Services Summary at https://workspace.google.com/terms/user_features.html, excluding any Third-Party Offerings.

"Covered Affiliate" means an Affiliate using the Services under Customer's Account.

"Customer Data" means data submitted, stored, sent, or received via the Services by Customer or its End Users.

"Customer Domain Name" means a domain name specified in the Order Form or Reseller Order to be used in connection with the Services.

"Customer Indemnified Materials" means Customer Data and Customer Brand Features.

"Data Processing Addendum" means the then-current terms describing data protection and processing obligations with respect to Customer Data, as described at https://gsuite.google.com/terms/dpa_terms.html.

"End User" or "Customer End User" means an individual that Customer permits to use the Services. For clarity, End Users may include employees of Customer Affiliates and other authorized third parties.

"End User Account" means a Google-hosted account established by Customer through the Services for an End User to use the Services.

"GDPR" has the meaning given to it in the Data Processing Addendum.

"Google Indemnified Materials" means the Services and Google's Brand Features.

"Google Workspace Service Specific Terms" means the then-current terms specific to one or more Services

described at https://workspace.google.com/terms/service-terms/.

"Google Workspace Technical Support Services" or "TSS" means the technical support service provided by Google to Customer under the Google Workspace Technical Support Services Guidelines.

"Google Workspace Technical Support Services Guidelines" or "TSS Guidelines" means the then-current Google Workspace support service guidelines described at https://workspace.google.com/terms/tssg.html.

"Key Services" means Gmail, Google Calendar, Google Docs, Google Sheets, Google Slides, Google Drive, Google Chat, Google Meet, and Google Forms.

"Notification Email Address" means the email address(es) designated by Customer in the Admin Console.

"Order Form" means an order form issued by Google, Reseller or Distributor and executed by Customer and issuer specifying the Services Google will provide to Customer under this Services Schedule.

"Other Services" means the then-current "Other Services" as described in the Services Summary at https://gsuite.google.com/terms/user_features.html, excluding any Third-Party Offerings.

"Personal Data" has the meaning given to it in the Data Processing Addendum.

"Prices" means the applicable prices described in the applicable Reseller Agreement or Distributor Agreement.

"Reseller Fees" means the fees (if any) for Services used or ordered by Customer as agreed in a Reseller Agreement, plus any applicable Taxes.

"Reseller Order" means, if applicable, an order form issued by a Reseller and executed by Customer and the Reseller specifying the Services Customer is ordering from the Reseller.

"Services" means the then-current Core Services and Other Services described at https://workspace.google.com/terms/user_features.html.

"SLA" means the then-current service level agreement described at https://gsuite.google.com/terms/sla.html.

"Third-Party Offerings" means third-party services, software, products, and other offerings that are not incorporated into the Services.

"URL Terms" means the AUP, Data Processing Addendum, Google Workspace Service Specific Terms, Google Workspace Technical Support Services Guidelines, and SLAs.

Google Cloud Master Agreement
Implementation Services Schedule

This Implementation Services Schedule (the "Services Schedule") supplements and is incorporated by reference into the Google Cloud Master Agreement. This Services Schedule applies to implementation and advisory services described in this Services Schedule that are designed to help Customer use Google products and services. Terms defined in the General Terms apply to this Services Schedule.

1. Services.

1.1 Provision of Services. Google will provide Services, including Deliverables, to Customer, subject to Customer fulfilling its obligations under Section 2.1 (Cooperation).

1.2 Training Services. Customer may order Training Services for use in connection with the Services. Training Services are subject to the Training Terms.

1.3 Invoices and Payment. Customer will pay all Fees for Services ordered under this Services Schedule. Fees for some Services may be non-cancellable, as specified in the Order Form.

1.4 Personnel. Google will determine which Personnel will perform the Services. If Customer requests a change of Personnel and provides a reasonable and lawful basis for such request, then Google will use commercially reasonable efforts to replace the assigned Personnel with alternative Personnel.

1.5 Compliance with Customer's Onsite Policies and Procedures. Google Personnel performing Services at Customer's facilities will comply with Customer's reasonable onsite policies and procedures made known to Google in writing in advance.

2. Customer Obligations.

2.1 Cooperation. Customer will provide reasonable and timely cooperation in connection with Google's provision of the Services. Google will not be liable for a delay caused by Customer's failure to provide Google with the information, materials, consents, or access to Customer facilities, networks, or systems required for Google to perform the Services. If Reseller, Distributor or Google informs Customer of such failure and Customer does not cure the failure within 30 days, then (a) Reseller, Distributor or Google may terminate any incomplete Services and (b) in addition to Fees in Section 6(b) (Effect on Payment), Customer will pay actual costs incurred by Reseller, Distributor or Google for the cancelled Services.

2.2 No Personal Data. Customer acknowledges that Google does not need to process Personal Data to perform the Services. Customer will not provide Google with access to Personal Data unless the parties have agreed in a separate agreement on the scope of work and any terms applicable to Google's processing of such Personal Data.

1.1 Customer will reimburse expenses (a) specifically described in the applicable Reseller Order Form; or (b) up to the amounts specified as "expenses" in the applicable Reseller Order Form that are actual, reasonable, and necessary.

2. Intellectual Property.

2.1 Background IP. Customer owns all rights, title, and interest in Customer's Background IP. Google owns all rights, title, and interest in Google's Background IP. Customer grants Google a license to use Customer's Background IP to perform the Services (with a right to sublicense to Google Affiliates and subcontractors). Except for the license rights under Sections 3.2 (Google Technology) and 3.3 (Deliverables), neither party will acquire any right, title, or interest in the other party's Background IP under this Services Schedule.

2.2 Google Technology. Google owns all rights, title, and interest in Google Technology. To the extent Google Technology is incorporated into Deliverables, Google grants Customer a limited, worldwide, non-exclusive, perpetual, non-transferable license (with the right to sublicense to Affiliates) to use the Google Technology in connection with the Deliverables for Customer's internal business purposes. This Services Schedule does not grant Customer any right to use materials, products, or services that are made available to Google customers under a separate agreement, license, or Services Schedule.

2.3 Deliverables. Google grants Customer a limited, worldwide, non-exclusive, perpetual, fully-paid, non-transferable license (with the right to sublicense to Affiliates) to use, reproduce, and modify the Deliverables for Customer's internal business purposes.

3. Warranties and Remedies.

3.1 Google Warranty. Google will perform the Services in a professional and workmanlike manner, in accordance with practices used by other service providers performing services similar to the Services. Google will use Personnel with requisite skills, experience, and qualifications to perform the Services.

3.2 Remedies. Google's entire liability and Customer's sole remedy for Google's failure to provide Services that conform with Section 4.1 (Google Warranty) will be for Google to, at its option, (a) use commercially reasonable efforts to re-perform the Services or (b) terminate the Order Form and refund any applicable Fees received for the nonconforming Services. Any claim that Google has breached the warranty as described in Section 4.1 (Google Warranty) must be made within 30 days after Google has performed the Services.

4. Indemnification.

4.1 Indemnification Exclusions. General Terms Sections 9.1 (Google Indemnification Obligations) and 9.2 (Customer Indemnification Obligations) will not apply to the extent the underlying allegation arises from (a) modifications to the Google Indemnified Materials or Customer Indemnified Materials (as applicable) by anyone other than the indemnifying party or (b) compliance with the indemnified party's instructions, design, or request for customized features.

4.2 Infringement Remedies. The remedies described in General Terms Section 9.5 (Remedies) also apply to Deliverables.

5. Effects of Termination. If this Services Schedule or an Order Form under this Services Schedule expires or terminates, then:

(a) Effect on Services. The rights under the Agreement granted by one party to the other regarding the Services will cease immediately except as described in this Section 6 (Effects of Termination), and Google will stop work on the Services.

(b) Effect on Payment. Customer will pay for (i) Services, including work-in-progress, performed before the effective date of termination or expiration and (ii) any remaining non-cancellable Fees. Google, Reseller, or Distributor will send Customer a final invoice for payment obligations under the Order Form.

(c) Survival. The following Sections of this Schedule will survive expiration or termination of this Services Schedule: 3 (Intellectual Property), 5 (Indemnification), 6 (Effects of Termination), and 9 (Additional Definitions).

6. RESERVED.

7. Termination of Previous Agreements. If Reseller, Distributor or Google and Customer have

previously entered into an agreement for Google to perform similar implementation services (including a Professional Services Agreement), then that agreement will terminate on the date of the last party's signature effectuating this Services Schedule, and the Agreement will govern the provision and use of the Services going forward.

8. Additional Definitions.

"Background IP" means all Intellectual Property Rights owned or licensed by a party (a) before the effective date of the applicable Order Form or (b) independent of the Services.

"Covered Affiliate" means an Affiliate receiving the Services under this Services Schedule.

"Customer Indemnified Materials" means (a) Customer Background IP and any other information, materials, or technology provided to Google by Customer in connection with the Services (in each case, excluding any open source software) and (b) Customer's Brand Features. Customer Indemnified Materials do not include Google Technology or Deliverables.

"Deliverables" means work product created for Customer by Google Personnel as part of the Services and specified as Deliverables in an Order Form.

"Google Indemnified Materials" means (a) Deliverables and Google Technology (in each case, excluding any open source software) or (b) Google's Brand Features. Google Indemnified Materials do not include Customer Background IP.

"Google Technology" means (a) Google Background IP; (b) all Intellectual Property and know-how applicable to Google products and services; and (c) tools, code, algorithms, modules, materials, documentation, reports, and technology developed in connection with the Services that have general application to Google's other customers, including derivatives of and improvements to Google's Background IP. Google Technology does not include Customer Background IP or Customer Confidential Information.

"Notification Email Address" means the email address(es) designated by Customer in the applicable Order Form.

"Order Form" means an order form, statement of work, or other document issued by Reseller, Distributor, or Google under the Agreement, including data sheets associated with Services described in the order form, and executed by Customer and Reseller or Distributor, specifying the Services Google will provide to Customer.

"Personal Data" means personal data that: (a) has the meaning given to it in: (i) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("EU GDPR"); or (ii) the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force ("UK GDPR"), as applicable; and (b) would cause Google to be subject to the EU GDPR or the UK GDPR (as applicable) as a data processor for Customer.

"Personnel" means a party's and its Affiliates' respective directors, officers, employees, agents, and subcontractors.

"Prices" means the applicable prices described in the applicable Reseller Agreement or Distributor Agreement.

"Services" means the then-current advisory and implementation services described at https://g.co/cloudpsoterms and an applicable Order Form and similar advisory or implementation services designed to help Customer use Google products and services. Services do not include Training Services.

"Training Services" means education and certification services related to Google products and services for individual users, as more fully described in an applicable Order Form. Training Services do not include

Deliverables.

"Training Terms" means the then-current terms applicable to Training Services described at https://enterprise.google.com/terms/training-services.htm

Google Cloud Master Agreement - U.S. Public Sector Partner
Looker Services Schedule

This Looker Services Schedule (the "Services Schedule") supplements and is incorporated by reference into the Google Cloud Master Agreement between the same parties to this Services Schedule. This Services Schedule applies solely to the services and software described in this Services Schedule and is effective for the Term of the Agreement. Terms defined in the General Terms apply to this Services Schedule.

1. **Using the Services.**

1.1. Use by Customer. Google (or Reseller or Distributor) will provide the Services to Customer by (a) providing access to an Instance for the Looker Hosted Deployment or (b) providing a license key for the Customer Hosted Deployment. Customer may only use the Services with databases and servers licensed and/or owned by Customer. Customer may configure the Services for Internal Business Purposes and External Business Purposes only to the extent authorized in the Order Form.

1.2. Use by Affiliates. Customer Affiliates may (i) access and use the Services as End Users, subject to the terms of Customer's Order Form so long as Customer remains responsible for the Affiliates' compliance with the Agreement and the applicable Order Form, or (ii) execute a separate Order Form that incorporates this Services Schedule by reference.

1.3. External Business Purposes. If the Order Form includes PBL and the PBL Client is bound to a written agreement with Customer that is at least as protective of Google as the rights and obligations contained in this Agreement, then Customer may make the Services available for use by PBL Users, including by embedding the Services into a Customer Application. Customer may not accept, and acknowledges that Google will not be bound by, any terms or conditions with the PBL Client that modify add to or change in any way the Agreement or Order Form.

1.4. Customer Responsibilities. Customer will be solely responsible, and Google disclaims responsibility for any acquisition, implementation, support or maintenance of third-party products or services purchased by Customer that may interoperate with the Services.

1.5. Additional Use Restrictions. Customer will not, and will not allow End Users to: (a) remove any copyright notices, trademarks or other proprietary notices or restrictions from the Services; (b) provide the Services on a time sharing, hosting, service provider or other similar basis, except as part of a Customer Application for External Business Purposes; (c) provide or obtain unauthorized access to the Services, including by sharing the log-on credentials for any End User with others; (d) circumvent any technical measures in the Software or Services; (e) conduct benchmarking tests or other comparative analysis of the Services for publication or disclosure to third parties or (f) disrupt the security, integrity or performance of the Services in any way.

1.6. Beta Features. Google may make Beta Features available to End Users subject to the provisions in the Looker Service Specific Terms.

2. **Data Processing and Security.** To the extent Customer provides Google with access to Customer Data under this Services Schedule, the following will apply:

2.1. Protection of Customer Data. Google will only access or use Customer Data to provide the Services and TSS ordered by Customer to Customer and will not use it for any other Google products, services, or advertising. Google has implemented and will maintain administrative, physical, and technical safeguards designed to protect the confidentiality, security, integrity, availability, and privacy of Customer Data stored in the Instance, as further described in the Data Processing Addendum. Notwithstanding any other provision of the Agreement, this Services Schedule or any other agreement related to the Services, Google will not be responsible for any breach or loss to the extent resulting from Customer's security configuration or Customer's administration of the Services.

2.2. Data Processing Addendums. The Data Processing Addendum is incorporated by reference into this Services Schedule.

3. Additional Payment Terms.

3.1. Usage and Invoicing. Customer will pay all Fees for the Services and TSS. Unless otherwise provided in the Agreement, the applicable Order Form or required by law, Fees for Services are non-refundable. Google's measurement tools will be used to determine Customer's usage of the Services. Each invoice, which shall be generated by Reseller or Distributor, will include data in sufficient detail to allow Customer to validate the Services purchased and associated Fees. If Customer exceeds the number of End Users, Scope of Use, or Deployment Attributes, Customer or the applicable Reseller or Distributor will, upon becoming aware, promptly notify the other party and the parties agree to discuss in good faith the additional Fees due by Customer for such over-deployment. The agreed upon additional Fees associated with the over-deployment will be memorialized in a new Order Form.

3.2. Additional Usage. Customer may purchase additional Deployment Attributes (including adding End Users) during an Order Term by executing an additional Order Form. Such purchase will have a pro-rated term ending on the last day of the applicable Order Term. Deployment Attributes cannot be decreased during the Order Term.

3.3. [RESERVED]

3.4. Services Use Review. Within 30 days of Google's reasonable written request, Customer will provide a sufficiently detailed written usage report listing the Deployment Attributes being used for each Scope of Use, the number and type of End Users using the Services during the requested period, and the Instance(s) deployed, along with the related license key(s). To the extent the usage reports can be measured by a ping from Google's license server, the ping will serve as the report. If there is a PBL deployment, Customer will provide a complete list of the software and applications where the Software and Services are deployed. If requested, Customer will provide reasonable assistance and access to information to verify the accuracy of any information provided to Google, which verification may include access to records relating to Customer's use of the Services. If the review indicates an underpayment, Customer agrees to negotiate in good faith a new or replacement Order Form that will cover the additional usage.

4. Updates to Services and Terms.

4.1. Changes to Services.

(a) Limitations on Changes. Google may update the Services, provided the updates do not result in a material reduction of the functionality, performance, availability, or security of the Services.

(b) Discontinuance. Google will notify Customer at least 12 months before discontinuing any Service (or associated material functionality), unless Google replaces such discontinued Service or functionality with a materially similar Service or functionality.

(c) Support. Google will continue to provide product and security updates, and TSS, until the conclusion of the applicable notice period under subsection (b) (Discontinuance).

4.2. Changes to Terms. Google may update the URL Terms, provided the updates do not (a) result in a material reduction of the security of the Services, (b) expand the scope of or remove any restrictions on Google's processing of Customer Data as described in the Data Processing Addendum(if applicable), or (c) have a material adverse impact on Customer's rights under the URL Terms. Google will notify Customer of any material updates to URL Terms.

4.3. Permitted Changes. Sections 4.1 (Changes to Services) and 4.2 (Changes to Terms) do not limit Google's ability to make changes required to comply with applicable law or address a material security risk, or that are applicable to Beta Features or new or pre-general availability Services, offerings, or functionality.

5. **Temporary Suspension.**

5.1. Services Suspension. Google may Suspend Services if (a) necessary to comply with law or protect the Services or Google's infrastructure supporting the Services or (b) Customer or any End User's use of the Services does not comply with the AUP, and it is not cured following notice from Google.

5.2. Limitations on Services Suspensions. If Google Suspends Services under Section 5.1 (Services Suspension), then (a) Google will provide Customer notice of the cause for Suspension without undue delay, to the extent legally permitted, and (b) the Suspension will be to the minimum extent and for the shortest duration required to resolve the cause for Suspension.

6. **Technical Support.** Unless otherwise agreed in an Order Form, Google will provide Looker Technical Support Services to Customer during the Order Term in accordance with the Looker Technical Support Services Guidelines. Customer is responsible for the technical support of its Customer Applications, including PBL Users using the Services for External Business Purposes.

7. **Provision of Software.** Google may make Software available to Customer in connection with Customer's use of the Services, including third-party software. Some Software may be subject to third-party license terms, which can be found at: https://looker.com/terms/notices-and-acknowledgements.

8. **Ceasing Software Use.** If the Agreement, this Services Schedule or the Order Form for the Services terminates or expires, then Customer will stop using the Software.

9. [RESERVED]

10. **Professional Services**. If Customer purchases PSO Services, such PSO Services will be provided in accordance with a separate agreement and not under this Services Schedule.

11. **Survival.** The following section of this Services Schedule will survive expiration or termination of this Services Schedule: 3 (Additional Payment Terms) and Section 13 (Additional Definitions).

12. **Termination of Previous Agreements.** If Customer has previously entered into an agreement for the Software or Services, then that agreement will terminate on the Services Start Date, and this Agreement, including the Order Form referencing this Services Schedule, will govern the provision and use of the Services going forward.

13. **Additional Definitions.**

"AUP" means the then-current acceptable use policy for the Services described at https://cloud.google.com/terms/aup

"Beta Features" has the meaning set forth in the Looker Service Specific Terms.

"Covered Affiliate" means Customer's Affiliate using the Services (i) via an Order Form that is subject to the terms of this Services Schedule, and (ii) in compliance with the Agreement and the applicable Order Form.

"Customer Application" means a software program that Customer creates or hosts and that uses the Services. A Customer Application may be a website.

"Customer Data" means (a) all data in Customer's databases provided to Google by Customer or End Users via the Services and (b) all results provided to Customer or End Users for queries executed against such data via the Services.

"Customer Hosted Deployment" means the Software installed by or for Customer at Customer's premises or on a Customer-controlled server within a data center selected and managed by Customer. A Customer Hosted Deployment includes the In-Product Services.

"Customer Indemnified Materials" means Customer Data and Customer Brand Features.

"Data Processing Addendum" or "DPA" means the then-current terms describing data processing and security obligations with respect to Customer Data described at https://looker.com/trust-center/legal/customers/dpst.

"Deployment Attributes" means the quantified usage of the Services as specified on an Order Form, which include, but are not limited to the number of Instances, End Users, API calls or other licensing attributes defined by the Scope of Use.

"Documentation" means the user guides and manuals for the Services provided by Google for all Customer's own internal use.

"End User" or "Customer End User" means an individual that Customer permits to use the Services. End Users may include employees of Customer's Affiliates or PBL Users.

"External Business Purposes", "PBL" or "Powered by Looker" means use of the Services by or for the benefit of Customer's customers or clients, and their users or other third parties.

"Google Indemnified Materials" means the Services, Software and Google's Brand Features.

"In-Product Services" means the services hosted and made accessible by Google through the Software, specifically licensing data, configuration backups, system error reports, data actions and support tickets.

"Instance" means one single configuration of the Software's administrative settings and application database, subject to the platform restrictions detailed in the Order Form. Each Instance requires a unique license key to operate. Multiple identically configured Instances running with separate configurations are considered separate instances.

"Internal Business Purposes" means use of the Services by or for the benefit of Customer's internal operations.

"Looker Hosted Deployment" means the Software installed by Google on a web connected platform that is run in a hosting facility designated by Google, unless otherwise agreed by the parties in an Order Form. A Looker Hosted Deployment includes the In-Product Services.

"Looker Service Specific Terms" means the then-current terms specific to the Services stated at https://looker.com/trust-center/legal/customers/service-terms

"Looker Technical Support Services" or "TSS" means the then-current technical support service provided by Google to Customer under the Looker Technical Support Services Guidelines.

"Looker Technical Support Services Guidelines" or "TSS Guidelines" means the then-current technical support service provided by Google to Customer described at https://looker.com/trust-center/legal/customers/support-lss.

"Notification Email Address" means the email address(es) designated by Customer in the Order Form.

"Order Form" means an order form issued by Google, Reseller or Distributor and executed by Customer and issuer specifying the Services Google will provide under this Services Schedule.

"PBL Client" means (i) the PBL User or (ii) Customer's client that authorizes use of the Services by PBL Users.

"PBL User" is an individual authorized to use the Services for External Business Purposes as an End User subject to the terms of the applicable Order Form.

"Prices" means the prices agreed to by Customer and Reseller or Distributor in the applicable Reseller Agreement or Distributor Agreement.

"PSO Services" means advisory and consulting services purchased by Customer from Reseller or Distributor.

"Scope of Use" means Customer's specific use case for the Services as defined in an Order Form, which may include limitations on Customer's use for Internal Business Purposes and/or External Business Purposes.

"Services" means integrated platform, including cloud-based infrastructure (if applicable), and software components (including any associated APIs) that enables businesses to analyze data and define business metrics across multiple data sources. Services exclude Third Party Offerings.

"SLA" means the then-current service level agreements applicable to the Looker Hosted Deployment only, described at https://looker.com/trust-center/legal/sla-lss.

"Software" means any downloadable tools, including the licensed data platform provided under the Services Schedule, and any other computer software provided by Google for use in connection with the Services, and any copies, modifications, derivative works or enhancements thereto, excluding any Third-Party Offerings.

"Third-Party Offerings" means (a) third-party services, software, products, and other offerings that are not incorporated into the Services or Software and (b) offerings identified in the "Third-Party Offerings" section of the Looker Service Specific Terms.

"URL Terms" means the AUP, Data Processing Addendum, Looker Technical Support Services Guidelines, and the SLAs.

HIPAA Business Associate Addendum

This HIPAA Business Associate Addendum ("BAA") is entered into between Google LLC ("Google") and West Virginia Office of Technology, with offices at Capitol Complex - Building 5, 10th Floor, 1900 Kanawha Blvd E, Charleston, WV 25305 ("Partner"), and supplements, amends and is incorporated into the Partner Agreement between Google and Partner. Capitalized terms used but not defined in this BAA have the meaning given to them in the Partner Agreement. This BAA will be effective as of the last signature date below (the "BAA Effective Date").

This BAA (a) only applies to Covered Services provided under the Google Cloud Platform Product Schedule of the Partner Agreement, (b) is valid and effective so long as there is a valid and effective Google Cloud Platform Product Schedule governing such Covered Services, and (c) together with the Partner Agreement, governs each party's respective obligations regarding Protected Health Information.

1. Definitions.

"Business Associate" has the definition given to it under HIPAA.

"Breach" has the definition given to it under HIPAA.

"Covered Entity" has the definition given to it under HIPAA.

"Covered Services" means the Google products and/or services specifically listed in the URLs on Attachment 1, as may be updated from time to time by Google with notice to Partner. Google may only remove a Covered Service from those URLs with at least 12 months prior notice.

"Designated Record Set" has the definition given to it under HIPAA.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the rules and the regulations thereunder, as amended.

"HIPAA Implementation Guide" means the informational guide that Google makes available at the URL in Attachment 2, or a successor URL, describing how the Covered Services may be configured by Customer in connection with Customer's HIPAA compliance efforts. For the purposes of this BAA, all references in the HIPAA Implementation Guide to "Customer" mean Partner.

"HITECH Act" means the Health Information Technology for Economic and Clinical Health Act enacted in the United States Congress, which is Title XIII of the American Recovery & Reinvestment Act, and the regulations thereunder, as amended.

"Notification Email Address(es)" means the email address(es) designated by Partner in the Admin Console or Order Form, to receive certain notifications from Google. Partner is responsible for using the Admin Console to ensure that its Notification Email Address remains current and valid.

"Protected Health Information" or "PHI" has the definition given to it under HIPAA and for purposes of this BAA is limited to PHI within Partner Data to which Google has access through the Covered Services in connection with Partner's or Partner End Users' permitted use of Covered Services.

"Partner Agreement" means the mutually agreed upon written agreement(s) between Google and Partner that authorizes Partner to resell the Covered Services under the Program.

"Required by Law" has the definition given to it under HIPAA.

"Security Incident" has the definition given to it under HIPAA.

"Subcontractor" means a person to whom a Business Associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such Business Associate.

2. **Applicability**. This BAA applies to the extent Partner is acting as a Covered Entity or a Business Associate to create, receive, maintain, or transmit PHI via a Covered Service and to the extent Google, as a result, is deemed under HIPAA to be acting as a Business Associate or Subcontractor of Partner. Partner acknowledges that this BAA does not apply to (a) any other Google product, service, or feature that is not a Covered Service; or (b) any PHI that Partner End Users create, receive, maintain, or transmit outside of the Covered Services (including Partner End User's use of its offline or on-premise storage tools or third-party applications).

3. **Permitted Use and Disclosure of PHI**.

   (a) Except as otherwise stated in this BAA, Google may use and disclose PHI only (i) as permitted or required by the Partner Agreement and/or this BAA or (ii) as required by law.

   (b) Google may use and disclose PHI for its proper management and administration and to carry out its legal responsibilities, provided that any disclosure of PHI for such purposes may only occur if (i) required by law; or (ii) Google obtains written reasonable assurances from the person to whom PHI will be disclosed that it will be held in confidence, used only for the purpose for which it was disclosed, and that Google will be notified of any Breach or Security Incident.

   (c) In conducting activities under the Partner Agreement that involve the use and/or disclosure of PHI of Customer, Google shall limit the use and/or disclosure of such PHI to the minimum amount of information necessary to accomplish the intended purpose of the use or disclosure.

4. **Partner Obligations**.

   (a) Partner and Partner End Users will not request that Google or the Covered Services use or disclose PHI in any manner that would not be permissible under HIPAA if done by Partner (if Partner is a Covered Entity) or by the Covered Entity to which Partner is a Business Associate (unless expressly permitted under HIPAA for a Business Associate).

   (b) For Partner End Users that use the Covered Services in connection with PHI, Partner will use controls available within the Services, including those detailed in the HIPAA Implementation Guide, to ensure its and its Partner End Users' use of PHI is limited to the Covered Services. Partner acknowledges and agrees that the HIPAA Implementation Guide is provided by Google solely as an informational guide with respect to Partner's configuration options, and that Partner is solely responsible for ensuring that its and Partner End Users' use of the Covered Services complies with HIPAA and HITECH.

5. **Appropriate Safeguards.** Google and Partner will each use, and Partner will ensure its Customers and Partner End Users are obligated to use appropriate safeguards designed to prevent against unauthorized use or disclosure of PHI, and as otherwise required under HIPAA, with respect to the Covered Services. These include:

(a) Limitation of the groups of its workforce and agents, to whom the PHI is disclosed to those reasonably required to accomplish the purposes stated in this Addendum, and the use and disclosure of the minimum PHI necessary to accomplish such use or disclosure

(b) Maintenance of a written PHI privacy and security program that includes administrative, technical and physical safeguards reasonably appropriate ot the size, nature, scope and complexity of Google's operations, in compliance with the Security Rule.

(c) Associate agrees that the mitigation measures described in 6(a) will mitigate, to the extent practicable, the harmful effects known to Associate of a use or disclosure of the PHI by Associate in violation of the requirements of this Addendum.

6. **Reporting and Related Obligations.**

(a) Google will promptly notify of (i) any Security Incident of which Google becomes aware, subject to Section 6(c); and (ii) any Breach that Google discovers, provided that any notice for Breach will be made promptly and without unreasonable delay, and in no case later than 60 calendar days after discovery. Notifications made under this section will describe, to the extent possible, details of a Breach, including steps taken to mitigate the potential risks and steps Google recommends Partner take to address the Breach.

(b) Google will send any applicable notifications to the Notification Email Address(es) or via direct communication with Partner.

(c) Notwithstanding Section 6(a), this Section 6(c) will be deemed as notice to Partner that Google periodically receives unsuccessful attempts for unauthorized access, use, disclosure, modification, or destruction of information, or interference with the general operation of Google's systems and the Covered Services.

(d) Partner is solely responsible for managing whether Customers and Partner End Users are authorized to share, disclose, create, and/or use PHI with Covered Services and Google will have no obligations relating to any Customer or Partner End User authorizations.

7. **Subcontractors.** Google will take appropriate measures to ensure that any Subcontractors used by Google to perform its obligations under the Partner Agreement that require access to PHI on behalf of Google are bound by written obligations that provide the same material level of protection for PHI as this BAA. To the extent Google uses Subcontractors in its performance of obligations hereunder, Google will remain responsible for their performance as if performed by Google.

8. **Access and Amendment.** Partner acknowledges and agrees that Partner is solely responsible for the form and content of PHI maintained by Partner within the Covered Services, including whether Partner maintains such PHI in a Designated Record Set within the Covered Services. Google will provide Partner with access to PHI received from Partner via the Covered Services so Partner may fulfill its obligations under HIPAA with respect to Individuals' rights of access and amendment, but will have no

other obligations to Partner or any Individual with respect to the rights afforded to Individuals by HIPAA with respect to Designated Record Sets, including rights of access or amendment of PHI. Partner is responsible for managing its and its Partner End Users' use of the Covered Services to appropriately respond to such individual requests.

9. **Accounting of Disclosures**. Google will document disclosures of PHI by Google and provide an accounting of such disclosures to Partner as and to the extent required of a Business Associate under HIPAA and in accordance with the requirements applicable to a Business Associate under HIPAA.

10. **Access to Records**. To the extent required by law, and subject to applicable attorney client privileges, Google will make its internal practices, books, and records concerning the use and disclosure of PHI received from Partner, or created or received by Google on behalf of Partner, available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for the purpose of the Secretary determining compliance with this BAA.

11. **Expiration and Termination**.

(a) This BAA will terminate on the earlier of (i) a permitted termination in accordance with Section 11(b), or (ii) the expiration or termination of the Partner Agreement under which Partner has access to a Covered Service.

(b) If either party materially breaches this BAA, the non-breaching party may terminate this BAA on 10 days' written notice to the breaching party unless the breach is cured within the 10-day period. If a cure under this Section 11(b) is not reasonably possible, the non-breaching party may immediately terminate this BAA, or if neither termination nor cure is reasonably possible under this Section 11(b), the non-breaching party may report the violation to the Secretary, subject to all applicable legal privileges.

(c) If this BAA is terminated earlier than the Partner Agreement, Partner may continue to use the Services in accordance with the Partner Agreement, but must delete any PHI it maintains in the Covered Services and cease to further create, receive, maintain, or transmit such PHI to Google.

12. **Return/Destruction of Information**. On termination of the Partner Agreement, Google will return or destroy all PHI received from Partner, and retain no copies, or created or received by Google on behalf of Partner; provided, however, that if such return or destruction is not feasible, Google will extend the protections of this BAA to the PHI not returned or destroyed and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible. The duty of Google and its agents and subcontractors to assist Partner with any HIPAA required account of disclosures survives the termination of the underlying Agreement to the extent required of a Business Associate under HIPAA.

13. **Miscellaneous**.

(a) Survival. Sections 12 (Return/Destruction of Information) and 13 (Miscellaneous) will survive termination or expiration of this BAA to the extent required of a Business Associate under HIPAA.

(b) Counterparts. The parties may execute this BAA in counterparts, including facsimile, PDF, or other electronic copies, which taken together will constitute one instrument.

(c) Effects of Addendum. The Partner Agreement remains in full force and effect except as modified by this BAA. To the extent the Partner Agreement and this BAA conflict, this BAA governs. The General Terms section titled "Governing Law" applies to this BAA.

Signed by the parties' authorized representatives on the dates below.

Google:	**Partner:**
By:	By:
Print Name:	Print Name:
Title:	Title:
Date:	Date:

Attachment 1
List of Covered Services

- Any Google Cloud Platform product or service specifically identified at https://cloud.google.com/security/compliance/hipaa/ as being covered by the Google Cloud BAA (collectively "GCP Covered Services").

- Looker Services described at https://cloud.google.com/terms/looker/security/hipaa as within scope for this BAA (the "Looker Covered Services").

Attachment 2 HIPAA Implementation Guide

For GCP Covered Services:

- The HIPAA Implementation Guide is available for review at the following URL: https://cloud.google.com/security/compliance/hipaa/

For Looker Covered Services:

- The HIPAA Implementation Guide is available for review at the following URL: https://cloud.google.com/terms/looker/security/hipaa

Back to Google Cloud Terms Directory (/product-terms) > Current

Cloud Data Processing Addendum (Customers)

This Cloud Data Processing Addendum including its appendices ("*Addendum*") is incorporated into the Agreement(s) under which Google has agreed to provide Google Cloud Platform, Google Workspace, or Cloud Identity (each as defined below), as applicable (the "*Services*"), to Customer. This Addendum was formerly known as the "Data Processing and Security Terms" under an Agreement for Google Cloud Platform and the "Data Processing Amendment" under an Agreement for Google Workspace or Cloud Identity.

1. Commencement

This Addendum will be effective and replace any terms previously applicable to the processing of Customer Data, including any Data Processing and Security Terms or Data Processing Amendment, from the Addendum Effective Date (as defined below).

2. Definitions

2.1 Capitalized terms used but not defined in this Addendum have the meaning given to them in the Agreement:

- *Account* has the meaning given in the applicable Agreement or, if no such meaning is given, means Customer's Google Cloud Platform account, Google Workspace account or Cloud Identity account, as applicable.
- *Addendum Effective Date* means the date on which Customer accepted, or the parties otherwise agreed to, this Addendum.
- *Additional Security Controls* means security resources, features, functionality and/or controls that Customer may use at its option and/or as it determines, including the

Admin Console, encryption, logging and monitoring, identity and access management, security scanning, and firewalls.

- *Adequate Country* means:

  (a) for data processed subject to the EU GDPR: the EEA, or a country or territory recognized as ensuring adequate protection under the EU GDPR;

  (b) for data processed subject to the UK GDPR: the UK, or a country or territory recognized as ensuring adequate protection under the UK GDPR and the Data Protection Act 2018; and/or

  (c) for data processed subject to the Swiss FDPA: Switzerland, or a country or territory that is: (i) included in the list of the states whose legislation ensures adequate protection as published by the Swiss Federal Data Protection and Information Commissioner, or (ii) recognized as ensuring adequate protection by the Swiss Federal Council under the Swiss FDPA;

  in each case, other than on the basis of an optional data protection framework.

- *Alternative Transfer Solution* means a solution, other than SCCs, that enables the lawful transfer of personal data to a third country in accordance with European Data Protection Law, for example a data protection framework recognized as ensuring that participating entities provide adequate protection.

- *Audited Services* means the then-current Services indicated as being in-scope for the relevant certification or report at https://cloud.google.com/security/compliance/services-in-scope (/security/compliance/services-in-scope). Google may not remove any Services from this URL unless those Services have been discontinued in accordance with the applicable Agreement.

- *Cloud Identity* means the Cloud Identity Services described at https://cloud.google.com/terms/identity/user-features (/terms/identity/user-features), when purchased under a standalone Agreement.

- *Customer Data* has the meaning given in the applicable Agreement or, if no such meaning is given, means:

  (a) data provided by or on behalf of Customer or its End Users via Google Cloud Platform under the Account; or

(b) data submitted, stored, sent or received by or on behalf of Customer or its End Users via Google Workspace or Cloud Identity under the Account.

- *Customer Personal Data* means the personal data contained within the Customer Data, including any special categories of personal data defined under European Data Protection Law.
- *Customer SCCs* means the SCCs (Controller-to-Processor), the SCCs (Processor-to-Processor) and/or the SCCs (Processor-to-Controller), as applicable.
- *Data Incident* means a breach of Google's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed by or otherwise controlled by Google.
- *EEA* means the European Economic Area.
- *EMEA* means Europe, the Middle East and Africa.
- *EU GDPR* means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
- *European Data Protection Law* means, as applicable: (a) the GDPR; and/or (b) the Swiss FDPA.
- *European Law* means, as applicable: (a) EU or EU Member State law (if the EU GDPR applies to the processing of Customer Personal Data); and (b) the law of the UK or a part of the UK (if the UK GDPR applies to the processing of Customer Personal Data).
- *GDPR* means, as applicable: (a) the EU GDPR; and/or (b) the UK GDPR.
- *Google Cloud Platform* means the Google Cloud Platform services described at https://cloud.google.com/terms/services (https://cloud.google.com/terms/services), excluding any Third-Party Offerings.
- *Google Workspace* means the Google Workspace or Google Workspace for Education services described at https://workspace.google.com/terms/user_features.html (https://workspace.google.com/terms/user_features.html), as applicable.

- *Google's Third Party Auditor* means a Google-appointed, qualified and independent third party auditor, whose then-current identity Google will disclose to Customer.
- *Instructions* has the meaning given in Section 5.2.1 (Compliance with Customer's Instructions).
- *Non-European Data Protection Law* means data protection or privacy laws in force outside the EEA, the UK and Switzerland.
- *Notification Email Address* means the email address(es) designated by Customer in the Admin Console or Order Form to receive certain notifications from Google. Customer is responsible for using the Admin Console to ensure that its Notification Email Address remains current and valid.
- *SCCs* means the Customer SCCs and/or SCCs (Processor-to-Processor, Google Exporter), as applicable.
- *SCCs (Controller-to-Processor)* means the terms at: https://cloud.google.com/terms/sccs/eu-c2p (https://cloud.google.com/terms/sccs/eu-c2p)
- *SCCs (Processor-to-Controller)* means the terms at: https://cloud.google.com/terms/sccs/eu-p2c (https://cloud.google.com/terms/sccs/eu-p2c)
- *SCCs (Processor-to-Processor)* means the terms at: https://cloud.google.com/terms/sccs/eu-p2p (https://cloud.google.com/terms/sccs/eu-p2p)
- *SCCs (Processor-to-Processor, Google Exporter)* means the terms at: https://cloud.google.com/terms/sccs/eu-p2p-google-exporter (https://cloud.google.com/terms/sccs/eu-p2p-google-exporter)
- *Security Documentation* means all documents and information made available by Google under Section 7.5.1 (Reviews of Security Documentation).
- *Security Measures* has the meaning given in Section 7.1.1 (Google's Security Measures).
- *Subprocessor* means a third party authorized as another processor under this Addendum to have logical access to and process Customer Data in order to provide parts of the Services and TSS.

- *Supervisory Authority* means, as applicable: (a) a "supervisory authority" as defined in the EU GDPR; and/or (b) the "Commissioner" as defined in the UK GDPR and/or the Swiss FDPA.
- *Swiss FDPA* means the Federal Data Protection Act of 19 June 1992 (Switzerland).
- *Term* means the period from the Addendum Effective Date until the end of Google's provision of the Services, including, if applicable, any period during which provision of the Services may be suspended and any post-termination period during which Google may continue providing the Services for transitional purposes.
- *UK GDPR* means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, and applicable secondary legislation made under that Act.

2.2 The terms "personal data", "data subject", "processing", "controller" and "processor" as used in this Addendum have the meanings given in the GDPR irrespective of whether European Data Protection Law or Non-European Data Protection Law applies.

3. Duration

Regardless of whether the applicable Agreement has terminated or expired, this Addendum will remain in effect until, and automatically expire when, Google deletes all Customer Data as described in this Addendum.

4. Scope of Data Protection Law

4.1 *Application of European Law*. The parties acknowledge that European Data Protection Law will apply to the processing of Customer Personal Data if, for example:

a. the processing is carried out in the context of the activities of an establishment of Customer in the territory of the EEA or the UK; and/or

b. the Customer Personal Data is personal data relating to data subjects who are in the EEA or the UK and the processing relates to the offering to them of goods or services in the EEA or the UK, or the monitoring of their behavior in the EEA or the UK.

4.2 *Application of Non-European Law*. The parties acknowledge that Non-European Data Protection Law may also apply to the processing of Customer Personal Data.

4.3 *Application of Addendum*. Except to the extent this Addendum states otherwise, this Addendum will apply irrespective of whether European Data Protection Law or Non-European Data Protection Law applies to the processing of Customer Personal Data.

5. Processing of Data

5.1 *Roles and Regulatory Compliance; Authorization*.

5.1.1 *Processor and Controller Responsibilities*. If European Data Protection Law applies to the processing of Customer Personal Data:

a. the subject matter and details of the processing are described in Appendix 1;

b. Google is a processor of that Customer Personal Data under European Data Protection Law;

c. Customer is a controller or processor, as applicable, of that Customer Personal Data under European Data Protection Law; and

d. each party will comply with the obligations applicable to it under European Data Protection Law with respect to the processing of that Customer Personal Data.

5.1.2 *Processor Customers*. If European Data Protection Law applies to the processing of Customer Personal Data and Customer is a processor:

a. Customer warrants on an ongoing basis that the relevant controller has authorized: (i) the Instructions, (ii) Customer's appointment of Google as another processor, and (iii) Google's engagement of Subprocessors as described in Section 11 (Subprocessors);

b. Customer will immediately forward to the relevant controller any notice provided by Google under Sections 5.2.2 (Instruction Notifications), 7.2.1 (Incident Notification), 9.2.1 (Responsibility for Requests), 11.4 (Opportunity to Object to Subprocessor Changes) or that refers to any SCCs; and

c. Customer may:

i. request access for the relevant controller to the SOC Reports in accordance with Section 7.5.3(a); and

ii. make available to the relevant controller any other information made available by Google under Sections 10.4 (Supplementary Measures and Information), 10.6 (Data Center Information) and 11.2 (Information about Subprocessors).

5.1.3 *Responsibilities under Non-European Law.* If Non-European Data Protection Law applies to either party's processing of Customer Personal Data, the relevant party will comply with any obligations applicable to it under that law with respect to the processing of that Customer Personal Data.

5.2 *Scope of Processing.*

5.2.1 *Compliance with Customer's Instructions.* Customer instructs Google to process Customer Data in accordance with the applicable Agreement (including this Addendum) and applicable law only: (a) to provide, secure, and monitor the Services and TSS; and (b) as further specified via (i) Customer's use of the Services (including the Admin Console and other Services functionality) and TSS, and (ii) any other written instructions given by Customer and acknowledged by Google as constituting instructions under this Addendum (collectively, the "*Instructions*"). Google will comply with the Instructions unless prohibited by European Law.

5.2.2 *Instruction Notifications.* Without prejudice to Google's obligations under Section 5.2.1 (Compliance with Customer's Instructions) or any other rights or obligations of either party under the applicable Agreement, Google will immediately notify Customer if, in Google's opinion: (a) European Law prohibits Google from complying with an Instruction; (b) an Instruction does not comply with European Data Protection Law; or (c) Google is otherwise unable to comply with an Instruction, in each case unless such notice is prohibited by European Law.

5.3 *Additional Products.* If Google at its option makes Additional Products available to Customer for use with Google Workspace or Cloud Identity in accordance with applicable Additional Product Terms:

a. Customer may enable or disable Additional Products via the Admin Console and will not need to use Additional Products in order to use Google Workspace or Cloud Identity; and

b. if Customer opts to install any Additional Products or to use them with Google Workspace or Cloud Identity, the Additional Products may access Customer Data as required to interoperate with Google Workspace or Cloud Identity (as applicable).

For clarity, this Addendum does not apply to the processing of personal data in connection with the provision of any Additional Products installed or used by Customer, including personal data transmitted to or from such Additional Products.

6. Data Deletion

6.1 *Deletion by Customer*. Google will enable Customer to delete Customer Data during the Term in a manner consistent with the functionality of the Services. If Customer uses the Services to delete any Customer Data during the Term and that Customer Data cannot be recovered by Customer, this use will constitute an Instruction to Google to delete the relevant Customer Data from Google's systems in accordance with applicable law. Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage.

6.2 *Return or Deletion When Term Ends*. If Customer wishes to retain any Customer Data after the end of the Term, it may instruct Google in accordance with Section 9.1 (Access; Rectification; Restricted Processing; Portability) to return that data during the Term. Subject to Section 6.3 (Deferred Deletion Instruction), Customer instructs Google to delete all remaining Customer Data (including existing copies) from Google's systems at the end of the Term in accordance with applicable law. After a recovery period of up to 30 days from that date, Google will comply with this Instruction as soon as reasonably practicable and within a maximum period of 180 days, unless European Law requires storage.

6.3. *Deferred Deletion Instruction*. To the extent any Customer Data covered by the deletion instruction described in Section 6.2 (Return or Deletion When Term Ends) is also processed, when the applicable Term under Section 6.2 expires, in relation to an Agreement with a continuing Term, such deletion instruction will take effect with respect to such Customer Data only when the continuing Term expires. For clarity, this Addendum will continue to apply to such Customer Data until its deletion by Google.

7. Data Security

7.1 *Google's Security Measures, Controls and Assistance*.

7.1.1 *Google's Security Measures*. Google will implement and maintain technical, organizational and physical measures to protect Customer Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access as described in Appendix 2 (the "*Security Measures*"). The Security Measures include measures to encrypt Customer Data; to help ensure ongoing confidentiality, integrity, availability and resilience

of Google's systems and services; to help restore timely access to Customer Data following an incident; and for regular testing of effectiveness. Google may update the Security Measures from time to time provided that such updates do not result in a material reduction of the security of the Services.

7.1.2 *Access and Compliance*. Google will: (a) authorize its employees, contractors and Subprocessors to access Customer Data only as strictly necessary to comply with Instructions; (b) take appropriate steps to ensure compliance with the Security Measures by its employees, contractors and Subprocessors to the extent applicable to their scope of performance; and (c) ensure that all persons authorized to process Customer Data are under an obligation of confidentiality.

7.1.3 *Additional Security Controls*. Google will make Additional Security Controls available to: (a) allow Customer to take steps to secure Customer Data; and (b) provide Customer with information about securing, accessing and using Customer Data.

7.1.4 *Google's Security Assistance*. Google will (taking into account the nature of the processing of Customer Personal Data and the information available to Google) assist Customer in ensuring compliance with its (or, where Customer is a processor, the relevant controller's) obligations under Articles 32 to 34 of the GDPR, by:

a. implementing and maintaining the Security Measures in accordance with Section 7.1.1 (Google's Security Measures);

b. making Additional Security Controls available to Customer in accordance with Section 7.1.3 (Additional Security Controls);

c. complying with the terms of Section 7.2 (Data Incidents);

d. providing Customer with the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation) and the information contained in the applicable Agreement (including this Addendum); and

e. if subsections (a)-(d) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

7.2 *Data Incidents*.

7.2.1 *Incident Notification*. Google will notify Customer promptly and without undue delay after becoming aware of a Data Incident, and promptly take reasonable steps to minimize

harm and secure Customer Data.

7.2.2 *Details of Data Incident*. Google's notification of a Data Incident will describe: the nature of the Data Incident including the Customer resources impacted; the measures Google has taken, or plans to take, to address the Data Incident and mitigate its potential risk; the measures, if any, Google recommends that Customer take to address the Data Incident; and details of a contact point where more information can be obtained. If it is not possible to provide all such information at the same time, Google's initial notification will contain the information then available and further information will be provided without undue delay as it becomes available.

7.2.3 *Delivery of Notification*. Notification(s) of any Data Incident(s) will be delivered to the Notification Email Address.

7.2.4 *No Assessment of Customer Data by Google*. Google has no obligation to assess Customer Data in order to identify information subject to any specific legal requirements.

7.2.5 *No Acknowledgement of Fault by Google*. Google's notification of or response to a Data Incident under this Section 7.2 (Data Incidents) will not be construed as an acknowledgement by Google of any fault or liability with respect to the Data Incident.

7.3 *Customer's Security Responsibilities and Assessment*.

7.3.1 *Customer's Security Responsibilities*. Without prejudice to Google's obligations under Sections 7.1 (Google's Security Measures, Controls and Assistance) and 7.2 (Data Incidents), and elsewhere in the applicable Agreement, Customer is responsible for its use of the Services and its storage of any copies of Customer Data outside Google's or Google's Subprocessors' systems, including:

a. using the Services and Additional Security Controls to ensure a level of security appropriate to the risk to the Customer Data;

b. securing the account authentication credentials, systems and devices Customer uses to access the Services; and

c. backing up or retaining copies of its Customer Data as appropriate.

7.3.2 *Customer's Security Assessment*. Customer agrees that the Services, Security Measures implemented and maintained by Google, Additional Security Controls and Google's commitments under this Section 7 (Data Security) provide a level of security appropriate to the risk to Customer Data (taking into account the state of the art, the costs

of implementation and the nature, scope, context and purposes of the processing of Customer Personal Data as well as the risks to individuals).

7.4 *Compliance Certifications and SOC Reports.* Google will maintain at least the following for the Audited Services in order to evaluate the continued effectiveness of the Security Measures: (a) certificates for ISO 27001, ISO 27017 and ISO 27018 and, for Google Cloud Platform, a PCI DSS Attestation of Compliance (the "*Compliance Certifications*"); and (b) SOC 2 and SOC 3 reports produced by Google's Third Party Auditor and updated annually based on an audit performed at least once every 12 months (the "*SOC Reports*"). Google may add standards at any time. Google may replace a Compliance Certification or SOC Report with an equivalent or enhanced alternative.

7.5 *Reviews and Audits of Compliance.*

7.5.1 *Reviews of Security Documentation.* Google will make the Compliance Certifications and the SOC Reports available for review by Customer to demonstrate compliance by Google with its obligations under this Addendum.

7.5.2 *Customer's Audit Rights.*

a. If European Data Protection Law applies to the processing of Customer Personal Data, Google will allow Customer or an independent auditor appointed by Customer to conduct audits (including inspections) to verify Google's compliance with its obligations under this Addendum in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits). During an audit, Google will make available all information necessary to demonstrate such compliance and contribute to the audit as described in Section 7.4 (Compliance Certifications and SOC Reports) and this Section 7.5 (Reviews and Audits of Compliance).

b. If Customer SCCs apply as described in Section 10.2 (Restricted European Transfers), Google will allow Customer (or an independent auditor appointed by Customer) to conduct audits as described in those SCCs and, during an audit, make available all information required by those SCCs, both in accordance with Section 7.5.3 (Additional Business Terms for Reviews and Audits).

c. Customer may conduct an audit to verify Google's compliance with its obligations under this Addendum by reviewing the Security Documentation (which reflects the outcome of audits conducted by Google's Third Party Auditor).

7.5.3 *Additional Business Terms for Reviews and Audits.*

a. Customer must send any requests for reviews of the SOC 2 report under Section 5.1.2(c)(i) or 7.5.1, or audits under Section 7.5.2(a) or 7.5.2(b), to Google's Cloud Data Protection Team as described in Section 12 (Cloud Data Protection Team; Processing Records).

b. Following receipt by Google of a request under Section 7.5.3(a), Google and Customer will discuss and agree in advance on: (i) the reasonable date(s) of and security and confidentiality controls applicable to any review of the SOC 2 report under Section 5.1.2(c)(i) or 7.5.1; and (ii) the reasonable start date, scope and duration of and security and confidentiality controls applicable to any audit under Section 7.5.2(a) or 7.5.2(b).

c. Google may charge a fee (based on Google's reasonable costs) for any audit under Section 7.5.2(a) or 7.5.2(b). Google will provide Customer with further details of any applicable fee, and the basis of its calculation, in advance of any such audit. Customer will be responsible for any fees charged by any auditor appointed by Customer to execute any such audit.

d. Google may object in writing to an auditor appointed by Customer to conduct any audit under Section 7.5.2(a) or 7.5.2(b) if the auditor is, in Google's reasonable opinion, not suitably qualified or independent, a competitor of Google, or otherwise manifestly unsuitable. Any such objection by Google will require Customer to appoint another auditor or conduct the audit itself.

8. Impact Assessments and Consultations

Google will (taking into account the nature of the processing and the information available to Google) assist Customer in ensuring compliance with its (or, where Customer is a processor, the relevant controller's) obligations under Articles 35 and 36 of the GDPR, by:

a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls) and the Security Documentation in accordance with Section 7.5.1 (Reviews of Security Documentation);

b. providing the information contained in the applicable Agreement (including this Addendum); and

c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

9. Access etc.; Data Subject Rights; Data Export

9.1 *Access; Rectification; Restricted Processing; Portability*. During the Term, Google will enable Customer, in a manner consistent with the functionality of the Services, to access, rectify and restrict processing of Customer Data, including via the deletion functionality provided by Google as described in Section 6.1 (Deletion by Customer), and to export Customer Data. If Customer becomes aware that any Customer Personal Data is inaccurate or outdated, Customer will be responsible for using such functionality to rectify or delete that data if required by applicable European Data Protection Law.

9.2 *Data Subject Requests*.

9.2.1 *Responsibility for Requests*. During the Term, if Google's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Google will: (a) advise the data subject to submit their request to Customer; (b) promptly notify Customer; and (c) not otherwise respond to that data subject's request without authorization from Customer. Customer will be responsible for responding to any such request including, where necessary, by using the functionality of the Services.

9.2.2 *Google's Data Subject Request Assistance*. Google will (taking into account the nature of the processing of Customer Personal Data) assist Customer in fulfilling its (or, where Customer is a processor, the relevant controller's) obligations under Chapter III of the GDPR to respond to requests for exercising the data subject's rights by:

a. providing Additional Security Controls in accordance with Section 7.1.3 (Additional Security Controls);

b. complying with Sections 9.1 (Access; Rectification; Restricted Processing; Portability) and 9.2.1 (Responsibility for Requests); and

c. if subsections (a) and (b) above are insufficient for Customer (or the relevant controller) to comply with such obligations, upon Customer's request, providing Customer with additional reasonable cooperation and assistance.

10. Data Transfers

10.1 *Data Storage and Processing Facilities*. Subject to Google's data location commitments under the Service Specific Terms and the remainder of this Section 10 (Data Transfers),

Customer Data may be processed in any country in which Google or its Subprocessors maintain facilities.

10.2 *Restricted European Transfers*. The parties acknowledge that European Data Protection Law does not require SCCs or an Alternative Transfer Solution in order for Customer Personal Data to be processed in or transferred to an Adequate Country. If Customer Personal Data is transferred to any other country and European Data Protection Law applies to the transfers (as certified by Customer under Section 10.3 (Certification by Non-EMEA Customers) if its billing address is outside EMEA) ("*Restricted European Transfers*"), then:

a. if Google has adopted an Alternative Transfer Solution for any Restricted European Transfers, then Google will inform Customer of the relevant solution and ensure that such Restricted European Transfers are made in accordance with it; and/or

b. if Google has not adopted, or informs Customer that Google is no longer adopting, an Alternative Transfer Solution for any Restricted European Transfers, then:

i. if Google's address is in an Adequate Country:

A. the SCCs (Processor-to-Processor, Google Exporter) will apply with respect to such Restricted European Transfers from Google to Subprocessors; and

B. in addition, if Customer's billing address is not in an Adequate Country, the SCCs (Processor-to Controller) will apply (regardless of whether Customer is a controller and/or processor) with respect to such Restricted European Transfers between Google and Customer; or

ii. if Google's address is not in an Adequate Country, the SCCs (Controller-to-Processor) and/or SCCs (Processor-to-Processor) will apply (according to whether Customer is a controller and/or processor) with respect to such Restricted European Transfers between Google and Customer.

10.3 *Certification by Non-EMEA Customers*. If Customer's billing address is outside EMEA, and the processing of Customer Personal Data is subject to European Data Protection Law, Customer will certify as such, and identify its competent Supervisory Authority, via the Admin Console for Google Cloud Platform or Google Workspace and Cloud Identity, as applicable.

10.4 *Supplementary Measures and Information*. Google will provide Customer with information relevant to Restricted European Transfers, including information about Additional Security Controls and other supplementary measures to protect Customer Personal Data:

a. as described in Section 7.5.1 (Reviews of Security Documentation);

b. in the documentation for the Services, available at https://cloud.google.com/docs (https://cloud.google.com/docs); and

c. in the Google Cloud Trust and Security website, available at https://cloud.google.com/security (/security).

10.5 *Termination*. If Customer concludes, based on its current or intended use of the Services, that the Alternative Transfer Solution and/or SCCs, as applicable, do not provide appropriate safeguards for Customer Personal Data, then Customer may immediately terminate the applicable Agreement for convenience by notifying Google.

10.6 *Data Center Information*. The locations of Google data centers are described at:

a. https://cloud.google.com/about/locations/ (https://cloud.google.com/about/locations/) for Google Cloud Platform; and

b. https://www.google.com/about/datacenters/locations/ (https://www.google.com/about/datacenters/locations/?_ga=2.51070953.1907356626.1655412346-310495072.1655412346) for Google Workspace and Cloud Identity.

11. Subprocessors

11.1 *Consent to Subprocessor Engagement*. Customer specifically authorizes the engagement as Subprocessors of those entities disclosed under Section 11.2 (Information about Subprocessors) as of the Addendum Effective Date. In addition, without prejudice to Section 11.4 (Opportunity to Object to Subprocessor Changes), Customer generally authorizes the engagement of other third parties as Subprocessors ("*New Subprocessors*").

11.2 *Information about Subprocessors*. Names, locations and activities of Subprocessors are described at:

a. https://cloud.google.com/terms/subprocessors (https://cloud.google.com/terms/third-party-suppliers) for Google Cloud Platform; and

b. https://workspace.google.com/intl/en/terms/subprocessors.html (https://workspace.google.com/intl/en/terms/subprocessors.html) for Google Workspace and Cloud Identity.

11.3 *Requirements for Subprocessor Engagement*. When engaging any Subprocessor, Google will:

a. ensure via a written contract that:

i. the Subprocessor only accesses and uses Customer Data to the extent required to perform the obligations subcontracted to it, and does so in accordance with the applicable Agreement (including this Addendum); and

ii. if the processing of Customer Personal Data is subject to European Data Protection Law, the data protection obligations described in this Addendum (as referred to in Article 28(3) of the GDPR, if applicable), are imposed on the Subprocessor; and

b. remain fully liable for all obligations subcontracted to, and all acts and omissions of, the Subprocessor.

11.4 *Opportunity to Object to Subprocessor Changes*.

a. When any New Subprocessor is engaged during the Term, Google will, at least 30 days before the New Subprocessor starts processing any Customer Data, notify Customer of the engagement (including the name, location and activities of the New Subprocessor).

b. Customer may, within 90 days after being notified of the engagement of a New Subprocessor, object by immediately terminating the applicable Agreement for convenience by notifying Google.

12. Cloud Data Protection Team; Processing Records

12.1 *Cloud Data Protection Team*. Google's Cloud Data Protection Team will provide prompt and reasonable assistance with any Customer queries related to processing of Customer Data under the applicable Agreement and can be contacted:

a. at https://support.google.com/cloud/contact/dpo (https://support.google.com/cloud/contact/dpo) for Google Cloud Platform;

b. at https://support.google.com/a/contact/googlecloud_dpr (https://support.google.com/a/contact/googlecloud_dpr) for Google Workspace and Cloud Identity (while Administrators are signed in to their Admin Account); or

c. as described in the Notices section of the applicable Agreement.

12.2 *Google's Processing Records*. Google will keep appropriate documentation of its processing activities as required by the GDPR. To the extent the GDPR requires Google to collect and maintain records of certain information relating to Customer, Customer will use the Admin Console to supply such information and keep it accurate and up-to-date. Google may make any such information available to the Supervisory Authorities if required by the GDPR.

12.3 *Controller Requests*. During the Term, if Google's Cloud Data Protection Team receives a request or instruction from a third party purporting to be a controller of Customer Personal Data, Google will advise the third party to contact Customer.

13. Interpretation

13.1 *Precedence*.

a. To the extent of any conflict or inconsistency between:

i. this Addendum and the remainder of the Agreement, this Addendum will prevail; and

ii. any Customer SCCs (which are incorporated by reference into this Addendum) and the remainder of the Agreement (including this Addendum), the Customer SCCs will prevail.

b. For clarity, if Customer has entered more than one Agreement, this Addendum will amend each of the Agreements separately.

13.2 *Legacy UK SCCs*. The supplementary terms for UK GDPR transfers in the SCCs will, as of 21 September 2022, supersede and terminate any standard contractual clauses approved under the UK GDPR or Data Protection Act 2018 and previously entered into by Customer and Google.

13.3 *No Modification of SCCs*. Nothing in the Agreement (including this Addendum) is intended to modify or contradict any SCCs or prejudice the fundamental rights or freedoms of data subjects under European Data Protection Law.

Appendix 1: Subject Matter and Details of the Data Processing

Subject Matter

Google's provision of the Services and TSS to Customer.

Duration of the Processing

The Term plus the period from the end of the Term until deletion of all Customer Data by Google in accordance with this Addendum.

Nature and Purpose of the Processing

Google will process Customer Personal Data for the purposes of providing the Services and TSS to Customer in accordance with this Addendum.

Categories of Data

Data relating to individuals provided to Google via the Services, by (or at the direction of) Customer or by its End Users.

Data Subjects

Data subjects include the individuals about whom data is provided to Google via the Services by (or at the direction of) Customer or by its End Users.

Appendix 2: Security Measures

As from the Addendum Effective Date, Google will implement and maintain the Security Measures described in this Appendix 2.

1. Data Center and Network Security

(a) Data Centers.

Infrastructure. Google maintains geographically distributed data centers. Google stores all production data in physically secure data centers.

Redundancy. Infrastructure systems have been designed to eliminate single points of failure and minimize the impact of anticipated environmental risks. Dual circuits, switches, networks or other necessary devices help provide this redundancy. The Services are designed to allow Google to perform certain types of preventative and corrective maintenance without interruption. All environmental equipment and facilities have documented preventative maintenance procedures that detail the process for and frequency of performance in accordance with the manufacturer's or internal specifications. Preventative and corrective maintenance of the data center equipment is scheduled through a standard change process according to documented procedures.

Power. The data center electrical power systems are designed to be redundant and maintainable without impact to continuous operations, 24 hours a day, 7 days a week. In most cases, a primary as well as an alternate power source, each with equal capacity, is provided for critical infrastructure components in the data center. Backup power is provided by various mechanisms such as uninterruptible power supplies (UPS) batteries, which supply consistently reliable power protection during utility brownouts, blackouts, over voltage, under voltage, and out-of-tolerance frequency conditions. If utility power is interrupted, backup power is designed to provide transitory power to the data center, at full capacity, for up to 10 minutes until the backup generator systems take over. The backup generators are capable of automatically starting up within seconds to provide enough emergency electrical power to run the data center at full capacity typically for a period of days.

Server Operating Systems. Google servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. Google employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Businesses Continuity. Google has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks and Transmission.

Data Transmission. Data centers are typically connected via high-speed private links to provide secure and fast data transfer between data centers. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media. Google transfers data via Internet standard protocols.

External Attack Surface. Google employs multiple layers of network devices and intrusion detection to protect its external attack surface. Google considers potential attack vectors and incorporates appropriate purpose built technologies into external facing systems.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. Google's intrusion detection involves:

1. tightly controlling the size and make-up of Google's attack surface through preventative measures;
2. employing intelligent detection controls at data entry points; and
3. employing technologies that automatically remedy certain dangerous situations.

Incident Response. Google monitors a variety of communication channels for security incidents, and Google's security personnel will react promptly to known incidents.

Encryption Technologies. Google makes HTTPS encryption (also referred to as SSL or TLS connection) available. Google servers support ephemeral elliptic curve Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

2. Access and Site Controls

(a) Site Controls.

On-site Data Center Security Operation. Google's data centers maintain an on-site security operation responsible for all physical data center security functions 24 hours a day, 7 days a week. The on-site security operation personnel monitor closed circuit TV (CCTV) cameras and all alarm systems. On-site security operation personnel perform internal and external patrols of the data center regularly.

Data Center Access Procedures. Google maintains formal access procedures for allowing physical access to the data centers. The data centers are housed in facilities that require electronic card key access, with alarms that are linked to the on-site security operation. All entrants to the data center are required to identify themselves as well as show proof of identity to on-site security operations. Only authorized employees, contractors and visitors are allowed entry to the data centers. Only authorized employees and contractors are permitted to request electronic card key access to these facilities. Data center electronic

card key access requests must be made through e-mail, and require the approval of the requestor's manager and the data center director. All other entrants requiring temporary data center access must: (i) obtain approval in advance from the data center managers for the specific data center and internal areas they wish to visit; (ii) sign in at on-site security operations; and (iii) reference an approved data center access record identifying the individual as approved.

On-site Data Center Security Devices. Google's data centers employ a dual authentication access control system that is linked to a system alarm. The access control system monitors and records each individual's electronic card key and when they access perimeter doors, shipping and receiving, and other critical areas. Unauthorized activity and failed access attempts are logged by the access control system and investigated, as appropriate. Authorized access throughout the business operations and data centers is restricted based on zones and the individual's job responsibilities. The fire doors at the data centers are alarmed. CCTV cameras are in operation both inside and outside the data centers. The positioning of the cameras has been designed to cover strategic areas including, among others, the perimeter, doors to the data center building, and shipping/receiving. On-site security operations personnel manage the CCTV monitoring, recording and control equipment. Secure cables throughout the data centers connect the CCTV equipment. Cameras record on site via digital video recorders 24 hours a day, 7 days a week. The surveillance records are retained for up to 30 days based on activity.

(b) Access Control.

Infrastructure Security Personnel. Google has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. Google's infrastructure security personnel are responsible for the ongoing monitoring of Google's security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. Customer's administrators and End Users must authenticate themselves via a central authentication system or via a single sign on system in order to use the Services.

Internal Data Access Processes and Policies – Access Policy. Google's internal data access processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process Customer Data. Google designs its systems to (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that Customer Data cannot be read, copied, altered or removed without

authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. Google employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. Google's authentication and authorization systems utilize SSH certificates and security keys, and are designed to provide Google with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. Google requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with Google's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g. login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength. For access to extremely sensitive information (e.g. credit card data), Google uses hardware tokens.

3. Data

(a) *Data Storage, Isolation and Logging*. Google stores data in a multi-tenant environment on Google-owned servers. Subject to any Instructions to the contrary (e.g. in the form of a data location selection), Google replicates Customer Data between multiple geographically dispersed data centers. Google also logically isolates Customer Data and, for Google Workspace and Cloud Identity: (i) Google logically separates each End User's data from the data of other End Users; and (ii) data for an authenticated End User will not be displayed to another End User (unless the former End User or an Administrator allows the data to be shared). Customer will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable Customer to determine the product sharing settings applicable to its End Users for specific purposes. Customer may choose to use logging functionality that Google makes available via the Services.

(b) *Decommissioned Disks and Disk Erase Policy*. Disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk is subject to a series of data destruction processes (the "Disk Erase Policy") before leaving Google's premises either for

reuse or destruction. Decommissioned Disks are erased in a multi-step process and verified complete by at least two independent validators. The erase results are logged by the Decommissioned Disk's serial number for tracking. Finally, the erased Decommissioned Disk is released to inventory for reuse and redeployment. If, due to hardware failure, the Decommissioned Disk cannot be erased, it is securely stored until it can be destroyed. Each facility is audited regularly to monitor compliance with the Disk Erase Policy.

4. Personnel Security

Google personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. Google conducts reasonably appropriate background checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, Google's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer Data are required to complete additional requirements appropriate to their role (e.g. certifications). Google's personnel will not process Customer Data without authorization.

5. Subprocessor Security

Before onboarding Subprocessors, Google conducts an audit of the security and privacy practices of Subprocessors to ensure Subprocessors provide a level of security and privacy appropriate to their access to data and the scope of the services they are engaged to provide. Once Google has assessed the risks presented by the Subprocessor, then subject to the requirements described in Section 11.3 (Requirements for Subprocessor Engagement) of this Addendum, the Subprocessor is required to enter into appropriate security, confidentiality and privacy contract terms.

Previous versions of Data Processing and Security Terms:

June 30, 2022 (/terms/data-processing-addendum/index-20220630) *September 24, 2021* (/terms/data-processing-terms/index-20210924) *August 19, 2020* (/terms/data-processing-terms/index-20200819)

Google Cloud

Additional Product Terms

From time to time, Google may make available one or more Google product(s) and/or service(s) referred to as 'Additional Products' or 'Additional Services' in Customer's Google Workspace Agreement, Cloud Identity Agreement or Hire Agreement (as applicable, the "**Agreement**"). For the purposes of these Additional Product Terms, such product(s) and/or service(s) will be collectively referred to as "**Additional Products**".

If Customer or any End User uses any Additional Products, Customer agrees to these Additional Product Terms, which will be incorporated into the applicable Agreement. If Customer or any End User uses any such Additional Products, Customer also agrees that the separate terms of service applicable to such products will apply as described below. For clarity, such terms of service will each form a separate agreement and are not governed by, or incorporated into, the applicable Agreement.

If Customer does not wish to enable any Additional Products, or if you are acting on behalf of Customer but do not have the requisite authority to bind Customer to these Additional Product Terms, please disable such Additional Products via the functionality of the Services.

1. **Definitions**. All capitalized terms used in these Additional Product Terms have the meanings given to them in the applicable Agreement, unless otherwise defined or stated herein.
2. **Applicable Terms of Service**. The Additional Products will be governed by (a) these Additional Product Terms, and (b) the Google Terms of Service located at https://policies.google.com/terms or any other terms of service Google may make available (as applicable, the "**Terms of Service**"). Customer will be responsible under these Additional Product Terms for any failure by its End Users to comply with such Terms of Service. Further details of the Additional Products and Terms of Service are provided at http://www.google.com/support/a/bin/answer.py?hl=en&answer=181865 and/or will be otherwise made available by Google. The Additional Products and Terms of Service may be updated or modified by Google from time to time.
3. **Availability**. Additional Products may not be available in all countries.
4. **Technical Support**. Customer is responsible for responding to questions from End Users relating to Customer's or End Users' use of the Additional Products. Google only provides technical support services for the Additional Products to the extent described in the applicable Terms of Service, and will not provide other technical support for the Additional Products unless Google agrees otherwise in writing.
5. **Compliance with Laws**. Customer agrees that it will provide Additional Products to its End Users in compliance with all applicable laws and regulations, including privacy and data protection laws, the US Family Educational Rights and Privacy Act (FERPA) of 1974, the US Children's Internet Protection Act (CIPA), and the US Children's Online Privacy Protection Act (COPPA) of 1998.
6. **Customer Access to End User Data**. Customer may be able to access, monitor, delete, rectify, export, use or disclose data provided by and related to End Users in the context of Additional Products or to disable End User Accounts for Additional Products. To the extent Customer has any such abilities, Customer will provide End Users with relevant information and facilitate the exercise of any related rights of End Users under

privacy or data protection laws. If Google receives any request from an End User pertaining to Customer's processing of his/her personal data in relation to any Additional Products, Google will advise the End User to submit his/her request to Customer, and Customer will be responsible for responding to the request.

7. **End User Consent**. Except in relation to End Users described in Section 8 (Parental Consent), Customer will, before it allows any End Users to access or use any Additional Products, obtain and maintain consents from those End Users to the collection and use of their personal information in connection with those Additional Products.
8. **Parental Consent**. Before Customer allows any End Users who are under the age of 16 (or such other minimum age as is specified in the relevant European Economic Area member state, the UK or Switzerland) and resident in the European Economic Area, the UK or Switzerland, or any other End Users under the age of 18, to access or use any Additional Products, Customer will obtain parental consent for the collection and use of personal data in connection with those Additional Products.
9. **Google Pay**. A Google Pay account opened by an End User is the End User's personal account and is subject to extensive regulatory requirements and prohibitions. While Customer may suspend an End User's access to his/her Google Pay account, Customer may not use an End User's Google Pay account or make any changes to the information in such Google Pay account. Customer may access information in an End User's Google Pay account only in accordance with Google Pay privacy policies and Customer's privacy policy.
10. **Refund for Paid Services**. If Customer disables an Additional Product for which Customer or an End User has provided payment, Google will not be obliged to refund any fees paid by Customer and/or the End User for unused paid services. Customer will indemnify Google from and against all liabilities, damages, losses, expenses and costs (including settlement costs and reasonable legal fees) arising out of End User claims concerning refunds for such paid services.
11. **Severability**. If any part of these Additional Product Terms is found to be unenforceable, the remainder of the Additional Product Terms will remain in full force and effect.
12. **Modifications**. Google may modify these Additional Product Terms from time to time.
13. **Interpretation of Conflicting Terms**. To the extent of any conflict or inconsistency between these Additional Product Terms and the remainder of the applicable Agreement, the remainder of the Agreement will prevail.

Back to Google Cloud Terms Directory (https://cloud.google.com/product-terms) > Current

Google Cloud Platform Acceptable Use Policy

Use of the Services is subject to this Acceptable Use Policy.

Capitalized terms have the meaning stated in the applicable agreement between Customer and Google.

Customer agrees not to, and not to allow third parties to use the Services:

- to violate, or encourage the violation of, the legal rights of others;
- to engage in, promote or encourage illegal activity, including child sexual exploitation, child abuse, or terrorism or violence that can cause death, serious harm, or injury to individuals or groups of individuals;
- for any unlawful, invasive, infringing, defamatory or fraudulent purpose including Non-consensual Explicit Imagery (NCEI), violating intellectual property rights of others, phishing, or creating a pyramid scheme;
- to distribute viruses, worms, Trojan horses, corrupted files, hoaxes, or other items of a destructive or deceptive nature;
- to gain unauthorized access to, disrupt, or impair the use of the Services, or the equipment used to provide the Services, by customers, authorized resellers, or other authorized users;
- to disable, interfere with or circumvent any aspect of the Services, Software, or the equipment used to provide the Services;
- to generate, distribute, publish or facilitate unsolicited mass email, promotions, advertisements, or other solicitations ("spam"); or

- to use the Services, or any interfaces provided with the Services, to access any other Google product or service in a manner that violates the terms of service of such other Google product or service.

PREVIOUS VERSIONS *(Last modified February 6, 2023)*

December 16, 2015 _(/terms/aup-20151216) September 18, 2012 (/terms/aup-20120918)

Back to Google Cloud Terms Directory (https://cloud.google.com/product-terms) > Current

Google Cloud Platform Services Summary

The complete list of services that form Google Cloud Platform is shown below. While Google offers many other services and APIs, only the services below are covered by the Google Cloud Platform terms of service, service level agreements (if applicable), and support offerings. Offerings identified below as Software or Premium Software are not Services under the Google Cloud Platform Terms of Service and the Cloud Data Processing Addendum.

> Services marked in *asterisks* are not available for resale under the Google Cloud Partner Advantage program, unless specifically authorized in writing by Google.

Compute

App Engine: App Engine enables you to build and host applications on the same systems that power Google applications. App Engine offers fast development and deployment; simple administration, with no need to worry about hardware, patches or backups; and effortless scalability.

Batch: Batch is a fully-managed service that allows you to create batch jobs at scale. The service dynamically provisions certain Google Cloud resources, schedules your batch job on the resources, manages the queue for the job, and executes the job. Batch is natively integrated with Google Cloud services for storage, logging, monitoring, and more.

Compute Engine: Compute Engine offers scalable and flexible virtual machine computing capabilities in the cloud, with options to utilize certain CPUs, GPUs, or Cloud TPUs. You can use Compute Engine to solve large-scale processing and analytic problems on Google's computing, storage, and networking infrastructure.

Google Cloud VMware Engine (GCVE): GCVE is a managed VMware-as-a-Service that is specifically designed for running VMware workloads on Google Cloud Platform. GCVE enables customers to run VMware virtual machines natively in a dedicated, private, software-defined data center.

Storage

Cloud Storage: Cloud Storage is a RESTful service for storing and accessing your data on Google's infrastructure. The service combines the performance and scalability of Google's cloud with advanced security and sharing capabilities.

Persistent Disk: Persistent Disk is a durable and high performance block storage service for Google Cloud Platform. Persistent Disk provides SSD and HDD storage that can be attached to instances running in either Compute Engine or Google Kubernetes Engine.

Cloud Filestore: Cloud Filestore is a scalable and highly available shared file service fully-managed by Google. Cloud Filestore provides persistent storage ideal for shared workloads. It is best suited for enterprise applications requiring persistent, durable, shared storage which is accessed by NFS or requires a POSIX compliant file system.

***Cloud Storage for Firebase**: Cloud Storage for Firebase adds customizable Google security (via Firebase Security Rules for Cloud Storage) to file uploads and downloads for your Firebase apps, as well as robust uploads and downloads regardless of network quality through the Firebase SDK. Cloud Storage for Firebase is backed by Cloud Storage, a service for storing and accessing your data on Google's infrastructure.

Databases

AlloyDB: AlloyDB is a fully-managed, PostgreSQL-compatible database for demanding transactional and analytical workloads. It is designed to provide enterprise-grade performance and availability while maintaining compatibility with open-source PostgreSQL.

Cloud Bigtable: Cloud Bigtable is a fast, fully-managed, highly-scalable NoSQL database service. It is designed for the collection and retention of data from 1TB to hundreds of PB.

Datastore: Datastore is a fully-managed, schemaless, non-relational datastore. It provides a rich set of query capabilities, supports atomic transactions, and automatically scales up and down in response to load. It can scale to support an application with 1,000 users or 10 million users with no code changes.

Firestore: Firestore is a NoSQL document database for storing, syncing, and querying data for mobile and web apps. Its client libraries provide live synchronization and offline support, while its security features and integrations with Firebase and Google Cloud Platform accelerate building serverless apps.

Memorystore: Memorystore, which includes Memorystore for Redis and Memorystore for Memcached, provides a fully-managed in-memory data store service that allows customers to deploy distributed caches that provide sub-millisecond data access.

Cloud Spanner: Cloud Spanner is a fully-managed, mission-critical relational database service. It is designed to provide a scalable online transaction processing (OLTP) database with high availability and strong consistency at global scale.

Cloud SQL: Cloud SQL is a web service that allows you to create, configure, and use relational databases that live in Google's cloud. It is a fully-managed service that maintains, manages, and administers your databases, allowing you to focus on your applications and services.

Networking

Cloud CDN: Cloud CDN uses Google's globally distributed edge points of presence to cache HTTP(S) load balanced content close to your users.

Cloud DNS: Cloud DNS is a high performance, resilient, global, fully-managed DNS service that provides a RESTful API to publish and manage DNS records for your applications and services.

Cloud IDS (Cloud Intrusion Detection System): Cloud IDS is a managed service that aids in detecting certain malware, spyware, command-and-control attacks, and other network-based threats.

Cloud Interconnect: Cloud Interconnect offers enterprise-grade connections to Google Cloud Platform using Google Services for Dedicated Interconnect, Partner Interconnect and Cloud VPN. This solution allows you to directly connect your on-premises network to your Virtual Private Cloud.

Cloud Load Balancing: Cloud Load Balancing provides scaling, high availability, and traffic management for your internet-facing and private applications.

Cloud NAT (Network Address Translation): Cloud NAT enables instances in a private network to communicate with the internet.

Cloud Router: Cloud Router enables dynamic Border Gateway Protocol (BGP) route updates between your VPC network and your non-Google network.

Cloud VPN: Cloud VPN allows you to connect to your Virtual Private Cloud (VPC) network from your existing network, such as your on-premises network, another VPC network, or another cloud provider's network, through an IPsec connection using (i) Classic VPN, which supports dynamic (BGP) routing or static routing (route-based or policy-based), or (ii) HA (high-availability) VPN, which supports dynamic routing with a simplified redundancy setup, separate failure domains for the gateway interfaces, and a higher service level objective.

Google Cloud Armor: Google Cloud Armor offers a policy framework and rules language for customizing access to internet-facing applications and deploying defenses against denial of service attacks as well as targeted application attacks. Components of Google Cloud Armor include: L3/L4 volumetric DDos Protection, preconfigured web-application firewall (WAF) rules, and custom rules language.

Google Cloud Armor Managed Protection Plus: Google Cloud Armor Managed Protection Plus is a managed application protection service subscription that bundles Google Cloud Armor WAF and DDoS Protection with additional services and capabilities including DDoS response support, DDoS bill protection, and Google Cloud Armor Adaptive Protection, which is Google's machine-learning based solution to protect internet-facing endpoints from network and application-based attacks.

Media CDN: Media CDN is a content delivery network that leverages Google's global edge cache nodes to deliver exceptional caching efficiency and end user experiences.

Network Connectivity Center: Network Connectivity Center is a hub-and-spoke model for network connectivity management in Google Cloud that facilitates connecting a customer's resources to its cloud network.

Network Intelligence Center: Network Intelligence Center is Google Cloud's comprehensive network monitoring, verification, and optimization platform across the Google Cloud, multi-cloud, and on-prem environments.

Network Service Tiers: Network Service Tiers enable you to select different quality networks (tiers) for outbound traffic to the internet: the Standard Tier primarily utilizes third

party transit providers while the Premium Tier leverages Google's private backbone and peering surface for egress.

Service Directory: Service Directory is a managed service that offers customers a single place to publish, discover and connect their services in a consistent way, regardless of their environment. Service Directory supports services in Google Cloud, multi-cloud, and on-prem environments and can scale up to thousands of services and endpoints for a single project.

Spectrum Access System: Spectrum Access System enables you to access the Citizens Broadband Radio Service (CBRS) in the United States, the 3.5 GHz band that is available for shared commercial use. You can use Spectrum Access System to register your CBRS devices, manage your CBRS deployments, and access a non-production test environment (if offered).

Traffic Director: Traffic Director is Google Cloud Platform's traffic management service for open service meshes.

Virtual Private Cloud: Virtual Private Cloud provides a private network topology with IP allocation, routing, and network firewall policies to create a secure environment for your deployments.

Operations

Cloud Debugger: Cloud Debugger connects your application's production data to your source code by inspecting the state of your application at any code location in production without stopping or slowing down your requests.

Cloud Logging: Cloud Logging is a fully-managed service that performs at scale and can ingest application and system log data, as well as custom log data from thousands of VMs and containers. Cloud Logging allows you to analyze and export selected logs to long-term storage in real time. Cloud Logging includes the Error Reporting feature, which analyzes and aggregates the errors in your cloud applications and notifies you when new errors are detected.

Cloud Monitoring: Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Cloud Monitoring collects metrics, events, and metadata from certain Services, hosted uptime probes, application instrumentation, alert management, notifications and a variety of common application components.

Cloud Profiler: Cloud Profiler provides continuous profiling of resource consumption in your production applications, helping you identify and eliminate potential performance issues.

Cloud Trace: Cloud Trace provides latency sampling and reporting for App Engine, including per-URL statistics and latency distributions.

Google Cloud Backup and DR: Google Cloud Backup and DR is a managed backup and disaster recovery service for centralized protection of workloads in Google Cloud.

Developer Tools

Artifact Registry: Artifact Registry is a service for managing container images and packages. It is integrated with Google Cloud tooling and runtimes and comes with support for native artifact protocols. This makes it simple to integrate it with your CI/CD tooling to set up automated pipelines.

Container Registry: Container Registry is a private Docker image storage system on Google Cloud Platform. The registry can be accessed through an HTTPS endpoint, so you can pull images from your machine, whether it's a Compute Engine instance or your own hardware.

Cloud Build: Cloud Build is a service that executes your builds on Google Cloud Platform infrastructure. Cloud Build can import source code from Cloud Storage, Cloud Source Repositories, GitHub, or Bitbucket; execute a build to your specifications; and produce artifacts such as Docker containers or Java archives.

Cloud Source Repositories: Cloud Source Repositories provides Git version control to support collaborative development of any application or service, including those that run on App Engine and Compute Engine.

***Firebase Test Lab**: Firebase Test Lab lets you test your mobile app using your test code or automatically on a wide variety of devices and device configurations hosted in a Google data center, with test results made available in the Firebase console.

Google Cloud Deploy: Google Cloud Deploy is a service for managing and performing application continuous delivery to Google Kubernetes Engine. It allows for process specification and control of application delivery.

Test Lab: Test Lab enables you to test mobile applications using physical and virtual devices in the cloud. It runs instrumentation tests and script-less robotic tests on a matrix of device configurations, and reports detailed results to help improve the quality of your mobile app.

Data Analytics

BigQuery: BigQuery is a fully-managed data analysis service that enables businesses to analyze Big Data. It features highly scalable data storage that accommodates up to hundreds of terabytes, the ability to perform ad hoc queries on multi-terabyte datasets, and the ability to share data insights via the web.

Cloud Composer: Cloud Composer is a managed workflow orchestration service that can be used to author, schedule, and monitor pipelines that span across clouds and on-premises data centers. Cloud Composer allows you to use Apache Airflow without the hassle of creating and managing complex Airflow infrastructure.

Cloud Data Fusion: Cloud Data Fusion is a fully-managed, cloud native, enterprise data integration service for quickly building and managing data pipelines. Cloud Data Fusion provides a graphical interface to help increase time efficiency and reduce complexity and allows business users, developers, and data scientists to easily and reliably build scalable data integration solutions to cleanse, prepare, blend, transfer, and transform data without having to wrestle with infrastructure.

Cloud Life Sciences (formerly Google Genomics): Cloud Life Sciences provides services and tools for managing, processing, and transforming life sciences data.

Data Catalog: Data Catalog is a fully-managed and scalable metadata management service that empowers organizations to quickly discover, manage, and understand their data in Google Cloud. It offers a central data catalog across certain Google Cloud Services that allows organizations to have a unified view of their data assets.

Dataplex: Dataplex is an intelligent data fabric that helps customers unify distributed data and automate management and governance across that data to power analytics at scale.

Dataflow: Dataflow is a fully-managed service for strongly consistent, parallel data-processing pipelines. It provides an SDK for Java with composable primitives for building data-processing pipelines for batch or continuous processing. This service manages the life cycle of Compute Engine resources of the processing pipeline(s). It also provides a monitoring user interface for understanding pipeline health.

Datalab: Datalab is an interactive tool for exploration, transformation, analysis and visualization of your data on Google Cloud Platform. It runs in your cloud project and enables you to write code to use other Big Data and storage services using a rich set of Google-authored and third party libraries.

Dataproc: Dataproc is a fast, easy to use, managed Spark and Hadoop service for distributed data processing. It provides management, integration, and development tools for unlocking the power of rich open source data processing tools. With Dataproc, you can create Spark/Hadoop clusters sized for your workloads precisely when you need them.

Dataproc Metastore: Dataproc Metastore provides a fully-managed metastore service that simplifies technical metadata management and is based on a fully-featured Apache Hive metastore. Dataproc Metastore can be used as a metadata storage service component for data lakes built on open source processing frameworks like Apache Hadoop, Apache Spark, Apache Hive, Presto, and others.

Datastream: Datastream is a serverless change data capture (CDC) and replication service that enables data synchronization across heterogeneous databases, storage systems, and applications with minimal latency.

Google Earth Engine: Google Earth Engine is a platform for global-scale analysis and visualization of geospatial datasets. Google Earth Engine can be used with custom datasets, or with any of the publicly available satellite imagery hosted (and ingested on a regular basis) by Earth Engine Data Catalog.

***Looker Studio**: Looker Studio is a data visualization and business intelligence product. It enables customers to connect to their data stored in other systems, create reports and dashboards using that data, and share them throughout their organization.

- **Looker Studio Pro:** Looker Studio Pro is a paid edition of Looker Studio that adds enterprise governance, team management features, and other features listed at https://cloud.google.com/looker-studio/ (https://cloud.google.com/looker-studio/) or a successor URL. Unlike Looker Studio, Looker Studio Pro is eligible for partner resale.

Pub/Sub: Pub/Sub is designed to provide reliable, many-to-many, asynchronous messaging between applications. Publisher applications can send messages to a "topic" and other applications can subscribe to that topic to receive the messages. By decoupling senders and receivers, Pub/Sub allows developers to communicate between independently written applications.

AI and Machine Learning

AI Building Blocks

AutoML: AutoML is a machine learning product suite that enables developers with limited machine learning expertise to provide their data sets and obtain access to quality trained models produced by Google's transfer learning and Neural Architecture Search (Google's technology for finding, generating, evaluating, and training numerous neural architectures to automatically select a solution for the customer's application):

- **AutoML Natural Language**: AutoML Natural Language enables customers to categorize input text into their own custom defined labels (supervised classification). Users can customize models to their own domain or use case.
- **AutoML Tables**: AutoML Tables enables your entire team of data scientists, analysts, and developers to automatically build and deploy state-of-the-art machine learning models on structured data at increased speed and scale.
- **AutoML Translation**: AutoML Translation is a simple and scalable translation solution that allows businesses and developers with limited machine learning expertise to customize the Google Neural Machine Translation (GNMT) model for their own domain or use-case.
- **AutoML Video**: AutoML Video is a simple and flexible machine learning service that lets businesses and developers easily train custom and scalable video models for their own domain or use cases.
- **AutoML Vision**: AutoML Vision is a simple and flexible machine learning service that lets businesses and developers with limited machine learning expertise train custom and scalable vision models for their own use cases.

Cloud Natural Language API: Cloud Natural Language API provides powerful natural language understanding as an easy to use API. This API enables application developers to answer the following questions: 1) What are the entities referred to in the block of text?; 2) What is the sentiment (positive or negative) for this block of text?; 3) What is the language of this block of text?; and 4) What is the syntax for this block of text (including parts of speech and dependency trees)? Users can call this API by passing in a block of text or by referring to a document in Cloud Storage.

Cloud Translation (including Cloud Translation v2 or any subsequent general availability version/release): Cloud Translation is a RESTful API that automatically translates text from one language to another language (e.g. French to English). You can use the API to programmatically translate text in your webpages or apps.

Cloud Vision: Cloud Vision enables developers to understand the content of an image by encapsulating powerful machine learning models in an easy to use API. It quickly classifies images into thousands of categories (e.g., "sailboat", "lion", "Eiffel Tower"), detects individual objects and faces within images, and finds and reads printed words contained within images. You can build metadata on your image catalog, moderate offensive content, or enable new marketing scenarios through image sentiment analysis. You can also analyze images uploaded in the request and integrate with your image storage on Cloud Storage.

Contact Center AI (CCAI): CCAI is a solution for improving the customer experience in your contact centers using AI. CCAI encompasses Dialogflow Essentials, Dialogflow Customer Experience Edition (CX), Speech-to-Text, and Text-to-Speech, and Speaker ID.

Contact Center AI Insights: Contact Center AI Insights helps customers extract value from their contact center data. It provides a console to explore the data, find relevant information and take action on the data. Customers can run advanced analysis within the platform to extract sentiment, topics and highlight key areas from their data.

Contact Center AI ("CCAI") Platform: CCAI Platform is an AI-driven contact-center-as-a-service (CCaaS) platform built natively on Google Cloud, leveraging Contact Center AI at its core. CCAI Platform is purpose-built to work alongside CRMs, providing organizations with a single source of truth for customer journeys. As a unified contact center platform, CCAI Platform accelerates the organization's ability to leverage and deploy AI-driven contact center functionalities without relying on multiple technology providers. CCAI Platform is a full-stack contact center platform for queuing and routing customer interactions across voice and digital channels. It provides easy routing of customer interactions to the appropriate resource pools, allowing a seamless transition to human agents.

Dialogflow Essentials(ES): Dialogflow is a development suite for voice and text conversational apps including chatbots and voicebots. Dialogflow is cross-platform and can connect to your own apps (on the web, Android, iOS, and IoT) or existing platforms (e.g., Telephony platforms like Genesys, Avaya, Cisco and digital platforms like Actions on Google, Facebook Messenger, Slack). Dialogflow Essentials Edition is a paid enterprise tier of Dialogflow provided under the Google Cloud Platform Terms of Service. (The free tier of

Dialogflow (Dialogflow Trial Edition) is not offered via the Google Cloud Platform Terms of Service and is instead provided under the Dialogflow Trial Edition Terms of Service).

Dialogflow Customer Experience Edition (CX): Dialogflow CX is an advanced development suite for creating conversational AI applications including chatbots and voicebots. It includes a visual bot building platform, collaboration and versioning tools, bot modularization tools, advanced IVR feature support (like DTMF, barge-in, etc.), and is optimized for enterprise scale and complexity. Dialogflow CX is cross-platform and can connect to your own apps (on the web, Android, iOS, and IoT) or existing platforms (e.g., telephony platforms like Genesys, Avaya, Cisco and digital platforms). Dialogflow CX is provided under the Google Cloud Platform Terms of Service.

Document AI: Document AI classifies and extracts structured data from documents to help discover insights and automate business processes.

- ***Human-in-the-Loop AI**: Human-in-the-Loop AI provides a user interface and workflow tools for human verification of data extracted from documents using Document AI.

Document AI Warehouse: Document AI Warehouse is a data management and governance platform that stores, searches, and organizes documents and their extracted and tagged metadata. Document AI Warehouse is highly scalable and fully managed, requiring no customer-deployed infrastructure, and can be integrated with enterprise document workflows, applications, and repositories.

Media Translation API: Media Translation API is a gRPC API that automatically translates audio from one language to another language (e.g., French to English) and supports streaming real time. You can use the API to programmatically translate audio in your apps.

***Speaker ID**: Speaker ID allows customers to enroll user voice prints and later verify users against a previously enrolled voice print.

Speech-to-Text: Speech-to-Text allows developers to convert audio to text by applying powerful neural network models in an easy to use API.

Text-to-Speech: Text-to-Speech synthesizes human-like speech based on input text in a variety of voices and languages.

Timeseries Insights API: Timeseries Insights API is a service that enables large-scale time series forecasting and anomaly detection in real time. The API is designed to scale to

billions of time series and their properties, and within a few seconds of implementation, detect trends, seasonality, and anomalies across the time series.

Vertex AI Vision: Vertex AI Vision is a service that allows you to easily build, deploy, and manage computer vision applications with a fully managed, end-to-end application development environment.

Video Intelligence API: Video Intelligence API makes videos searchable, and discoverable, by extracting metadata with an easy to use REST API. It quickly annotates videos stored in Cloud Storage, and helps you identify key noun entities of your video and when they occur within the video.

Visual Inspection AI: Visual Inspection AI enables developers to train and deploy AI models to automatically detect, classify, and localize abnormalities found in images in order to improve production quality and develop enhanced analytics across multiple industries.

Vertex AI, AI Platform, and Accelerators

AI Platform Data Labeling: AI Platform Data Labeling is a service that helps developers obtain high quality data to train and evaluate their machine learning models. It supports labeling for image, video, text, and audio as well as management of all of your labeled data in one place.

AI Platform Deep Learning Container: AI Platform Deep Learning Container is a Docker image with the most popular AI frameworks. Machine learning developers and data scientists can customize AI Platform Deep Learning Container and use it with AI Workbench (also known as Notebooks), Google Kubernetes Engine (GKE), Vertex AI, Cloud Run, Compute Engine, Kubernetes, and Docker Swarm.

AI Platform Neural Architecture Search (NAS): NAS is a managed service leveraging Google's neural architecture search technology to generate, evaluate, and train numerous model architectures for a customer's application. NAS training services facilitate management of large-scale experiments.

AI Platform Training and Prediction: AI Platform Training and Prediction is a managed service that enables you to easily build and use machine learning models. It provides scalable training and prediction services that work on large scale datasets.

Vertex AI: Vertex AI is a service for managing the entire lifecycle of AI and machine learning development. With Vertex AI, you can (i) manage image, video, text, and tabular

datasets and associated labels; (ii) build machine learning pipelines to train and evaluate models using Google Cloud algorithms or custom training code; (iii) deploy models for online or batch use cases all on scalable managed infrastructure (including additional discovery points and API endpoints for functionality replacing the legacy services of AI Platform Data Labeling, AI Platform Training and Prediction, AI Platform Neutral Architecture Search (NAS), AutoML Natural Language, AutoML Video, AutoML Vision, and AutoML Tables); (iv) manage your entire data science workflow using Vertex AI Workbench (also known as Notebooks), which offers Google and user-managed options for a notebook-based development environment, including JupyterLab instances; and (v) create realistic plans to optimize your business with Optimization AI and related functionality.

Industry Solutions

***Talent Solution**: Talent Solution offers access to Google's machine learning, enabling company career sites, job boards, ATS, staffing agencies, and other recruitment technology platforms to improve the talent acquisition experience.

Discovery Solutions: Discovery Solutions allow customers in retail, media, and other verticals to deliver Google-quality search results and recommendations on their own websites and mobile applications.

- ***Recommendations AI:** Recommendations AI enables you to build an end-to-end personalized recommendation system based on state-of-the-art deep learning ML models, without a need for expertise in ML or recommendation system architecture.
- ***Recommendationengine API:** Recommendationengine API is the Version 1 API of Recommendations AI described above. This API will be deprecated in 2023 and is not accepting new customers.
- ***Retail Search**: Retail Search, powered by Google's Retail API, allows retailers to leverage Google's search capabilities on their own retail websites and mobile applications. With Retail Search, retailers receive fast, accurate, and high quality search results that help improve conversion and increase customer engagement.

API Management

Apigee and Apigee Edge: Apigee and Apigee Edge are full-lifecycle API management platforms that let customers design, secure, analyze, and scale APIs, giving them visibility and control.

- **Apigee:** Apigee is available as Apigee X, a fully-managed service, and as Apigee hybrid, a hybrid model that's partially hosted and managed by the customer.
- **Apigee Edge:** Apigee Edge is available as a fully-managed service and as Apigee Private Cloud, a customer-hosted Premium Software solution.

API Gateway: API Gateway is a fully-managed service that helps you develop, deploy, and secure your APIs running on Google Cloud Platform.

Cloud Endpoints: Cloud Endpoints is a tool that helps you to develop, deploy, secure and monitor your APIs running on Google Cloud Platform.

Payment Gateway: Payment Gateway is a managed service that provides a reliable, scalable and secure way for customers to integrate with real time payment systems like Unified Payments Interface (UPI).

- **Issuer Switch:** Issuer Switch provides customers with a managed deployment of standard payment interfaces for performing payment and non-payment transactions on their users' accounts.

Hybrid and Multi-cloud

Anthos: Anthos is a solution designed for building and managing modern applications running across hybrid cloud environments. Anthos is an integrated platform incorporating cloud-based services and software components, including:

- **Anthos Config Management**: Anthos Config Management is a policy management solution for enabling consistent configuration across multiple Kubernetes clusters. Anthos Config Management allows you to specify one single source of truth and then enforce those policies on your cluster.
- **Anthos Identity Service**: Anthos Identity Service is an authentication service that lets customers bring existing identity solutions for authentication to multiple Anthos environments. Users can log in to and access their Anthos clusters from the command line or from the Google Cloud console, all using their existing identity providers.
- **Anthos Integration with Google Cloud Platform Services**: Google Cloud Platform services and components may be used in connection with Anthos deployments, including Google Kubernetes Engine (GKE), Cloud Logging, Cloud Monitoring, Traffic Director, and Google Cloud Platform Marketplace.

- **Anthos Premium Software**: Anthos includes the software components listed below as Premium Software.
- **Anthos Service Mesh**: Anthos Service Mesh is a managed service mesh service that includes (i) a managed certificate authority that issues cryptographic certificates that identify customer workloads within the Anthos Service Mesh for mutual authentication, and (ii) telemetry for customers to manage and monitor their services. Customers receive details showing an inventory of services, can understand their service dependencies, and receive metrics for monitoring their services. For clarity this service does not include Anthos Service Mesh -- Software (see below regarding Premium Software).
- **Google Kubernetes Engine**: Google Kubernetes Engine, powered by the open source container scheduler Kubernetes, enables you to run containers on Google Cloud Platform. Kubernetes Engine takes care of provisioning and maintaining the underlying virtual machine cluster, scaling your application, and operational logistics such as logging, monitoring, and cluster health management.
- **Connect**: Connect is a service that enables both users and Google-hosted components to interact with clusters through a connection to the in-cluster Connect software agent.
- **Hub**: Hub is centralized control-plane that enables a user to register clusters running in a variety of environments, including Google's cloud, on premises in customer datacenters, or other third party clouds. Hub provides a way for customers to centrally manage features and services on customer-registered clusters.

Cloud Run for Anthos: Cloud Run for Anthos lets you run stateless containers on Anthos.

Google-Managed Multi-Cloud Services

***BigQuery Omni:** BigQuery Omni is a Google-managed multi-cloud analytics solution that enables analysts to access and analyze data stored on other supported public clouds from a singular BigQuery control-plane on GCP.

Bare Metal

Bare Metal Solution: Bare Metal Solution allows you to operate and manage dedicated bare metal hardware (servers and attached storage) in Google's subprocessors' data

centers to run specialized workloads with low latency.

Migration

BigQuery Data Transfer Service: BigQuery Data Transfer Service automates data movement from SaaS applications to BigQuery on a scheduled, managed basis. With the BigQuery Data Transfer Service, you can transfer data to BigQuery from SaaS applications including Google Ads, Campaign Manager, Google Ad Manager, and YouTube.

BigQuery Migration Service: BigQuery Migration Service is a solution for migrating your existing data warehouse to BigQuery. It includes tools, such as batch and interactive SQL translators, that can help with each phase of migration from assessment and planning to execution and verification.

Database Migration Service: Database Migration Service is a fully-managed migration service that makes it simple to perform high fidelity, minimal-downtime migrations at scale. You can use Database Migration Service to migrate from your on-premises environments, Compute Engine, and other clouds to certain Google Cloud-managed databases with minimal downtime.

Google Distributed Cloud Edge Appliance Service: Google Distributed Cloud Edge Appliance Service allows you to run private Google Kubernetes Engine clusters on ruggedized hardware deployed on customer premises. You can use Google Distributed Cloud Edge Appliance Service to offload sensor data for storage, low latency processing, and ML/AI inference in bandwidth-limited locations.

Migration Center: Migration Center enables you to automatically discover your existing infrastructure, analyze the cost benefits of public cloud, and facilitate planning your migration to Google Cloud.

Migrate to Virtual Machines: Migrate to Virtual Machines is a fully-managed migration service that enables you to migrate workloads at scale into Google Cloud Compute Engine with minimal down time by utilizing replication-based migration technology.

Storage Transfer Service: Storage Transfer Service enables you to import large amounts of online data into Cloud Storage, quickly and cost-effectively. With Storage Transfer Service, you can transfer data from locations reachable by the general internet (e.g., HTTP/HTTPS), including Amazon Simple Storage Service (Amazon S3), as well as transfer data between Google Cloud products (e.g., between two Cloud Storage buckets). You can

also use Storage Transfer Service to move data between private data center storage (e.g., NFS) and Google Cloud products (e.g., transfer from NFS to Cloud Storage).

Transfer Appliance: Transfer Appliance is a solution that uses hardware appliances and software to transfer large amounts of data quickly and cost-effectively into Google Cloud Platform.

Security and Identity

Security

Access Transparency: Access Transparency captures near real-time logs of manual, targeted accesses by Google administrators, and serves them to customers via their Cloud Logging account.

Assured Workloads: Assured Workloads provides functionality to create security controls that are enforced on your cloud environment. These security controls can assist with your compliance requirements (for example, FedRAMP Moderate).

Binary Authorization: Binary Authorization helps customers ensure that only signed and explicitly-authorized workload artifacts are deployed to their production environments. It offers tools for customers to formalize and codify secure supply chain policies for their organizations.

Certificate Authority Service: Certificate Authority Service is a cloud-hosted certificate issuance service that lets customers issue and manage certificates for their cloud or on-premises workloads. Certificate Authority Service can be used to create certificate authorities using Cloud KMS keys to issue, revoke, and renew subordinate and end-entity certificates.

Certificate Manager: Certificate Manager provides a central place for customers to control where certificates are used and how to obtain certificates, and to see the state of the certificates.

Cloud Asset Inventory: Cloud Asset Inventory is an inventory of cloud assets with history. It enables users to export cloud resource metadata at a given timestamp or cloud resource metadata history within a time window.

Cloud Data Loss Prevention: Cloud Data Loss Prevention is a fully-managed service designed to help you discover, classify, and protect your most sensitive data. You can

inspect, mask, and de-identify sensitive data like personally identifiable information (PII).

Cloud External Key Manager (Cloud EKM): Cloud EKM lets you encrypt data in Google Cloud Platform with encryption keys that are stored and managed in a third-party key management system deployed outside Google's infrastructure.

Cloud HSM: Cloud HSM (Hardware Security Module) is a cloud-hosted key management service that lets you protect encryption keys and perform cryptographic operations within a managed HSM service. You can generate, use, rotate, and destroy various symmetric and asymmetric keys.

Cloud Key Management Service: Cloud Key Management Service is a cloud-hosted key management service that lets you manage cryptographic keys for your cloud services the same way you do on premises. You can generate, use, rotate, and destroy AES256, RSA 2048, RSA 3072, RSA 4096, EC P256, and EC P384 cryptographic keys.

Event Threat Detection: Event Threat Detection helps detect threats in log data. Threat findings are written to Security Command Center and optionally to Cloud Logging.

Key Access Justifications (KAJ): KAJ provides a justification for every request sent through Cloud EKM for an encryption key that permits data to change state from at-rest to in-use.

Risk Manager: Risk Manager allows customers to scan their cloud environments and generate reports around their compliance with industry-standard security best practices, including CIS benchmarks. Customers then have the ability to share these reports with insurance providers and brokers.

Security Command Center: Security Command Center is Google Cloud's centralized vulnerability and threat reporting service. Security Command Center provides asset inventory and discovery and allows you to identify misconfigurations, vulnerabilities and threats, helping you to mitigate and remediate risks.

VPC Service Controls: VPC Service Controls provide administrators the ability to configure security perimeters around resources of API based cloud services (such as Cloud Storage, BigQuery, Bigtable) and limit access to authorized VPC networks, thereby mitigating data exfiltration risks.

Secret Manager: Secret Manager provides a secure and convenient method for storing API keys, passwords, certificates, and other sensitive data.

Web Security Scanner: Web Security Scanner is a web application security scanner that enables developers to easily check for a subset of common web application vulnerabilities in websites built on App Engine and Compute Engine.

Identity & Access

Access Approval: Access Approval allows customers to approve eligible manual, targeted accesses by Google administrators to their data or workloads before those accesses happen.

Access Context Manager: Access Context Manager allows Google Cloud organization administrators to define fine-grained, attribute based access control for projects, apps and resources.

BeyondCorp Enterprise: BeyondCorp Enterprise is a solution designed to enable zero-trust application access to enterprise users and protect enterprises from data leakage, malware and phishing attacks. BeyondCorp Enterprise is an integrated platform incorporating cloud-based services and software components, including:

- **On-premises Connector**, which forwards Identity-Aware Proxy traffic from Google Cloud Platform to applications and VMs deployed in non-Google Cloud Platform environments.
- **BCE app connector**, which provides secure access to private applications in non-Google cloud environments using a remote agent installed on a customer-owned virtual machine.
- **BCE client connector**, which provides end users secure access to private non-web applications using a remote endpoint agent installed on customer endpoint devices.
- **Endpoint Verification**, which allows administrators to build an inventory of devices and set the security posture of the devices.
- **Threat and Data Protection Services**, which are a set of security services that work by aggregating threat intelligence and are designed to protect enterprise users from malware transfers, phishing, malicious site visits, and sensitive data leakage.
- **BeyondCorp Enterprise Integration with Chrome Browser Cloud Management**, which enables malware, phishing, and data leakage protection for managed Chrome browsers.

- Other features listed at https://cloud.google.com/beyondcorp-enterprise/pricing (https://cloud.google.com/beyondcorp-enterprise/pricing) or a successor URL.

Cloud Identity Services: Cloud Identity Services are the services and editions as described at: https://cloud.google.com/terms/identity/user-features.html (https://cloud.google.com/terms/identity/user-features) or such other URL as Google may provide.

***Firebase Authentication**: Firebase Authentication provides a service as part of the Firebase platform to authenticate and manage users in your applications. It supports authentication using email & password, phone number and popular federated identity providers like Google and Facebook.

Google Cloud Identity-Aware Proxy: Google Cloud Identity-Aware Proxy is a tool that helps control access, based on a user's identity and group membership, to applications running on Google Cloud Platform.

Identity & Access Management (IAM): IAM provides administrators the ability to manage cloud resources centrally by controlling who can take what action on specific resources.

Identity Platform: Identity Platform provides you with functionality and tools to manage your users' identities and access to your applications. Identity Platform supports authentication and management of users with a variety of methods, including email & password, phone number, and popular federated identity providers like Google and Facebook.

Managed Service for Microsoft Active Directory (AD): Managed Service for Microsoft Active Directory is a Google Cloud service running Microsoft AD that enables you to deploy, configure and manage cloud-based AD-dependent workloads and applications. It is a fully-managed service that is highly available, applies network firewall rules, and keeps AD servers updated with Operating System patches.

Resource Manager API: Resource Manager API allows you to programmatically manage Google Cloud Platform container resources (such as Organizations and Projects), that allow you to group and hierarchically organize other Google Cloud Platform resources. This hierarchical organization lets you easily manage common aspects of your resources such as access control and configuration settings.

Google Distributed Cloud

Google Distributed Cloud Edge: Google Distributed Cloud Edge allows you to run private Google Kubernetes Engine clusters on dedicated hardware, which is provided and maintained by Google on Customer premises.This solution also provides you with a VPN connection to Google Cloud Platform, allowing you to interact with other GCP Services or other applications running in your Virtual Private Cloud.

Sovereign Controls by Partners

Sovereign Controls by Partners: Sovereign Controls by Partners are solutions comprising a suite of Services offered by Google that are complemented by a set of services, offered by, and under separate terms of service with, third party partners ("**Sovereign Controls Partners**"), which together create additional security controls for certain Services, while also allowing the relevant Sovereign Controls Partner to provide additional security measures for those Services, as further described at: https://cloud.google.com/terms/in-scope-sovereign-cloud (https://cloud.google.com/terms/in-scope-sovereign-cloud).

User Protection Services

reCAPTCHA Enterprise: reCAPTCHA Enterprise helps detect fraudulent activity on websites.

Web Risk API: Web Risk API is a Google Cloud service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources.

Serverless Computing

Cloud Run: Cloud Run (fully-managed) lets you run stateless containers on a fully-managed environment.

Cloud Functions: Cloud Functions is a lightweight, event-based, asynchronous compute solution that allows you to create small, single-purpose functions that respond to cloud events without the need to manage a server or a runtime environment.

***Cloud Functions for Firebase**: Cloud Functions for Firebase lets you write code that responds to events and invokes functionality exposed by other Firebase features, once you deploy JavaScript code in a hosted, private, and scalable Node.js environment that requires no maintenance.

Cloud Scheduler: Cloud Scheduler is a fully-managed enterprise-grade cron job scheduler. It allows you to schedule virtually any job, including batch, big data jobs, cloud infrastructure operations, and more. You can automate everything, including retries in case of failure to reduce manual toil and intervention. Cloud Scheduler even acts as a single pane of glass, allowing you to manage all your automation tasks from one place.

Cloud Tasks: Cloud Tasks is a fully-managed service that allows you to manage the execution, dispatch, and delivery of a large number of distributed tasks. Using Cloud Tasks, you can perform work asynchronously outside of a user or service-to-service request. Cloud Tasks provides all the benefits of a distributed task queue such as task offloading wherein heavyweight, background and long running processes can be dispatched to a task queue, loose coupling between microservices allowing them to scale independently, and enhanced system reliability as tasks are persisted in storage and retried automatically, making your infrastructure resilient to intermittent failures.

Eventarc: Eventarc is a fully-managed service for eventing on Google Cloud Platform. Eventarc connects various Google Cloud services together, allowing source services (e.g., Cloud Storage) to emit events that are delivered to target services (e.g., Cloud Run or Cloud Functions).

Workflows: Workflows is a fully-managed service for reliably executing sequences of operations across microservices, Google Cloud services, and HTTP-based APIs.

Internet of Things (IoT)

IoT Core: IoT Core is a fully-managed service that allows you to easily and securely connect, manage, and ingest data from internet connected devices. It permits utilization of other Google Cloud services for collecting, processing, analyzing, and visualizing IoT data in real time. IoT Core will be discontinued on August 16, 2023 and is not accepting new customers.

Management Tools

Google Cloud App: Google Cloud app is a native mobile app that enables customers to manage key Google Cloud services. It provides monitoring, alerting, and the ability to take actions on resources.

Cloud Deployment Manager: Cloud Deployment Manager is a hosted configuration tool which allows developers and administrators to provision and manage their infrastructure on

Google Cloud Platform. It uses a declarative model which allows users to define or change the resources necessary to run their applications and will then provision and manage those resources.

Cloud Shell: Cloud Shell is a tool that provides command-line access to cloud resources directly from your browser. You can use Cloud Shell to run experiments, execute Cloud SDK commands, manage projects and resources, and do lightweight software development via the built-in web editor.

Recommenders: Recommenders automatically analyze your usage patterns to provide recommendations and insights across services to help you use Google Cloud Platform in a more secure, cost-effective, and efficient manner.

Service Infrastructure: Service Infrastructure is a foundational platform for creating, managing, securing, and consuming APIs and services. It includes:

- Service Management API, which lets service producers manage their APIs and services;
- Service Consumer Management API, which lets service producers manage their relationships with their service consumers; and
- Service Control API, which lets managed services integrate with Service Infrastructure for admission control and telemetry reporting functionality.
- Service Usage API, which lets service consumers manage their usage of APIs and services.

Healthcare and Life Sciences

Cloud Healthcare: Cloud Healthcare is a fully-managed service to send, receive, store, query, transform, and analyze healthcare and life sciences data and enable advanced insights and operational workflows using highly scalable and compliance-focused infrastructure.

***Healthcare Data Engine (HDE)**: HDE is a solution that enables (1) harmonization of healthcare data to the Fast Healthcare Interoperability Resources ("FHIR") standard and (2) streaming of healthcare data to an analytic environment.

Media and Gaming

Game Servers: Game Servers is a managed service that enables game developers to deploy and manage their dedicated game servers across multiple Agones clusters around the world through a single interface.

Live Stream API: Live Stream API is a cloud-based live encoder that processes high-quality contribution feeds for 24x7 live linear or live events and prepares the streams for digital distribution. It compresses the video and audio elementary streams with the latest video codecs and packages the streams in standardized container formats to reach all IP connected devices.

Transcoder API: Transcoder API can batch convert media files into optimized formats to enable streaming across web, mobile, and living room devices. It provides fast, easy to use, large-scale processing of advanced codecs while utilizing Google's storage, networking, and delivery infrastructure.

Video Stitcher API: Video Stitcher API enables users to dynamically insert content or ads using server-side video insertion technology. Video and ads are conditioned into a single stream for video on demand (VOD) or live streams to deliver flexible and target personalization at scale.

Google Cloud Platform Premium Software

Below is a list of available software components subject to the Google Cloud Platform Service Specific Terms as Premium Software.

Anthos: Anthos includes the following Premium Software components:

- **Anthos core software**: Anthos core software enables you to run containers on Kubernetes and can be deployed on premises in your own data center, as well as in both private and public clouds.
- **Anthos Service Mesh - Software**: Anthos Service Mesh - Software is a suite of tools to run a reliable service mesh on Anthos, to help you monitor, manage and secure traffic between the services deployed on Anthos.
- **Anthos Identity Service - Software**: Anthos Identity Service - Software may be downloaded and installed in supported cluster types and environments to let administrators set up authentication with their preferred Identity providers for one or more Anthos clusters.

- **Connect Software**: Connect Software may be downloaded and installed in clusters to enable connectivity between the customer-registered cluster and Google Cloud.
- **Cloud Logging and Cloud Monitoring for Anthos**: Cloud Logging and Cloud Monitoring can be deployed in a range of hybrid cloud environments to enable centralized log storage, log analysis, metrics capture, metrics trending, customized alerting, and application debug tracing.

***Apigee hybrid runtime**: Apigee hybrid runtime enables you to run the Apigee runtime plane in containers on Kubernetes within your data center.

***Apigee Private Cloud**: Apigee Private Cloud enables you to host and run Apigee entirely within your data center.

Cloud Vision OCR On-Prem: Cloud Vision OCR On-Prem enables you to run Cloud Vision OCR models within your data center and across multiple cloud environments.

Speech On Device: Speech On Device allows customers to deploy speech-to-text (STT) and text-to-speech (TTS) services locally on their custom embedded hardware and operating systems.

Speech-to-Text On-Prem: Speech-to-Text On-Prem enables you to run Cloud Speech-to-Text models within your data center and across multiple cloud environments.

Google Cloud Platform Software

Below is a non-exclusive list of available software components subject to the Google Cloud Platform Service Specific Terms as Software.

- **BigQuery Connector for SAP** replicates, in connection with SAP Landscape Transformation Replication Server, SAP NetWeaver-based application data changes in near real-time and directly into BigQuery.
- **Cloud Run for Anthos deployed on VMware** enables you to run stateless containers on VMware.
- **Config Connector** is a Kubernetes add-on that allows you to manage your Google Cloud resources through Kubernetes configuration files.

- **Google Cloud SDK**: Google Cloud SDK is a set of tools to manage resources and applications hosted on Google Cloud Platform. It includes the Google Cloud Command Line Interface (CLI), Cloud Client Libraries for programmatic access to Google Cloud Platform services, the gsutil, kubectl, and bq command line tools, and various service and data emulators for local platform development. The Google Cloud SDK provides the primary programmatic interfaces to Google Cloud Platform.
- **Kf** enables you to migrate and run applications from the open-source Cloud Foundry platform into containers in Google Kubernetes Engine and Anthos.
- **Migrate to Containers** enables you to migrate and run applications from virtual machines on-premise or other clouds into containers in Google Kubernetes Engine, Anthos, and Cloud Run, while producing container and data artifacts for integration with modern CI/CD, Anthos and Google Cloud services. Migrated container images and artifacts are portable for use across a variety of Google Kubernetes Engine, Anthos, and Cloud Run hybrid configurations as listed in the applicable software documentation. With Migrate to Containers, the need for application rewrite is minimized.
- **Migrate for Compute Engine v4.X** enables you to validate, run, and migrate applications from on-premise or other clouds into Compute Engine while minimizing downtime and application rewrite.

PREVIOUS VERSIONS *(Last modified February 16, 2023)*

December 13, 2022 _ (/terms/services/index-20221213) November 3, 2022 (/terms/services/index-20221103) October 11, 2022 _ (/terms/services/index-20221011) October 3, 2022 _ (/terms/services/index-20221003) September 29, 2022 (/terms/services/index-20220929) August 31, 2022 _ (/terms/services/index-20220831) August 22, 2022 _ (/terms/services/index-20220822) August 16, 2022 (/terms/services/index-20220816) August 1, 2022 _ (/terms/services/index-20220801)

July 13, 2022 _ (/terms/services/index-20220713) June 28, 2022 (/terms/services/index-20220628) June 16, 2022 _ (/terms/services/index-20220616) May 19, 2022 _ (/terms/services/index-20220519) April 25, 2022 (/terms/services/index-20220425) April 12, 2022 _ (/terms/services/index-20220412) April 4, 2022 _ (/terms/services/index-20220404) March 31, 2022 (/terms/services/index-20220331) February 28, 2022 _ (/terms/services/index-20220228) February 2, 2022 _ (/terms/services/index-20220202) January 19, 2022 (/terms/services/index-20220119) December 13, 2021 _ (/terms/services/index-20211213) November 30, 2021 _ (/terms/services/index-20211130) October 18, 2021 (/terms/services/index-20211018) September 30, 2021 _ (/terms/services/index-20210930) September 13, 2021 _ (/terms/services/index-20210913) August 24, 2021 (/terms/services/index-20210824) July 20, 2021 _ (/terms/services-20210720) June 22, 2021 _ (/terms/services-20210622) May 18, 2021 _ (/terms/services-20210518) April 30, 2021 _ (/terms/services-20210430) April 14, 2021 _ (/terms/services-20210414) April 8, 2021 _ (/terms/services-20210408) March 31, 2021 _ (/terms/services-20210331) March 2, 2021 _ (/terms/services-20210302) February 4, 2021 (/terms/services-20210204) January 26, 2021 _ (/terms/services-20210126) January 6, 2021 _ (/terms/services-20210106) November 2, 2020 (/terms/services-20201102) September 15, 2020 _ (/terms/services-20200915) September 1, 2020 _ (/terms/services-20200901) August 19, 2020 (/terms/services-20200819) August 7, 2020 _ (/terms/services-20200807) July 27, 2020

(/terms/services-20200727) July 24, 2020 _ (/terms/services-20200724) July 13, 2020

(/terms/services-20200713) June 30, 2020 _ (/terms/services-20200630) June 9, 2020

(/terms/services-20200609) April 27, 2020 _ (/terms/services-20200427) April 22, 2020

(/terms/services-20200422) April 15, 2020 _ (/terms/services-20200415) April 9, 2020

(/terms/services-20200409) March 31, 2020 _ (/terms/services-20200331)

March 26, 2020 _ (/terms/services-20200326) March 16, 2020

(/terms/services-20200316) March 11, 2020 _ (/terms/services-20200311)

February 25, 2020 _ (/terms/services-20200225) February 3, 2020

(/terms/services-20200203) December 12, 2019 _ (/terms/services-20191212)

December 3, 2019 _ (/terms/services-20191203) November 14, 2019

(/terms/services-20191114) November 4, 2019 _ (/terms/services-20191104)

October 7, 2019 _ (/terms/services-20191007) October 1, 2019

(/terms/services-20191001) August 21, 2019 _ (/terms/services-20190821) June 25, 2019

(/terms/services-20190625) June 17, 2019 _ (/terms/services-20190617) May 31, 2019

(/terms/services-20190531) May 16, 2019 _ (/terms/services-20190516) April 10, 2019

(/terms/services-20190410) April 9, 2019 _ (/terms/services-20190409) March 11, 2019

(/terms/services-20190311) February 1, 2019 _ (/terms/services-20190201)

January 2, 2019 _ (/terms/services-20190102) December 13, 2018

(/terms/services-20181213) December 3, 2018 _ (/terms/services-20181203)

October 7, 2018 _ (/terms/services-20181007) September 18, 2018

(/terms/services-20180918) August 29, 2018 _ (/terms/services-20180829)

August 16, 2018 _ (/terms/services-20180816) August 2, 2018 (/terms/services-20180802) July 31, 2018 _ (/terms/services-20180731) July 24, 2018 (/terms/services-20180724) July 10, 2018 _ (/terms/services-20180710) June 28, 2018 (/terms/services-20180628) May 18, 2018 _ (/terms/services-20180518) May 9, 2018 (/terms/services-20180509) May 8, 2018 _ (/terms/services-20180508) April 13, 2018 (/terms/services-20180413) March 27, 2018 _ (/terms/services-20180327) March 23, 2018 _ (/terms/services-20180323) March 21, 2018 (/terms/services-20180321) February 6, 2018 _ (/terms/services-20180206) January 17, 2018 _ (/terms/services-20180117) November 16, 2017 (/terms/services-20171116) November 13, 2017 _ (/terms/services-20171113) November 9, 2017 _ (/terms/services-20171109) October 3, 2017 (/terms/services-20171003) September 25, 2017 _ (/terms/services-20170925) September 13, 2017 _ (/terms/services-20170913) August 30, 2017 (/terms/services-20170830)

Back to Google Cloud Terms Directory (https://cloud.google.com/product-terms) > Current

Google Cloud Platform Services: Technical Support Services Guidelines

These technical support services guidelines ("Guidelines") are incorporated into the agreement under which Google has agreed to provide Google Cloud Platform to Customer (the "Agreement"). Capitalized terms used but not defined in the Guidelines have the meaning given to them in the Agreement. Google does not provide Technical Support Services ("TSS") for certain Google Cloud Platform Services and some Google Cloud Platform Services and related products are subject to additional or different technical support terms as noted in the General Support Services Terms: Exceptions section.

Collapse all

General Support Services Terms

1. **Generally.** As part of Customer's purchase of Google Cloud Platform Services, Google will provide Basic (formerly Bronze) Support to Customer. Customer may order additional TSS for an additional fee.

2. **Basic Support.** Customer will receive automatic Services upgrades and Maintenance updates, support for billing inquiries, and access to documentation, white papers, online best practices guides, and community forums.

3. **Support Request Submission.**

3.1. *First Line Support*. Customer will provide first-level support to Customer End Users. Google will provide second-level support to Customer's Designated Contacts only.

3.2. *Customer Efforts to Fix Errors*. Prior to making a request to Google, Customer will use reasonable efforts to fix any error, bug, malfunction or network connectivity defect without escalation to Google. Thereafter, Customer may submit a Request for TSS.

3.3. *Characterization of Requests*. Customer designates P1-P4 priority upon submission of Requests. Google will review Customer's priority designation and may reclassify designations (a) that Google believes are incorrect or (b) where Customer fails to maintain continuous availability, as described in Section 3.4 (Procedures for Acknowledgement and Resolution of Requests) through the resolution of a Request. Any such determination made by Google is final and binding on Customer. Any reclassification by Google of the Priority designation pursuant to subsection (b) will be reversed once Customer resumes continuous availability with Google in accordance with Section 3.4 (Procedures for Acknowledgement and Resolution of Requests).

3.4. *Procedures for Acknowledgement and Resolution of Requests*. When making a Request, Customer will provide all requested diagnostic information and assist Google Support Personnel as may be required to resolve a Request. Customer must provide up-to-date contact information (i.e., phone or email) to assist with data gathering, testing and applying resolutions. In the case of P1 Requests, Customer must maintain continuous availability until resolution of such Requests. Upon resolution of a Request, Customer may receive an optional survey to provide feedback to Google on the support Request experience.

3.5. *Request Acknowledgement*. Google may respond to a Request by acknowledging receipt of the Request. Customer acknowledges and understands that Google may be unable to provide answers to, or resolve all Requests.

3.6. *Feature Requests*. If Google deems a Request to be a Feature Request, Google will log such Request for consideration to add to a future update or release of the Services and will consider the matter closed. Google is under no obligation to respond to or resolve any Feature Request or to include any such Feature Request in any future update or release.

3.7. *Building Applications*. Google has no obligation under these Guidelines to: (a) write, build or improve any software Applications, or write code to facilitate Applications; (b) configure the Services for Customer; or (c) design, build or review Customer infrastructure.

3.8. *Pre-General Availability Offerings*. Google has no obligation to provide TSS for Pre-GA Offerings, but will consider Requests relating to Pre-GA Offerings on a case-by-case basis.

4. **Accessing Support.**

4.1. *Setting Designated Contacts*. Customer-designated support admins may add Designated Contacts to its Account. Solely with respect to Silver, Gold, and Platinum TSS, if Customer wishes to change its Designated Contacts, it will notify Google via the Google Support Tool at least five Business Days prior to the change, as applicable.

4.2. *Support Hours and Target Initial Response Times*. Google will process Requests during the Hours of Operation and in accordance with the applicable target initial response times for each support level, unless otherwise indicated in these Guidelines. Any Requests received outside of the Hours of Operation will be logged and processed during the next Business Day.

4.3. *Compliance with Applicable Law*. Google will not provide TSS if prohibited from doing so by applicable law.

5. **Maintenance.** To ensure optimal performance of the Services, Google performs periodic Maintenance. In most cases, Maintenance will have limited or no negative impact on the availability and functionality of the Services. If Google expects planned Maintenance to negatively affect the availability or functionality of the Services, Google will use commercially reasonable efforts to provide at least seven days' advance notice of the Maintenance. In addition, Google may perform emergency unscheduled Maintenance at any time. If Google expects such emergency unscheduled Maintenance to negatively affect the availability or functionality of the Services, Google will use commercially reasonable efforts to provide advance notice of such Maintenance. Maintenance notices noted above will be provided via the Google Support Tool or via an email to the Notification Email Address.

6. **Language Support.** All support provided by Google pursuant to these Guidelines will be provided in the English language except as provided

at https://cloud.google.com/support/docs/language-working-hours (https://cloud.google.com/support/docs/language-working-hours).

7. **Support Data Processing Activities.** Google collects and processes Support Data for the purpose of providing TSS under these Guidelines and maintaining the Services.

8. **Technical Account Management (TAM).** As part of the Platinum, Enterprise and Premium Support offerings, Customer will receive access to a named Technical Account Manager to: (a) assist Customer in developing a strategy with respect to the Services, (b) provide best practice guidance on implementation and use of the Services, and (c) manage technical support escalations and coordinate with Google subject matter experts to address technical inquiries related to the Services. Additional access to Technical Account Management may be purchased, subject to additional fees and terms.

9. **Professional Services.** In addition to the support and maintenance services described above, Google may provide limited advisory services to Customer under these Guidelines in accordance with an order form executed by Google and Customer and datasheets associated with the services. Additional fees may apply. Advisory services are recommendations only. Customer is responsible for the results achieved when determining whether to implement recommendations from Google. Google may deliver recommendations to Customer in the form of a working paper or report, which Customer may use, modify and reproduce for its internal business purposes. Google will not otherwise license any intellectual property to Customer as part of the advisory services provided under these Guidelines. Any other advisory, professional or implementation services will be subject to the terms of a separate agreement between Google and Customer.

10. **Collaborative Support.** In recognition that Customer may deploy and use Services that are offered in connection with or that rely upon a range of third party hardware and software components and computing platforms, resolving Requests may sometimes require input from third party providers who have qualified to participate in the Google Cloud Platform collaborative support program (such providers, "Collaborative Support Partners"). Google will, in its reasonable determination, identify to Customer any Requests that require the involvement of Collaborative Support Partner(s). Google may include Collaborative Support Partners in support communications with Customer, subject to the following terms:

10.1. Customer may only receive support from a Collaborative Support Partner if Customer has a valid support agreement in place with that Collaborative Support

Partner. Neither these Guidelines nor the Agreement grant to Customer any right to receive support services from Collaborative Support Partners.

10.2. Google will include Collaborative Support Partners in direct support communications with Customer solely at Customer's direction. Google Support Personnel will only reach out to a Collaborative Support Partner after receiving Customer's consent.

10.3. When Customer consents to include a Collaborative Support Partner in an ongoing support case, Customer consents to Google providing that Collaborative Support Partner with Support Data Google reasonably deems relevant to the Request, including Customer's name, contact information, and a description of the Request. When Customer directs Google to engage a Collaborative Support Partner, the Collaborative Support Partner acts as an independent contractor of the Customer, not Google. The Collaborative Support Partner, not Google, is solely responsible for the processing and use of any information, including Support Data, provided to that Collaborative Support Partner in the course of providing support services.

11. **Resold Customer.** A customer (a "Resold Customer") of a Google-authorized unaffiliated Google Cloud Platform reseller (a "Reseller") may purchase Google-supplied technical support services that are approved and enabled for resale through the Reseller ("Resold TSS"), provided that:

11.1. the prices and fees for Resold TSS, and the terms applicable to Resold Customer's use of Resold TSS, are agreed as between Resold Customer and the Reseller;

11.2. any payment for Resold TSS is made directly to Reseller under Resold Customer's applicable agreement with the Reseller; and

11.3. Google will not provide Resold Customer any billing inquiry support on the Services.

12. **Chrome Support**. If Customer purchases Enhanced or Premium Support then Google Support Personnel will also respond to Requests related to Chrome installation, Chrome Core Functionality, Chrome's security and administrative policies, and Chrome's interoperability with Services on Supported Platforms as set forth in these Guidelines. Google may choose not to respond to Requests for other Chrome related technical issues, such as but not limited to, rendering problems for specific web pages, technical issues related to the underlying operating system, device driver or printer problems. If Google

makes a code change to Chrome to resolve a technical issue, that code change will be released in an upcoming release and will not be ported back to an earlier version of Chrome.

13. **Exceptions.** Regardless of any other statement in the Agreement or these Guidelines, Google does not offer TSS for Looker Studio (except for Looker Studio Pro).

For the following Google Cloud Platform Services, Google offers technical support under separate terms set forth at the corresponding URL:

Service	Technical Support Terms
Cloud Identity	https://cloud.google.com/terms/identity/tssg (/terms/identity/tssg)
Apigee Edge	https://cloud.google.com/terms/apigee-support (/terms/apigee-support)

For the following Google Cloud Platform Services and related products, Google offers TSS under these Guidelines except as provided at the corresponding URL:

Service/Product	Technical Support Terms
Looker Platform Services	https://cloud.google.com/terms/tssg/looker (/terms/tssg/looker)
Firebase	https://cloud.google.com/terms/tssg/firebase (/terms/tssg/firebase)
Apigee	https://cloud.google.com/terms/apigee-support-services-guide (/terms/apigee-support-services-guide)
Google Cloud Backup and DR	https://cloud.google.com/terms/gcbdr-services-guide (/terms/gcbdr-services-guide)

14. **Additional Definitions.**

14.1. *"Application"* has the meaning given in the Agreement or, if not such meaning is given, has the meaning given to "Customer Application" in the Agreement.

14.2. *"Business Day"* means any day during the Hours of Operation.

14.3. *"Chrome"* means the Chrome web browser as released by Google for Supported Platforms and available for download at the URL https://www.google.com/chrome/ (https://www.google.com/chrome/) or the installer provided at the URL https://chromeenterprise.google/browser/ (https://chromeenterprise.google/browser/) or at another URL that Google may provide.

14.4. *"Chrome Core Functionality"* means the features and functionality in the latest released Chrome browser version, excluding Google Chrome extensions, and Google Play.

14.5. *"Customer End User"* has the meaning given in the Agreement or, if no such meaning is given, has the meaning given to "End Users" in the Agreement.

14.6. *"Designated Contacts"* means administrators or technical employees designated by Customer or Reseller (if Customer is accessing TSS as a customer of a Reseller) who are allowed to contact Google for technical support.

14.7. *"Feature Request"* means a Request by a Designated Contact to incorporate a new feature or enhance an existing feature of the Services that is currently not available as part of the existing Services.

14.8. *"Google Support Tool"* means the Admin Console or a support tool located at a URL (as may be updated from time to time) provided by Google.

14.9. *"Google Support Personnel"* means the Google representatives responsible for handling Requests.

14.10. *"Hours of Operation"* means 17:00 on Sunday to 17:00 on Friday Pacific Time Zone, except for holidays in local time for each region documented in the Google Support Tool.

14.11. *"Maintenance"* means maintenance work that is performed on hardware or software delivering the Services.

14.12. *"Notification Email Address"* has the meaning given in the Cloud Data Processing Addendum.

14.13. *"P0"* means impact to operating environments that have been provisioned to support Mission Critical Services.

14.14. *"P1"* means Critical Impact – Service Unusable in Production.

14.15. *"P2"* means High Impact – Service Use Severely Impaired.

14.16. *"P3"* means Medium Impact – Service Use Partially Impaired.

14.17. "P4" means Low Impact – Service Fully Usable.

14.18. *"Priority"* means P0, P1, P2, P3 or P4 depending on the level of impact a Request is having on Customer's operations and is used to establish initial target response times.

14.19. *"Request"* means a request from a Designated Contact to Google Support Personnel for technical support to resolve a question or problem report regarding the Services, Chrome, or Chrome Core Functionality, as applicable.

14.20. *"Reseller"* has the meaning given to it in Section 11 (Resold Customer) in the General Support Service Terms of these Guidelines.

14.21. *"Support Data"* means account details and the information that Customer provides to Google for the purpose of obtaining TSS under these Guidelines, including requests for support and the details provided to Google about the specific support issue.

14.22. *"Support Role"* means the level of support available to a Designated Contact under Role-Based Support, as defined by one of two tiers (Development or Production) and as designated by Customer in accordance with Section 1 (Support Roles) of the Role-Based Support terms.

14.23. *"Supported Platform"* means an operating system and version listed at https://support.google.com/a/bin/answer.py?answer=2763059 (https://support.google.com/a/bin/answer.py?answer=2763059) for which Chrome is released by Google. Google may choose not to respond to issues with preview versions of Chrome (also known as beta, dev, and canary) or preview features. Chrome OS is not a Supported Platform under these Guidelines; dedicated Google technical support and hardware service for Chrome OS is available under a separate agreement. Chrome Frame is a separate product not covered under these Guidelines.

14.24. *"Value Add Services"* means additional TSS available to Customer for an additional fee.

Standard Support

1. **Standard Support.** Standard Support includes unlimited Designated Contacts.

2. **Target Initial Response Times for Standard Support.**

Priority	Target Initial Response Times during the Hours of Operation
P1	N/A
P2	4 hours
P3	8 hours
P4	8 hours

3. **Enrollment and Unenrollment of Standard Support.**

3.1 Standard Support requires a minimum commitment through the end of each calendar month.

3.2 Customer may unenroll from Standard Support through the Google Support Tool, in which case Basic Support will apply after the end of the calendar month. If Customer upgrades from Standard Support, the applicable Fees for the new support level will be calculated from the date of such upgrade.

Enhanced Support

1. **Enhanced Support**

1.1. Enhanced Support includes unlimited Designated Contacts.

1.2. *Value Add Services*. Customer may purchase the following Value Add Services for an additional fee:

1.2.1. *Technical Account Advisor Service (TAAS)*. Customer will receive access to a Technical Account Advisor. TAAS includes: (a) guided support onboarding, (b) guidance on best practices for case handling, (c) management of technical support escalations, (d) reviews of operational and case metrics, and (e) recommendations for training and optimization of the Services.

1.2.2. *Assured Support for Enhanced Support*. Google will provide TSS for Assured Workloads ("Assured Support") in accordance with the Customer-selected Admin Console controls. All Requests for Assured Support by Customer must be submitted via the "create case" option from within the Google Support Tool and include the project name (ID) in the project field, which corresponds to an Assured Workloads project. Google will provide Assured Support in English and Hebrew languages only.

1.2.3. *Planned Event Support (PES)*. If Customer wishes to purchase PES for an event, it must do so no less than 30 days before that event to ensure proper planning. Each event is limited to a maximum of five calendar days. During each event, regardless of Section 2 (Target Initial Response Times for Enhanced Support) below, Google will respond to P1 Requests that are related to the event with a target initial response time of 15 minutes. Customer can purchase PES for up to three events per calendar year.

1.2.4. *Sovereign Controls by Partners Support for Enhanced Support*. If (i) Customer is using Sovereign Controls by Partners; (ii) the Sovereign Controls Partner does not provide technical support for Sovereign Controls by Partners; and (iii) Customer has purchased Enhanced Support, then Google will provide TSS for the In-scope Google Cloud Controls defined in the Service Specific Terms ("Sovereign Controls by Partners Support") in accordance with the Customer-selected security controls in the Admin Console. All Requests for Sovereign Controls by Partners Support must be submitted via the "create case" option from within the Google Support Tool and include the Project name (ID) in the Project field, which corresponds to a Sovereign Controls by Partners Project with the relevant Sovereign Controls Partner. Google will provide Sovereign Controls by Partners Support in the English language only.

2. **Target Initial Response Times for Enhanced Support.**

Priority	Target Initial Response Times
P1	**1 hour**
P2	**4 hours**
P3	**8 hours***
P4	**8 hours***

*during the Hours of Operation

3. **Enrollment and Unenrollment of Enhanced Support.**

3.1. Enhanced Support requires a minimum commitment through the end of each calendar month or as described in the applicable Order Form.

3.2. Customer may unenroll from Enhanced Support by notifying Google in writing or through the Google Support Tool, as applicable, in which case Basic Support will apply after the end of the applicable commitment period. If Customer enrolls in another support level other than Basic Support, the applicable Fees for the new support level will be calculated from the date of such new enrollment.

Premium Support, Partner-Led Premium Support, and Tech Partner Premium Support

1. **Premium Support.**

1.1. Premium Support includes unlimited Designated Contacts.

1.2. Premium Support includes support from Google's Technical Account Management, as described in Section 8 of the General Support Services Terms (Technical Account Management).

1.3. *Value Add Services*. Customer may purchase the following Value Add Services for Premium Support for an additional fee:

1.3.1. *Assured Support for Premium Support*. Google will provide TSS for Assured Workloads ("Assured Support") in accordance with the Customer-selected Admin Console controls. All Requests for Assured Support by Customer must be submitted via the "create case" option from within the Google Support Tool and include the project name (ID) in the project field, which corresponds to an Assured Workloads project. Google will provide Assured Support in English and Hebrew languages only.

1.3.2. *Mission Critical Services (MCS)*. Google will provide a target initial response time of 5 minutes for P0 cases for operating environments that have been provisioned to support MCS, as noted in the table in Section 3 (Target Initial Response Times for Premium Support and Partner-Led Premium Support). Google will provide TSS for MCS in the English language only.

1.3.3. *Sovereign Controls by Partners Support for Premium Support*. If (i) Customer is using Sovereign Controls by Partners; (ii) the Sovereign Controls Partner does not provide technical support for Sovereign Controls by Partners; and (iii) Customer has purchased Premium Support, then Google will provide TSS for the In-scope Google Cloud Controls defined in the Service Specific Terms ("Sovereign Controls by Partners Support") in accordance with the Customer-selected security controls in the Admin Console. All Requests for Sovereign Controls by Partners Support by Customer must be submitted via the "create case" option from within the Google Support Tool and include the Project name (ID) in the Project field, which corresponds to a Sovereign Controls by Partners Project with the relevant Sovereign Controls Partner. Google will provide Sovereign Controls by Partners Support in the English language only.

2. **Partner-Led Premium Support and Tech Partner Premium Support.**

2.1. Partner-Led Premium Support and Tech Partner Premium Support includes unlimited Designated Contacts.

2.2. *Partner Operations Management (POM)*. As part of the Partner-Led Premium Support and Tech Partner Premium Support offerings, Customer will receive access to a named Partner Operations Manager. POM includes: (a) assistance in developing a cloud strategy with respect to the Services, (b) best practices guidance on

implementing and using the Services, and (c) management of technical support escalations and coordination with Google subject matter experts to address technical inquiries related to the Services.

3. **Target Initial Response Times for Premium Support, Partner-Led Premium Support and Tech Partner Premium Support.**

Priority	Target Initial Response Times
P0	5 minutes (Premium Support with MCS only)
P1	15 minutes
P2	2 hours
P3	4 hours*
P4	8 hours*

*during the Hours of Operation

4. **On-Site Support for Premium Support and Partner-Led Premium Support.** Google may, at its discretion and with Customer's approval, send Google Support Personnel on-site in response to an issue that cannot be resolved remotely. Google Support Personnel performing support at Customer's facilities will comply with Customer's reasonable onsite policies and procedures made known to Google in writing in advance.

5. **Enrollment and Unenrollment of Premium Support, Partner-Led Premium Support and Tech Partner Premium Support.**

5.1. Premium Support, Partner-Led Premium Support and Tech Partner Premium Support requires a minimum 1-year Fee commitment from the date on which Customer enrolls.

5.2. Customer may unenroll from Premium Support, Partner-Led Premium Support or Tech Partner Premium Support at any time by notifying Google in writing and any such unenrollment will take effect, and applicable Fees for Customer's downgraded support level will be calculated at the downgraded amount, from the later of (a) the

date of such unenrollment, and (b) the Business Day following the 1-year anniversary of Customer's enrollment in Premium Support, Partner-Led Premium Support, or Tech Partner Premium Support. Unenrollment from Premium Support automatically unenrolls all Value Add Services.

5.3. Sections 5.1 and 5.2 above will not apply if Customer is an existing Platinum or Enterprise Support customer. Instead, the minimum term of Customer's current Platinum or Enterprise Support Order Form will govern its use of Premium Support, Partner-Led Premium Support, or Tech Partner Premium Support until the expiration of such Order Form.

[Legacy] Silver, Gold and Platinum Support

1. **Silver.** The Silver support level includes all the items in Basic Support plus the ability to submit support Requests for questions about Services functionality, best practice guidance on how to architect with the Services, and Services errors reports, as well as up to two Designated Contacts.

2. **Gold.** The Gold support level includes all the items in the Silver level plus consultation on application development, and specific guidance on how to architect with the Services for Customer's proposed use case, as well as up to five Designated Contacts.

3. **Platinum.** The Platinum support level includes all the items in the Gold level plus Unlimited Designated Contacts and access to Google's Technical Account Management team as described in the General Support Service Terms Section 8 (Technical Account Management).

4. **Target Initial Response Times for Silver, Gold and Platinum Support.**

Priority	Target Initial Response Times		
	Silver	Gold	Platinum
P1	4 hours*	1 hours	15 minutes

Priority		Target Initial Response Times	
P2	8 hours*	4 hours*	4 hours*
P3	8 hours*	8 hours*	8 hours*
P4	8 hours*	8 hours*	8 hours*

*during the Hours of Operation

5. **Priority Designations.** Notwithstanding Section 3.3 (Characterization of Requests) of the General Support Services Terms of these Guidelines, Google will inform Customer of any change of Customer's Priority designation in its response to the support Request. Customer may appeal any such reclassification to Google's Support management for review through any available support channel.

[Legacy] Role-Based Support

1. **Support Roles.** Google will provide Customer with technical support through its Designated Contacts, according to their designated Support Role as follows:

1.1. *Development*. The Development Support Role includes all the items in Basic Support plus the ability to submit Requests related to Services functionality, best practices guidance on how to architect with the Services, and Services errors reports.

1.2. *Production*. The Production Support Role includes all the items in the Development Support Role plus limited guidance on how to architect with the Services for Customer's proposed use case.

2. **Target Initial Response Times for Role-Based Support.**

Priority	Target Initial Response Times	
	Development	Production
P1	N/A	1 hour
P2	4 hours*	4 hours*
P3	8 hours*	8 hours*
P4	8 hours*	8 hours*

*during the Hours of Operation

3. **Upgrading/Downgrading Support Roles in Role-Based Support.** All Support Roles require a minimum 30-day Fee commitment.

3.1. *Upgrades*. Customer may designate or upgrade a Support Role for a Designated Contact at any time. When Customer designates or upgrades any Support Role for a Designated Contact, any applicable Fees will be pro-rated in that month, and will automatically renew at the beginning of the following month. Customer may upgrade a Support Role for a Designated Contact at any time. Any applicable Fees for such upgraded Support Role will be calculated at the upgraded rate beginning on the day that the upgrade is processed.

3.2. *Downgrades*. Customer may downgrade or remove a Support Role for a Designated Contact at any time. Such downgrade or removal will take effect, and any applicable Fees for such downgraded or removed Support Role will be calculated at the downgraded amount, from the later of (a) the date of such downgrade or removal, and (b) 30 days after the Support Role for the Designated Contact was last changed, and the applicable Fees will automatically renew at the beginning of the month following such downgrade or removal.

[Legacy] Enterprise Support

1. **Enterprise Support.**

1.1. The Enterprise Support offering includes unlimited Designated Contacts, each with Customer's chosen Support Role. The "Business Critical" level of support is only available to Customers who have enrolled in Enterprise Support.

1.2. If enrolled in the Enterprise Support program, Customer may assign the "Business Critical" role to each of its unlimited Designated Contacts.

2. **Target Initial Response Times for Enterprise Support.**

Priority	Target Initial Response Times during the Hours of Operation
P1	15 minutes 24x7
P2	4 hours 24x7
P3	8 hours
P4	8 hours

3. The Enterprise Support offering includes support from Google's Technical Account Management, as described in Section 8 of the General Support Services Terms (Technical Account Management).

4. **On-Site Support.** Google may, at its discretion and with Customer's approval, send Google Support Personnel on-site in response to an issue that cannot be resolved remotely. Google Support Personnel performing support at Customer's facilities will comply with Customer's reasonable onsite policies and procedures made known to Google in writing in advance.

5. **Enrollment and Unenrollment.**

5.1. The Enterprise Support program requires a minimum 1-year Fee commitment from the date on which Customer enrolls.

5.2. Customer may unenroll from the Enterprise Support program at any time by notifying Google in writing and any such unenrollment will take effect, and applicable Fees for Customer's downgraded Support Role(s) will be calculated at the downgraded amount, from the later of (a) the date of such unenrollment, and (b) the Business Day following the 1-year anniversary of Customer's enrollment in Enterprise Support.

5.3. Sections 5.1 and 5.2 above will not apply if Customer is an existing Platinum Support customer. Instead of Customer's current Platinum Support Order Form will govern its use of Enterprise Support until the expiration of such Order Form.

PREVIOUS VERSIONS *(Last modified February 16, 2023)*

January 31, 2023 _ (/terms/tssg/index-20230131) November 14, 2022 (/terms/tssg/index-20221114) October 11, 2022 _ (/terms/tssg/index-20221011) October 3, 2022 _ (/terms/tssg/index-20221003) September 20, 2022 (/terms/tssg/index-20220920) September 15, 2022 _ (/terms/tssg/index-20220915) August 1, 2022 _ (/terms/tssg/index-20220801) June 28, 2022 (/terms/tssg/index-20220628) April 28, 2022 _ (/terms/tssg/index-20220428) April 25, 2022 _ (/terms/tssg/index-20220425) March 28, 2022 (/terms/tssg/index-20220328) February 16, 2022 _ (/terms/tssg/index-20220216) February 14, 2022 _ (/terms/tssg/index-20220214) July 29, 2021 (/terms/tssg/index-20210729) May 17, 2021 _ (/terms/tssg/index-20210517) March 8, 2021 _ (/terms/tssg/index-20210308) February 22, 2021 (/terms/tssg/index-20210222) February 2, 2021 _ (/terms/tssg/index-20210202)

January 28, 2021 _ (/terms/tssg/index-20210128) February 13, 2020 (/terms/tssg/index-20200213) December 11, 2019 _ (/terms/tssg/index-20191211) October 1, 2019 _ (/terms/tssg/index-20191001) June 17, 2019 (/terms/tssg/index-20190617) April 18, 2019 _ (/terms/tssg/index-20190418) May 23, 2018 _ (/terms/tssg/index-20180523) March 20, 2018 (/terms/tssg/index-20180320) August 7, 2017 _ (/terms/tssg/index-20170807)

Google Cloud Customer Experience

Implementation Services

Service	SKU	Data Sheet
G Suite Transformation Advisory	GAPPS-PROF-SVC-TSP	Link
G Suite Security Assessment	GAPPS-PROF-SVC-SA	Link
G Suite Change Management Advisory	GAPPS-PROF-SVC-CMAS	Link
G Suite Deployment Advisory	GAPPS-PROF-SVC-PMO	Link
Cloud Discover	CP-PROF-SVC-DISCOVER	Link
Cloud Start: Infrastructure, Data & Analytics, App Development	CP-PROF-SVC-START	Link
Cloud Sprint: Infrastructure	CP-PROF-SVC-SPRINT	Link
Cloud Sprint: SAP	CP-PROF-SVC-SPRINT	Link
Cloud Plan and Foundations: Infrastructure	CP-PROF-SVC-PLAN-INF	Link
Cloud Plan: Data & Analytics	CP-PROF-SVC-PLAN-DA	Link
Cloud Plan: App Development	CP-PROF-SVC-PLAN-APP	Link
Cloud Deploy	ANC-PROF-SVC-PMO	Link
	ANC-PROF-SVC-PWK	Link
	CP-PROF-SVC-CON	See SOW
Cloud Pilot Service	ANC-PROF-SVC-PILOT	Link
Custom AI Solution (AI as a Service)*	D1C1-4F68-8F7B	Link
Partner Success Services (partner only)	ANC-PROF-SVC-PSS	Link

Training/Learning Services

Service	SKU	Data Sheet
ASL Immersive Education: Machine Learning	ASL-PROF-SVC-PHASE1	Link
GCP Certification	CP-CERT-ASC, CP-CERT-PRO, CP-CERT-FUN	Link
GCP Instructor-Led Training	CP-PROF-SVC-TRAIN	Link
GCP On Demand Training	CP-PROF-SVC-OLT	Link
Learning Journey Management	CP-CERT-JNY	Link
Learning Program Management Service	CP-LEARNING-SVC-LPM	Link
Qwiklabs Credits	CP-PROF-SVC-LABS	Link
Qwiklabs Subscription	CP-PROF-SVC-OLL	Link

Stored Value

Prepaid Training & Implementation Services	CP-PROF-SVC-CREDITS	Link
Prepaid Learning Services	CP-LEARNING-SVC-PLS.	Link
Learning Funds	CP-LEARNING-SVC-LF	Link

The availability of services and the service descriptions in the corresponding data sheets are subject to change without notice.

Last updated: February 20, 2023

Google Cloud

Additional Product Terms

From time to time, Google may make available one or more Google product(s) and/or service(s) referred to as 'Additional Products' or 'Additional Services' in Customer's Google Workspace Agreement, Cloud Identity Agreement or Hire Agreement (as applicable, the "**Agreement**"). For the purposes of these Additional Product Terms, such product(s) and/or service(s) will be collectively referred to as "**Additional Products**".

If Customer or any End User uses any Additional Products, Customer agrees to these Additional Product Terms, which will be incorporated into the applicable Agreement. If Customer or any End User uses any such Additional Products, Customer also agrees that the separate terms of service applicable to such products will apply as described below. For clarity, such terms of service will each form a separate agreement and are not governed by, or incorporated into, the applicable Agreement.

If Customer does not wish to enable any Additional Products, or if you are acting on behalf of Customer but do not have the requisite authority to bind Customer to these Additional Product Terms, please disable such Additional Products via the functionality of the Services.

1. **Definitions**. All capitalized terms used in these Additional Product Terms have the meanings given to them in the applicable Agreement, unless otherwise defined or stated herein.
2. **Applicable Terms of Service**. The Additional Products will be governed by (a) these Additional Product Terms, and (b) the Google Terms of Service located at https://policies.google.com/terms or any other terms of service Google may make available (as applicable, the "**Terms of Service**"). Customer will be responsible under these Additional Product Terms for any failure by its End Users to comply with such Terms of Service. Further details of the Additional Products and Terms of Service are provided at http://www.google.com/support/a/bin/answer.py?hl=en&answer=181865 and/or will be otherwise made available by Google. The Additional Products and Terms of Service may be updated or modified by Google from time to time.
3. **Availability**. Additional Products may not be available in all countries.
4. **Technical Support**. Customer is responsible for responding to questions from End Users relating to Customer's or End Users' use of the Additional Products. Google only provides technical support services for the Additional Products to the extent described in the applicable Terms of Service, and will not provide other technical support for the Additional Products unless Google agrees otherwise in writing.
5. **Compliance with Laws**. Customer agrees that it will provide Additional Products to its End Users in compliance with all applicable laws and regulations, including privacy and data protection laws, the US Family Educational Rights and Privacy Act (FERPA) of 1974, the US Children's Internet Protection Act (CIPA), and the US Children's Online Privacy Protection Act (COPPA) of 1998.
6. **Customer Access to End User Data**. Customer may be able to access, monitor, delete, rectify, export, use or disclose data provided by and related to End Users in the context of Additional Products or to disable End User Accounts for Additional Products. To the extent Customer has any such abilities, Customer will provide End Users with relevant information and facilitate the exercise of any related rights of End Users under

privacy or data protection laws. If Google receives any request from an End User pertaining to Customer's processing of his/her personal data in relation to any Additional Products, Google will advise the End User to submit his/her request to Customer, and Customer will be responsible for responding to the request.

7. **End User Consent**. Except in relation to End Users described in Section 8 (Parental Consent), Customer will, before it allows any End Users to access or use any Additional Products, obtain and maintain consents from those End Users to the collection and use of their personal information in connection with those Additional Products.
8. **Parental Consent**. Before Customer allows any End Users who are under the age of 16 (or such other minimum age as is specified in the relevant European Economic Area member state, the UK or Switzerland) and resident in the European Economic Area, the UK or Switzerland, or any other End Users under the age of 18, to access or use any Additional Products, Customer will obtain parental consent for the collection and use of personal data in connection with those Additional Products.
9. **Google Pay**. A Google Pay account opened by an End User is the End User's personal account and is subject to extensive regulatory requirements and prohibitions. While Customer may suspend an End User's access to his/her Google Pay account, Customer may not use an End User's Google Pay account or make any changes to the information in such Google Pay account. Customer may access information in an End User's Google Pay account only in accordance with Google Pay privacy policies and Customer's privacy policy.
10. **Refund for Paid Services**. If Customer disables an Additional Product for which Customer or an End User has provided payment, Google will not be obliged to refund any fees paid by Customer and/or the End User for unused paid services. Customer will indemnify Google from and against all liabilities, damages, losses, expenses and costs (including settlement costs and reasonable legal fees) arising out of End User claims concerning refunds for such paid services.
11. **Severability**. If any part of these Additional Product Terms is found to be unenforceable, the remainder of the Additional Product Terms will remain in full force and effect.
12. **Modifications**. Google may modify these Additional Product Terms from time to time.
13. **Interpretation of Conflicting Terms**. To the extent of any conflict or inconsistency between these Additional Product Terms and the remainder of the applicable Agreement, the remainder of the Agreement will prevail.

Back to Google Cloud Terms Directory (/product-terms) > Current

Google's Looker Platform Service Level Agreement (SLA) for Looker Hosted Deployments

During the Term of the agreement under which Google has agreed to provide the Covered Services to Customer (as applicable, the "Agreement"), the Covered Services will be Available to Customer as described below (the "Service Level Objective" or "SLO"). Capitalized terms used in this SLA, but not defined in this SLA, have the meanings given to them in the Agreement.

Looker Platform: Each Looker Platform will include a Service Level Objective as follows:

Looker Platform	Monthly Uptime Percentage the Covered Service will be Available (SLO)
Standard	>= 99.5%
Advanced or Elite	>= 99.9%

- **SLO Exclusions**. The SLO does not apply to any of the following: (a) Customer's environment or use of the Covered Services not consistent with the Documentation or as described in the Agreement, (b) Maintenance performed, including update/upgrade releases for the Services, (c) any unavailability caused by circumstances or events outside Google's reasonable control, including any force majeure event, internet access, Customer's or any third party's actions or inactions, equipment, software, or other technology, (d) Instances provisioned for development, staging or other non-production usage, or (e) a Suspension or remedial action described in the Agreement.
- **Availability**. In the event the Covered Services do not meet the applicable SLO, and if Customer meets its obligations under this SLA, Customer will be eligible to receive a

Service Credit. This SLA states Customer's sole and exclusive remedy for any failure by Google to meet the applicable SLO.

- **Service Credit Calculation**. The Service Credit is calculated as a percentage of Customer's Monthly Fee. Service Credits will apply only against future payments due from Customer. A Service Credit awarded in any calendar month shall not, under any circumstances, exceed the Monthly Fee paid by Customer.
- **Service Credit Request Requirement**. Customer must provide all reasonable details regarding the claim, including but not limited to, a detailed description of the incident, the duration of the incident, the number of affected End Users, and any attempts made by Customer to resolve the incident. Customer must submit a request by completing the form at the following link: https://support.google.com/cloud/contact/looker_sla (https://support.google.com/cloud/contact/looker_sla) by the end of the month following the month in which the incident occurred. If Customer is past due with respect to any payment or in default with respect to any material contractual obligations to Google, then Customer is not eligible for any Service Credit under this SLA. Google shall review and grant requests for Services Credits by using Google's system logs and other records, which shall be considered definitive.

SLA Definitions

- "Available" means that the Covered Services can be accessed by End Users.
- "Covered Services" means Looker Hosted Deployment Services.
- "End User Fee" means the average number of End Users subscribed on the affected Instance during the month in which the Covered Services did not meet the applicable SLO multiplied by the monthly per End User fee, as specified in the applicable Order Form.
- "Maintenance" means maintenance work that is performed on hardware or software delivering the Services.
- "Monthly Fee" means the Platform Fee plus the End User Fee.
- "Platform Fee" means the total Platform fee, as specified in the applicable Order Form, paid by Customer for the affected Instance divided by the total number of months in the Term.

- "Service Credit" means the following for each of the respective Looker Platforms:

Standard Platform

Monthly Uptime Percentage Standard Platform	Service Credit Percentage
99.0% <= 99.5%	10%
< 99%	25%

Advanced or Elite Platform

Monthly Uptime Percentage Advanced or Elite	Service Credit Percentage
99.0% <= 99.9%	10%
< 99%	25%

PREVIOUS VERSIONS *(Last modified May 5, 2022)*

April 1, 2021 _ (/terms/looker/legal/customers/sla/sla-20210401) June 1, 2020 (/terms/looker/legal/customers/sla/sla-20200601) March 9, 2020 (/terms/looker/legal/customers/sla/sla-20200309)

Back to Google Cloud Terms Directory (/product-terms) > Current

Looker Service Specific Terms

These Looker Service Specific Terms are incorporated into the agreement under which Google has agreed to provide the Looker platform to Customer or Customer's Affiliate for Internal Business Purposes or External Business Purposes ("Agreement"). Capitalized terms used but not defined in these Looker Service Specific Terms have the meaning stated in the Agreement.

1. Beta Feature Offering Terms

Google may make available features or functionality for Customer to try at no additional cost, and which are designated as "Beta", "Trial", "Non-Production" or other similar designation (collectively, the "Beta Features"). While Beta Features are not Services, Customer's use of Beta Features is subject to the terms of the Agreement applicable to Services, as amended by this "Beta Feature Offering Terms" section.

A. **Test Applications**. Customer may opt into being a test user of one or more Beta Features via permissions granted by Customer via the Looker Services ("Test Application(s)"). If Google accepts Customer as a test user of any Beta Feature (based on Google's then-current domain level requirements for test users), Google will make those Beta Features available for use by Customer subject to the terms of this "Beta Feature Offering Terms" Section. Additional terms ("Specific Test Terms") may apply to that Beta Feature and, if applicable, will be provided by Google via the Test Application or otherwise in writing before any use of the Beta Feature by Customer. The Test Application and any Specific Test Terms are incorporated into this Beta Feature Offering Terms Section.

B. **Use of Customer Test Data**. Google may, and Customer will (including by collecting or providing any required consents or notices) ensure that Google may use any Customer Data (including Customer Personal Data) submitted, stored, sent or received via any Beta Feature by Customer or its End Users ("Customer Test Data") to provide, test, analyze, develop and improve those Beta Features and any Google products and services used with

them without any restriction or obligation to Customer, any End User or any third party, other than as stated in the Agreement's confidentiality provisions and below.

C. **Application of the Data Processing Addendum.** If Customer has accepted, or the parties have otherwise agreed, to Google's then-current terms describing data protection and processing obligations with respect to Customer Data at https://cloud.google.com/terms/looker/dpst (/terms/looker/dpst) (the "Data Processing Addendum"), it will apply to Beta Features as "Services" for purposes of the Data Processing Addendum. Unless stated otherwise in the applicable Beta Features, the entirety of this "Beta Features" section will form part of the "Agreement" referred to in Section 5.2.1 (Customer's Instructions) of the DPST, subject to the following amendments:

i. Unless stated otherwise in the Test Application or Specific Test Terms, information about Subprocessors (as defined in the Data Processing Addendum) will be made available in writing by Google upon Customer's request;

ii. For the duration of Customer's use of any Beta Features, Google will inform Customer of the engagement of any new third-party Subprocessor in relation to the Beta Features by sending an email to the Notification Email Address before the new Subprocessor starts processing any Customer Test Data;

iii. Customer may, as its sole and exclusive remedy if Customer objects to the Subprocessor, cease using the applicable Beta Feature;

iv. Beta Features are not "Audited Services" under the Data Processing Addendum.

v. Customer acknowledges that, for purposes of Section 6.1 (Deletion by Customer) of the Data Processing Addendum and to the extent permitted by applicable law, the functionality of the Beta Features may not allow deletion of Customer Test Data during the period during which Customer is permitted to use the Beta Feature ("Beta Feature Term"), but that Customer Test Data will be deleted upon expiration of the Beta Feature Term in accordance with Section 6.2 (Return or Deletion When Term Ends) of the Data Processing Addendum;

D. **Use Restrictions.** Customer will not, and will not allow End Users to: (i) use Beta Features to process protected health information as defined in the Health Insurance Portability and Accountability Act of 1996, or (ii) use Beta Features to process data subject to legal or regulatory compliance requirements.

E. **Disclaimer.** Beta Features made available by Google are provided to Customer for testing purposes only, and Google does not make any commitment to provide Beta Features in any future versions of the Services. Customer is not required to use Beta Features. Customer may disable Beta Features at its sole discretion. Google may immediately and without notice remove Beta Features for any reason without liability to Customer. Notwithstanding anything to the contrary in the Agreement, Google does not provide TSS for Beta Features. All Beta Features are provided "AS IS" without warranty of any kind.

F. **Feedback**. Customer may provide feedback and suggestions about the Beta Features to Google, and Google and its Affiliates may use any feedback or suggestions provided without restriction and without obligation to Customer.

2. Third-Party Offerings

Looker Marketplace. The Looker Marketplace includes software and services that are not owned by Google in which case Customer's use of such software or services will be governed by a separate agreement between Customer and the third party provider. Customer may need to accept third party terms and conditions before accessing or downloading such software or services via the Looker Marketplace. Customer acknowledges and agrees that Google is not responsible for, and makes no representations or warranties regarding the installation, integration, interoperability, functionality or content of any third party software or services provided via the Looker Marketplace.

3. Third-Party Terms

The Oracle JDBC software components used in conjunction with the Services are subject to the terms and conditions stated at https://cloud.google.com/terms/looker/legal/customers/service-terms/oracle (/terms/looker/legal/customers/service-terms/oracle).

PREVIOUS VERSIONS *(Last modified January 4, 2023)*

February 14, 2022 | _ (/terms/looker/legal/customers/service-terms/index-20220214)

Back to Google Cloud Terms Directory (/product-terms) > Current

Looker Technical Support Services Guidelines

These Looker Technical Support Services Guidelines ("Looker Guidelines") are incorporated into the agreement under which Google has agreed to provide the Looker platform and related technical support to Customer (the "Agreement"). Capitalized terms used but not defined in these Looker Guidelines have the meaning given to them in the Agreement.

Regardless of any other statement in the Agreement or these Looker Guidelines, if Customer has purchased or purchases Google Cloud's Standard, Enhanced or Premium Support services for Customer's Google Cloud Platform services, these Looker Guidelines will not apply to Google's provision of technical support for the Looker Services. Instead, Google will provide technical support for the Looker Services in accordance with the Looker Support Services Guide (available at https://cloud.google.com/terms/tssg/looker (https://cloud.google.com/terms/tssg/looker)).

1. OVERVIEW

The Looker TSS provides technical assistance for the Services, access to the Documentation and update/upgrade releases for the Services. Unless otherwise noted in the Order Form, Google shall provide TSS (as specified below) during the Term. Capitalized terms used but not defined herein have the meaning given to them in the Agreement.

2. SUPPORT TERMS

A. Technical Assistance. The Looker TSS' staff shall provide technical assistance to support the administration of the Services to the Customer's Authorized Contacts in accordance with the terms below. Customer agrees that only Authorized Contacts will contact Google

for TSS and that Customer, and not Google, shall be responsible for providing front-line support to Customer's End Users. TSS does not include Professional Services.

B. Support Availability. The Looker TSS staff is available to provide in-app chat support to an Authorized Contact in accordance with the terms below. Eligibility for chat support requires an active User license for the Looker Software and will only be provided to an Authorized Contact.

C. Maintenance. To ensure optimal performance of the Services, Google performs periodic Maintenance. In most cases, Maintenance will have limited or no negative impact on the availability and functionality of the Services. If Google expects planned Maintenance to negatively affect the availability or functionality of the Services, Google will use commercially reasonable efforts to provide advance notice of the Maintenance. In addition, Google may perform emergency unscheduled Maintenance at any time. If Google expects such emergency unscheduled Maintenance to negatively affect the availability or functionality of the Services, Google will use commercially reasonable efforts to provide advance notice of such Maintenance. Maintenance notices noted above will be provided via an email to the Notification Email Address.

D. Language of Support. Unless specific arrangements are made in writing in advance, all Customer Support will be provided in English.

E. Scope of Support. Google is not obligated to provide TSS if: (a) the Services have not been used in a manner consistent with the Documentation; (b) Customer has disabled connectivity required for TSS; (c) the Services have been altered or modified by any party other than Google; (d) an upgrade, update or patch that Google has recommended and made available has not been installed due to Customer's actions or instructions; or (e) Google is not able, after commercially reasonable efforts, to replicate an error or problem in the Services within the Looker TSS laboratory environment. Google does not provide support for third-party software or hardware.

3. ISSUE REPORTING

A. Issue Severity Definitions:

- S1 - Critical: Complete loss of application functionality causing a critical impact on business operations.
- S2 - Urgent: The Services are operative but degraded causing a significant impact on business operation.

- S3 - Tolerable: The Services are usable, non-critical functionality or components are affected, most operations are unaffected.
- S4 - Question: Includes general questions, requests for documentation, or other non-critical system related issues. Operations are not affected.

B. Reclassification. Google may reclassify the priority level upward or downward and modify the order, classifications and method of responding to and/or addressing such issues, if any, at any time.

C. Priority Response Time. Google will use commercially reasonable efforts to respond within the Response Time set forth below in accordance with: (a) the specific priority level assigned by Google, and (b) the Support Services Plan purchased by Customer.

Google's response consists of either: (a) Google remediation of the support issue, or (b) confirmation that Google has received the support issue reported and indication of active remediation efforts.

Support Services:

Issue Severity Level	Response Time (Business Hours/Off Hours)	Update Frequency (Business Hours/Off Hours)
S1	1 hour/2 hours	8 hours/12 hours
S2	4 hours/6 hours	12 hours/Next Business Day
S3 & S4	8 hours	On Request

4. SERVICES UPDATES

A. New Releases. During the Term, Google will notify Customer of new releases for the Services if and when they are made available. Releases may include version updates, feature releases, and patches.

B. End of Life Policy. Google provides active support to the most recent minor release (e.g. 6.4), the previous two minor releases (e.g. 6.2, 6.0) and the most recent Extended Support Release. Beyond these releases, we consider versions End-of-Life (EOL) as designated by the Officially Supported Releases at https://docs.looker.com/relnotes/supported-releases (https://docs.looker.com/relnotes/supported-releases)

5. TERMS OF SUPPORT SERVICES PLAN

Support Services include the following:

- Access to 24/7 email case submission
- Access to 24/7 Customer community forum
- Customer may request voice or chat support via email for S1 and S2 issues to "urgent at looker dot com"
- Access to in-app Chat during Business Hours and Business Days only
- 1 hour response for Severity 1 issues during Business Hours
- 2 hour response for Severity 1 issues during Off Hours
- Unlimited number of support cases
- Unlimited number of Authorized Contacts

TSS Definitions

- "Authorized Contact" means an individual who has either of the following: (i) completed training (including implementation training) or (ii) certified partner status including implementation training.
- "Business Days" means Monday through Friday, excluding US, UK and Japan local holidays.
- "Business Hours" means between 17:00 on Sunday to 17:00 on Friday Pacific Time Zone.
- "Looker Services" has the same meaning as "Services" as defined in the Agreement.
- "Maintenance" means maintenance work that is performed on hardware or software delivering the Services.

PREVIOUS VERSIONS *(Last modified August 8, 2022)*

April 1, 2021 _ (/terms/looker/support/index-20210401) October 30, 2020 (/terms/looker/support/support-20201030) June 1, 2020 (/terms/looker/support/support-20200601) March 9, 2020 (/terms/looker/support/support-20200309) December 31, 2019 (/terms/looker/support/support-201912)

Back to Google Cloud Terms Directory (/product-terms) > Current

Looker Notices & Acknowledgements

Looker Marketplace

The Looker Marketplace includes software, content, components, packages or other items not authored by or on behalf of Looker ("Third Party Packages"), which are each subject to their own terms and conditions.

You acknowledge and agree that:

1. Looker is not responsible for, and makes no representations or warranties regarding, the installation, integration, interoperability, functionality or content of any Third Party Package.
2. You may have to accept the terms and conditions of a Third Party Package in order to access it.

Looker mobile application

These Supplemental License Terms (the "Terms") apply to the Looker mobile application (the "Mobile App"). These Terms supplement the terms and conditions contained in the customer or evaluation agreement between your company or other legal entity ("Company") and Looker Data Sciences, Inc. ("Looker")(the "Agreement"). By downloading and/or using the Mobile App, you agree to be bound by these Terms. Further you represent and warrant that you are authorized to bind Company to the Terms. Company, and by extension you, constitute "you" for purposes of these Terms.

Apple App Store Requirements. (a) The Agreement is between you and Looker only, and not with Apple, Inc. ("Apple"), and Apple has no liability for the Mobile App; (b) your use of the Mobile App is limited to Apple-branded products that you own or control and as permitted by the Usage Rules set forth in the App Store Terms of Service; (c) Apple has no obligation to furnish any maintenance and support services with respect to the Mobile App; (d) in the event of any failure of the Mobile App to conform to any applicable warranty, (i)

you may notify Apple, and Apple will refund the purchased price you paid through the App Store for the Mobile App, and (ii) to the maximum extent permitted by applicable law, Apple will have no other warranty obligation with respect to the Mobile App; (e) Apple is not responsible for addressing any claims of yours or any third party relating to the Mobile App, including, but not limited to (i) product liability claims; (ii) any claim that the Mobile App fails to conform to any applicable legal or regulatory requirement and (iii) consumer protection or similar claims; (f) Apple is not responsible for the investigation, defense, settlement and discharge of any third party claim that the Mobile App or your possession and use of the Mobile App infringes such third party's intellectual property right; (g) you represent and warrant that (i) you are not located in a country that is subject to a U.S. Government embargo, or that has been designated by the U.S. Government as a "terrorist supporting" country and (ii) you are not listed on any U.S. Government list of prohibited or restricted parties; (h) if you have any questions concerning these Terms, please write to Looker at Looker Data Sciences, 1600 Amphitheatre Parkway, Mountain View, CA 94043; (i) you are responsible for complying with any applicable third party terms of agreement when using the Mobile App; and (j) Apple and its subsidiaries are third party beneficiaries of the Agreement; as a third party beneficiary, Apple will have the right to enforce the Agreement against you.

Oracle JDBC Driver

These Supplemental License Terms (the "Terms") apply to the Oracle JDBC Driver. These Terms supplement the terms and conditions contained in the customer or evaluation agreement between your company or other legal entity ("Company") and Looker Data Sciences, Inc. ("Looker")(the "Agreement"). By downloading and/or using the Oracle JDBC Driver, you agree to be bound by these Terms. Further you represent and warrant that you are authorized to bind Company to the Terms. Company, and by extension you, constitute "you" or "You" for purposes of these Terms.

License Rights and Restrictions

Oracle grants You a nonexclusive, nontransferable, limited license to, subject to the restrictions stated in these Terms, internally use the Oracle JDBC Driver solely for the purposes of developing, testing, prototyping and demonstrating Your applications, and running the Oracle JDBC Driver for Your own internal business operations. You may allow Your contractor(s) to use the Oracle JDBC Driver, provided they are acting on Your behalf to exercise license rights granted in these Terms and further provided that You are responsible for their compliance with these Terms in such use. You will have a written

agreement with Your contractor(s) that strictly limits their right to use the Oracle JDBC Driver and that otherwise protects Oracle's intellectual property rights to the same extent as these Terms. You may make copies of the Oracle JDBC Driver to the extent reasonably necessary to exercise the license rights granted in these Terms. You may make one copy of the Oracle JDBC Driver for backup purposes.

Further, You may not:

- remove or modify any Oracle JDBC Driver markings or any notice of Oracle's or a licensor's proprietary rights;
- use the Oracle JDBC Driver to provide third party training unless Oracle expressly authorizes such use on the Oracle JDBC Driver's download page;
- assign these Terms or distribute, give, or transfer the Oracle JDBC Driver or an interest in them to any third party, except as expressly permitted in these Terms (the foregoing shall not be construed to limit the rights You may otherwise have with respect to Separately Licensed Third Party Technology) ("Separately Licensed Third Party Technology" refers to third party technology that is licensed under separate terms and not under these Terms);
- cause or permit reverse engineering (unless required by law for interoperability), disassembly or decompilation of the Oracle JDBC Driver; and
- disclose results of any Oracle JDBC Driver benchmark tests without Oracle's prior consent.

The Oracle JDBC Driver may contain source code that, unless expressly licensed in these Terms for other purposes (for example, licensed under an open source license), is provided solely for reference purposes pursuant to the terms of these Terms and may not be modified.

All rights not expressly granted in these Terms are reserved by Oracle. If You want to use the Oracle JDBC Driver or Your application for any purpose other than as expressly permitted under these Terms, You must obtain from Oracle or an Oracle reseller a valid Oracle JDBC Driver license under a separate agreement permitting such use. However, You acknowledge that the Oracle JDBC Driver may not be intended for production use and/or Oracle may not make a version of the Oracle JDBC Driver available for production or other purposes; any development or other work You undertake with the Oracle JDBC Driver is at Your sole risk.

Ownership

Oracle or its licensors retain all ownership and intellectual property rights to the Oracle JDBC Driver.

Export Controls

Export laws and regulations of the United States and any other relevant local export laws and regulations apply to the Oracle JDBC Driver. You agree that such export control laws govern Your use of the Oracle JDBC Driver (including technical data) and any services deliverables provided under this agreement, and You agree to comply with all such export laws and regulations (including "deemed export" and "deemed re-export" regulations). You agree that no data, information, program and/or materials resulting from Programs or services (or direct products thereof) will be exported, directly or indirectly, in violation of these laws, or will be used for any purpose prohibited by these laws including, without limitation, nuclear, chemical, or biological weapons proliferation, or development of missile technology. Accordingly, You confirm:

- You will not download, provide, make available or otherwise export or re-export the Oracle JDBC Driver, directly or indirectly, to countries prohibited by applicable laws and regulations nor to citizens, nationals or residents of those countries.
- You are not listed on the United States Department of Treasury lists of Specially Designated Nationals and Blocked Persons, Specially Designated Terrorists, and Specially Designated Narcotic Traffickers, nor are You listed on the United States Department of Commerce Table of Denial Orders.
- You will not download or otherwise export or re-export the Oracle JDBC Driver, directly or indirectly, to persons on the above mentioned lists.
- You will not use the Oracle JDBC Driver for, and will not allow the Oracle JDBC Driver to be used for, any purposes prohibited by applicable law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical or biological weapons of mass destruction.

Disclaimer of Warranties; Limitation of Liability

THE ORACLE JDBC DRIVER IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ORACLE FURTHER DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED,

INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NONINFRINGEMENT.

IN NO EVENT WILL ORACLE BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS, REVENUE, DATA OR DATA USE, INCURRED BY YOU OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF ORACLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. ORACLE'S ENTIRE LIABILITY FOR DAMAGES UNDER THIS AGREEMENT SHALL IN NO EVENT EXCEED ONE THOUSAND DOLLARS (U.S. $1,000).

No Technical Support

Unless Oracle support for the Oracle JDBC Driver, if any, is expressly included in a separate, current support agreement between You and Oracle, Oracle's technical support organization will not provide technical support, phone support, or updates to You for the Oracle JDBC Driver provided under these Terms.

Termination

You may terminate these Terms by destroying all copies of the Oracle JDBC Driver. These Terms shall automatically terminate without notice if You fail to comply with any of the Terms, in which case You shall promptly destroy all copies of the Oracle JDBC Driver.

Relationship Between the Parties

Oracle is an independent contractor and You agree that no partnership, joint venture, or agency relationship exists between You and Oracle. You and Oracle each will be responsible for paying our own employees, including employment related taxes and insurance. Nothing in these Terms shall be construed to limit either party's right to independently develop or distribute software that is functionally similar to the other party's products, so long as proprietary information of the other party is not included in such software.

U.S. Government End Users

The Oracle JDBC Driver and/or Oracle JDBC Driver Documentation delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use duplication, disclosure, modification, and adaptation of the Oracle JDBC Driver and/or

Oracle JDBC Driver Documentation shall be subject to the license terms and license restrictions set forth in this Agreement. No other rights are granted to the U.S. Government.

No Right to Distribute

You do not have a right to distribute the Oracle JDBC Driver or Oracle JDBC Driver Documentation.

Third Party Beneficiary

Oracle is a third party beneficiary to the Agreement.