



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Chapter 10

11/11/2019

General Information

[Contact](#) | [Default Values](#) | [Discussion](#) | [Document Information](#) | [Certification Request](#)

Procurement Folder: 1810678

Procurement Types: Central Contract - Fixed And

Wardlaw ID: 0000010588

Legal Name: CARAHSOFT TECHNOLOGY CORP

Also CDA:

Total Price: \$2,699.00

Response Date: 8/31/2005

Response Time: 8.6 s

Responded By User ID: [carghett](#)

First Name: Caitlyn

Last Name: Lewis

Email: schoen@ceatshsfr.com

Phone: 570.327.1050

SO Doc Code: CAFQ

940 Gupta, Bhatia, & Bhatia

DOI: 10.1002/anie.201705117

Published Date: 3/2016

Close Date: 3/7/25

Close Time: 13.00

<p>Status: Closed</p> <p>Solicitation Description: Addendum No. 2 Cybersecurity e-Discovery SaaS (QT25112)</p>	
--	--

Total of Header Attachments: 0

Total of All Attachments: 6



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder: 1619676
Solicitation Description: Addendum No 2 Cybersecurity e-Discovery SAAS (OT25112)
Proc Type: Central Contract - Fixed Amt

Solicitation Closes	Solicitation Response	Version
2025-03-07 13:30	SR 0231 ESR03072500000005381	1

VENDOR
000000195808
CARAHSOFT TECHNOLOGY CORP

Solicitation Number: CRFQ 0231 OOT2500000017
Total Bid: 2600
Response Date: 2025-03-07
Response Time: 08:51:28
Comments:

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor Signature X	FEIN#	DATE
---------------------------	--------------	-------------

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Contract Services: e-Discovery System				2600.00

Comm Code	Manufacturer	Specification	Model #
43231511			

Commodity Line Comments:

Extended Description:

Please see the attached Exhibit A Pricing Page
Please note: Vendor must provide Exhibit A Pricing Page with their submitted bid response. Failure to do so will result in disqualification of your bid.

**EXHIBIT A – Pricing Page
eDiscovery SaaS - (OT25112)**

Section	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
4.1.1	Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	\$ -	\$ -
4.1.2	Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must be rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	\$ 6.50	\$ 650.00
4.1.7	Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	\$ -	\$ -
4.1.7.4	Contract Item #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00	\$ -	\$ -
4.1.7.5	Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00	\$ -	\$ -
4.1.7.7	Contract Item #6: e-Discovery SaaS Project Management	HR	100.00	\$ -	\$ -
4.1.8	Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00	\$ -	\$ -
4.1.7.6	Contract Item #8: Maintenance and Support Year 1	LS	1.00	\$ -	\$ -
4.1.1	Optional Renewal Year 2: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	\$ -	\$ -
4.1.2	Optional Renewal Year 2: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must be rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	\$ 6.50	\$ 650.00
4.1.7	Optional Renewal Year 2:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	\$ -	\$ -
4.1.7.4	Optional Renewal Year 2: #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00	\$ -	\$ -
4.1.7.5	Optional Renewal Year 2: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00	\$ -	\$ -
4.1.7.7	Optional Renewal Year 2: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00	\$ -	\$ -
4.1.8	Optional Renewal Year 2: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00	\$ -	\$ -
4.1.7.6	Optional Renewal Year 2: Contract Item #8: Maintenance and Support Year 1	LS	1.00	\$ -	\$ -
4.1.1	Optional Renewal Year 3: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	\$ -	\$ -
4.1.2	Optional Renewal Year 3: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must be rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	\$ 6.50	\$ 650.00
4.1.7	Optional Renewal Year 3:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	\$ -	\$ -
4.1.7.4	Optional Renewal Year 3; #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00	\$ -	\$ -
4.1.7.5	Optional Renewal Year 3: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00	\$ -	\$ -
4.1.7.7	Optional Renewal Year 3: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00	\$ -	\$ -
4.1.8	Optional Renewal Year 3: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00	\$ -	\$ -
4.1.7.6	Optional Renewal Year 3: Contract Item #8: Maintenance and Support Year 1	LS	1.00	\$ -	\$ -
4.1.1	Optional Renewal Year 4: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00	\$ -	\$ -
4.1.2	Optional Renewal Year 4: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must be rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00	\$ 6.50	\$ 650.00
4.1.7	Optional Renewal Year 4:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00	\$ -	\$ -
4.1.7.4	Optional Renewal Year 4; #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00	\$ -	\$ -
4.1.7.5	Optional Renewal Year 3: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00	\$ -	\$ -
4.1.7.7	Optional Renewal Year 4: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00	\$ -	\$ -
4.1.8	Optional Renewal Year 4: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00	\$ -	\$ -
4.1.7.6	Optional Renewal Year 4: Contract Item #8: Maintenance and Support Year 1	LS	1.00	\$ -	\$ -
Total Cost				\$	2,600.00

Contract will be evaluated on all lines but only awarded on first year. Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years

Jennifer Kanach
Vendor Signature:

3/7/2025
Date:

Note: The above pricing provided by Everlaw is based on the assumption of 10TB of data as noted by the Agency is Addendum 2.

APPENDIX A:

SOFTWARE AS A SERVICE ADDENDUM

Begins on next page.

Version 11-1--19

Software as a Service Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at <https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN>.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means 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.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

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.

Version 11-1--19

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a 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.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction 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 contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

- a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

Version 11-1--19

the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.

- b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.
- c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.
- d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.
- e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.
- f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.
- g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.
- h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.
- i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

Version 11-1--19

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

- a) Incident Response: The service provider 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 defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.
- b) Security Incident Reporting Requirements: The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.
- c) Breach Reporting Requirements: Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

- a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

Version 11-1--19

- b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.
- c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.
- d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations 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.
- e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

Version 11-1--19

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

- a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.
- b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.
- c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction 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 service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

- d) The public jurisdiction 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 the Contract.
- e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. 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 public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

Version 11-1--19

of the contract, including subcontractors, 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 service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction 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.

14. Security:

- a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

Version 11-1--19

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

- b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.
- c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

Version 11-1--19

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider 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.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

- Access and use the service for its business purposes;
- For SaaS, use underlying software as embodied or used in the service; and
- View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

Version 11-1--19

AGREED:

Name of Agency: _____

Signature: _____

Title: _____

Date: _____

Name of Vendor: Everlaw, Inc

Signed by:
Joe Glass Joe Glass
F8BC908180A04EC...

Title: CRO

Date: 2/19/2025

Version 11-1--19

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: _____

Name of Agency: _____

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
Yes ☐
No ☐
2. If yes to #1, does the restricted information include personal data?
Yes ☐
No ☐
3. If yes to #1, does the restricted information include non-public data?
Yes ☐
No ☐
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
Yes ☐
No ☐
5. Provide name and email address for the Department privacy officer:

Name: _____

Email address: _____

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

Name: _____

Email address: _____

Phone Number: _____

Customer Terms of Service

These Customer Terms of Service (the “**Terms**”) and accompanying **Order Form** referencing these Terms (an “Order Form,” and together with these Terms, the “**Agreement**”), constitute a binding agreement Everlaw, Inc., a Delaware corporation (“**Everlaw**”) and the party named as Customer in the Order Form. This Agreement governs Customer’s access to and use of the Service. Please refer to Section 14 (Definitions) for definitions of certain capitalized terms used in these Terms.

1. THE SERVICE.

1. **Subscriptions.** Everlaw and Customer may enter into one or more Order Forms referencing these Terms, under which Customer may purchase a Subscription. During the Term of a Subscription, Everlaw will provide Customer and Authorized Users with non-exclusive access to the Service. Customer and Authorized Users may use the Service solely for Customer’s own internal business purposes.
2. **Technical Support Services.** During the Term of a Subscription, Everlaw will provide TSS to Customer in accordance with the TSS Guidelines.
3. **Professional Services.** Customer may engage Everlaw to provide certain Professional Services. Any Professional Services Everlaw performs are governed by Everlaw’s PSA.
4. **Updates.** Everlaw may update the Service from time to time. If Everlaw changes the Service in a manner that materially reduces functionality, Everlaw will notify Customer by sending an email to the Commercial Contact’s address. For certain significant new features, Everlaw may notify Authorized Users of the new features by posting a notice in the Service.
5. **Unpaid Subscription.** Everlaw may offer Customers an Unpaid Subscription. For Unpaid Subscriptions, Everlaw may, in its sole discretion: (A) terminate any Unpaid Subscription at any time, without liability to the applicable Customer and Authorized Users; (B) exclude and remove Customers and Authorized Users from the Service; (C) delete or suspend Case Materials; or (D) limit Customer’s maximum Storage Usage.
6. **Third Party Services.** Use of any third party services contained within the Service or in combination with the Service is governed by the Service Specific Terms ([here](#)).

7. **No Practice of Law.** Everlaw is not a law firm and does not provide legal advice or engage in the practice of law. Customer acknowledges that it is not relying on Everlaw for legal advice and has not engaged Everlaw or any Everlaw employee as legal counsel.

2. **MANAGING AUTHORIZED USERS.**

1. **Management and Permissions.** Customer, or the applicable Reseller, is responsible for managing the Authorized Users on its account on the Service. Customer, or the applicable Reseller, is solely in control of the individual permissions on Customer's or the applicable Reseller's accounts, Databases, and Projects. Authorized Users may not be able to access the Service from certain countries where Everlaw does not conduct business.
2. **Suspending an Authorized User.** Customer, or the applicable Reseller, must suspend an Authorized User's access to the Service if Customer, the applicable Reseller, or Everlaw reasonably determines that: (A) Authorized User's use of the Service disrupts or creates a security risk to the Service or Everlaw systems; or (B) Authorized User is using the Service in violation of any applicable law or regulation, Section 3 (Acceptable Use), the Terms of Use, or the applicable Agreement. If Everlaw detects any Authorized User's violation or suspected violation of Section 3 (Acceptable Use), the Terms of Use, or the applicable Agreement, Everlaw will use commercially reasonable efforts to notify Customer by sending an email to the Commercial Contact's address. Everlaw reserves the right to suspend or terminate an Authorized User's access to the Service for any of the reasons stated in (A) or (B) above.

3. **ACCEPTABLE USE.**

1. **Authorized Users.** Customer is responsible for all actions by Authorized Users on Customer's account.
2. **Prohibited Uses.** Customer, or the applicable Reseller, will ensure that it and Authorized Users will not: (A) resell or sublicense the Service (except that, if Customer is a lawyer or law firm, it may pass Everlaw's fees onto its clients); (B) modify, adapt, decompile, reverse engineer, or copy the Service; (C) violate the Agreement; or (D) put Everlaw in breach of any applicable law.
3. **Controlled Data.** Except as stated in Section 3.4 below, Customer will not store or manage the following on the Service: (A) classified government data or information; (B) data controlled by U.S. or other applicable export control regulations, including the International Traffic in Arms Regulations (ITAR), the

Export Administration Regulations (EAR), and the regulations governing nuclear data administered by the National Nuclear Security Administration (NNSA); (C) criminal justice information; or (D) data that falls within the definition of “Protected Health Information” under HIPAA.

4. **Exceptions.** Customer may store ITAR, EAR or criminal justice data if there is a mutually signed Order Form that specifically states Customer will store export-controlled such data exclusively on the FedRAMP-authorized version of the Service. Customer may store Protected Health Information on the Service if the parties have executed a HIPAA Business Associate Agreement. As between Everlaw and Customer, Customer is responsible for configuring the relevant version of the Service (in some cases, the FedRAMP-authorized version) to comply with the ITAR, EAR, HIPAA, and other applicable regulations.
5. **Obligations.** Customer, or the applicable Reseller, will ensure that it and Authorized Users: (A) prevent unauthorized use of, or access to the Service; (B) take reasonable care when (i) inviting individuals to use or access the Service and (ii) granting permissions; (C) report all actual or suspected security incidents or vulnerabilities, or violations of this Section 3 to security@everlaw.com; and (D) obtain and maintain all necessary consents before accessing, uploading, processing, and storing Case Materials and other content in the Service.

4. FEES AND BILLING.

1. **Fees.** Customer will pay the fees and will be billed in accordance with the terms in the applicable Order Form and as further described in the Documentation. Customer must pay for the entire purchased Subscription whether or not the Service is used. Payment for invoices is due within 30 days of the date of any invoice.
2. **Taxes.** Customer is solely responsible for payment of any taxes, duties, or the like that apply to the provision or resulting from the use of the Service (except for Everlaw’s employment taxes and taxes based on Everlaw’s net income). If any such taxes are required to be withheld, Customer will pay an amount to Everlaw such that the net amount payable to Everlaw after withholding of taxes will equal the amount that would have been otherwise payable under this Agreement.

3. **Invoice Disputes.** Any invoice disputes must be submitted to billing@everlaw.com before the respective invoice's due date. If an invoice has not been disputed before its due date, then it will be deemed to have been accepted.
4. **Late Charges.** Late payments are subject to interest charges equal to the lesser of 1.5% per month or the maximum amount allowed by law.
5. **Fee Adjustments.** Everlaw may increase or add new fees and charges for any existing Service Customer uses by giving Customer 30 days' written notice before any renewal Term.

5. INTELLECTUAL PROPERTY RIGHTS & RESTRICTIONS.

1. **Case Materials.** Everlaw agrees that it obtains no Intellectual Property Rights in the Case Materials except for the limited license stated in this Agreement. Customer grants Everlaw a worldwide, limited, non-exclusive, royalty-free license to use the Case Materials to provide the Service to Customer and Authorized Users and to support, manage, and improve the Service, subject to (A) the obligations in Section 7 (Confidentiality) and (B) the limits regarding use of Input and Output in Section 8.5 (Everlaw AI Assistant).
2. **Everlaw Intellectual Property.** Everlaw will retain all Intellectual Property Rights in the Service, including all derivatives, changes, and improvements, and Customer agrees that it obtains no Intellectual Property Rights or licenses by this Agreement except those expressly granted.
3. **Feedback.** Customer and Authorized Users may provide Feedback to Everlaw. Everlaw and its Affiliates may use that Feedback without restriction and without obligation to Customer or Authorized Users.
4. **Marketing Rights.** Everlaw may include Customer's name and logo in a list of Everlaw customers, online or in promotional materials. Provided Everlaw receives Customer's approval, Everlaw may (A) work together on an announcement of Customer being an Everlaw customer on a mutually agreed upon date within 6 months of the Signature Date (stated in the applicable Order Form); and (B) engage Customer in other joint marketing such as customer testimonials, social media promotions, public speaking events, and press/analyst interviews. In the event Everlaw permits Customer to use Everlaw's trademarks, Customer agrees to comply with the Trademark Policy.

6. DATA PROTECTION.

1. **Security.** In addition to Customer and Reseller obligations under Section 3 (Acceptable Use), Everlaw will implement reasonable and appropriate measures designed to help secure the Case Materials and Proprietary Information against accidental or unlawful loss, access, use, or disclosure.
2. **DPA.** To the extent Customer's Case Materials are subject to any Applicable Privacy Law (as defined in the DPA) and are processed by Everlaw on Customer's behalf in connection with the Service, Everlaw and Customer, or the applicable Reseller, agree to the terms of the DPA. This Agreement constitutes Customer's instructions to process Personal Data (as defined in the DPA) protected by Applicable Privacy Law. To the extent Case Materials include Personal Data, Everlaw agrees to process, access, use, disclose, store, and transfer such Personal Data in compliance with the DPA.
3. **Privacy Notice.** Personal Information (defined in the Privacy Notice) provided to us by Customer, Reseller, or Authorized Users, including Account Information and Service-Generated Data, will be used and protected as described in the Privacy Notice. Personal data contained in Case Materials will be subject to Section 6.2 (DPA).

7. CONFIDENTIALITY.

1. **Nondisclosure.** The Recipient will only use the Disclosing Party's Proprietary Information to exercise its rights and fulfill its obligations under this Agreement, and will use reasonable care to protect against the disclosure of the Disclosing Party's Proprietary Information. Notwithstanding the foregoing, the Recipient may disclose the Disclosing Party's Proprietary Information: (A) to its employees, consultants, contractors, service providers or advisors who have a need to know and who are bound by obligations of confidentiality and nonuse at least as protective of such information as this Agreement; (B) with the Disclosing Party's written consent; or (C) regardless of any other provision in this Agreement, as necessary to comply with applicable laws and regulations or a court or other legal order, provided the Recipient promptly notifies the Disclosing Party before such disclosure unless legally prohibited to do so. The Recipient will comply with the Disclosing Party's reasonable requests to oppose and narrow the scope of disclosure of its Proprietary Information at Disclosing Party's cost.

2. **Exceptions.** Information is not Proprietary Information if a party can prove the information: (A) is known before receipt from the Disclosing Party, without any obligation of confidentiality; (B) becomes known to the Recipient directly or indirectly from a source other than one having an obligation of confidentiality to the Disclosing Party; (C) becomes publicly known or otherwise publicly available, except through a breach of this Agreement; (D) Recipient has independently developed the information without use of the Disclosing Party's Proprietary Information; or (E) is disclosed with the prior written approval of the Disclosing Party.

8. REPRESENTATIONS AND WARRANTIES.

1. **Mutual Representations and Warranties.** Each party represents and warrants that it has the necessary corporate authority to enter into this Agreement, and this Agreement is a valid and binding obligation enforceable against it.
2. **Customer Representations and Warranties.** Customer represents and warrants that: (A) it and Authorized Users have all necessary rights and authority to upload or make available Case Materials to the Service without violating any export control laws or any third party's proprietary or privacy rights, including Intellectual Property Rights; (B) the Case Materials do not contain any viruses, worms, Trojan horses, or other harmful or destructive code or content; and (C) it will comply with all applicable laws, rules, and regulations, and in accordance with this Agreement.
3. **Everlaw Representations and Warranties.** Everlaw represents and warrants that it will comply with all laws and regulations applicable to its provision of the Service.
4. **DISCLAIMER OF WARRANTIES.** EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, EVERLAW PROVIDES THE SERVICE TO CUSTOMER ON AN "AS-IS" BASIS, "AS AVAILABLE" BASIS, WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR PARTICULAR PURPOSE, WHETHER ALLEGED TO ARISE BY LAW, BY USAGE IN THE TRADE, BY COURSE OF DEALING, OR COURSE OF PERFORMANCE. IN ADDITION, CUSTOMER ACKNOWLEDGES THAT OUTPUT IS GENERATED BY GENERATIVE ARTIFICIAL INTELLIGENCE FUNCTIONALITY, AND EVERLAW MAKES NO WARRANTY OR GUARANTEE AS TO THE ACCURACY, COMPLETENESS OR

RELIABILITY OF THE OUTPUT. EVERLAW DOES NOT WARRANT THAT THE SERVICE WILL BE DELIVERED OR PERFORMED ERROR-FREE OR WITHOUT INTERRUPTION OR THAT CUSTOMER WILL ACHIEVE ANY PARTICULAR BUSINESS RESULTS BY USE OF THE SERVICE.

5. **Everlaw AI Assistant.** Customer is responsible for Customer's use of Everlaw AI Assistant, and will not use Everlaw AI Assistant or any Output in a manner that violates applicable laws or this Agreement. Customer acknowledges that Output is probabilistic and may not be accurate, reliable, or otherwise appropriate for Customer's use. Customer should independently evaluate Output for accuracy and appropriateness for Customer's use case(s), including through human review, and modify Output as necessary before relying on, publishing, or otherwise using Output. Where appropriate, Customer should provide a disclaimer that Output has been created using generative AI, and Customer and its Authorized Users will not misrepresent that Output has been created without the use or assistance of generative artificial intelligence functionalities. Everlaw will not use Input or Output to train or finetune a generative AI model for general use through the Service.

9. INDEMNIFICATION.

1. **Everlaw Indemnities.** Subject to the terms of this Agreement, Everlaw will defend and indemnify Customer and its officers, directors, employees, successors, and permitted assigns, against any Claims, and all damages, costs, liabilities, and expenses (including reasonable attorneys' fees), in each case, that are actually paid or payable to third parties under such Claims, to the extent such Claims allege that the Service infringes any third-party Intellectual Property Right. Everlaw will have no indemnity obligation or other liability under this Section 9 if such Claim arises from: (A) Customer's negligence, breach of the Agreement, or alteration of the Service provided by Everlaw; (B) combination of the Service with any materials, products, or services not provided by Everlaw (including, without limitation, any Case Materials); (C) third-party components, products or services; or (D) Customer's use of Everlaw AI Assistant and (i) the Claim alleges the Output infringes a third party's trademark or related rights, or (ii) the Claim alleges the Output infringes on a third party's Intellectual Property Rights.
2. **Customer Indemnities.** Customer will defend and indemnify Everlaw and its officers, directors, employees, successors, and permitted assigns, against

any Claims, and all damages, costs, liabilities, and expenses (including reasonable attorneys' fees), in each case, that are actually paid or payable to third parties under such Claims, to the extent such Claims arise from: (A) the use or display of any Documents uploaded to, or content created in, the Service, including the Case Materials; (B) any litigation matter in which Customer or Authorized Users are engaged; or (C) Customer's breach of its obligations of its warranties under this Agreement.

3. **Indemnification Procedure.** Each party's obligations under Sections 9.1 (Everlaw Indemnities) and 9.2 (Customer Indemnities) are expressly conditional on the party seeking indemnification providing the indemnifying party with: (A) prompt written notice of each Claim; (B) sole control over the defense and settlement of the indemnified portion of each Claim; and (C) information as may be reasonably requested by the indemnifying party in connection with each Claim. Further, Everlaw will have the right to approve the counsel selected by Customer for defense of any Claim, which approval will not be unreasonably withheld. Customer will not settle any Claim in a manner that does not unconditionally release Everlaw without Everlaw's written consent, not to be unreasonably withheld or delayed.
4. **Remedies.** If Everlaw reasonably believes the Service might infringe a third party's Intellectual Property Rights, then Everlaw may, at its sole option and expense: (A) procure the right for Customer to continue using the Service; (B) modify the Service to make it non-infringing without materially reducing its functionality; or (C) replace the Service with a non-infringing, functionally equivalent alternative. If Everlaw does not believe the remedies in this Section 9.4 are commercially reasonable, then Everlaw may suspend or terminate Customer's use of the Service.
5. **Sole Rights and Obligations.** Without affecting either party's termination rights, this Section 9 states the parties' sole rights and obligations under this Agreement for Intellectual Property Rights-related Claims.

10. LIMITATION OF LIABILITY.

1. **Insurance.** Customer agrees that: (A) Everlaw is not an insurance company; (B) Everlaw's fees for the Service would be substantially higher if Everlaw were to agree to undertake additional obligations and liabilities beyond what Everlaw has expressly undertaken in this Agreement; and (C) Customer should look solely to its insurance or self-insurance programs to the extent

that any losses, costs, judgments, or expenses are not covered by Everlaw's express obligations and liabilities contained in this Agreement.

2. **EXCLUSION OF DAMAGES.** IN NO EVENT WILL EITHER PARTY BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES, LOST PROFITS, LOST REVENUE, LOSS OF USE, LOSS OF DATA, OR COST OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, HOWEVER CAUSED, AND ON ANY THEORY OF LIABILITY.
3. **MAXIMUM AGGREGATE LIABILITY.** EACH PARTY'S MAXIMUM AGGREGATE LIABILITY IN CONNECTION WITH THIS AGREEMENT AND/OR THE SERVICE, WILL NOT EXCEED THE TOTAL AMOUNT OF FEES PAID OR PAYABLE BY CUSTOMER TO EVERLAW DURING THE 12 MONTHS PRECEDING THE DATE THE LIABILITY FIRST ARISES. EVERLAW'S MAXIMUM AGGREGATE LIABILITY WITH RESPECT TO ANY UNPAID SUBSCRIPTION WILL NOT EXCEED \$100.
4. **ACKNOWLEDGEMENT.** THE LIABILITIES LIMITED BY THIS SECTION 10 WILL APPLY TO ALL LIABILITY: (A) REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND STRICT LIABILITY), OR OTHERWISE; (B) EVEN IF A PARTY IS ADVISED IN ADVANCE OF THE POSSIBILITY OF THE DAMAGES IN QUESTION AND EVEN IF SUCH DAMAGES WERE FORESEEABLE; AND (C) EVEN IF THE ESSENTIAL PURPOSE OF A PARTY'S REMEDIES FAIL. IF APPLICABLE LAW LIMITS THE APPLICATION OF THE PROVISIONS OF THIS SECTION 10, EACH PARTY'S LIABILITY WILL BE LIMITED TO THE MAXIMUM EXTENT PERMISSIBLE BY SUCH LAW.

11. GOVERNING LAW; DISPUTE RESOLUTION

1. **Governing Law.** The Agreement is governed by the laws of the State of California, without regard to its conflict of laws principles. If Customer is a state, local, or educational governmental entity, then the Agreement is governed by the laws of Customer's state, excluding its conflict of law principles. The United Nations Convention on Contracts for the International Sales of Goods and the Uniform Computer Information Transactions Act do not apply to the Agreement.
2. **Informal Resolution.** Any Dispute Customer has with Everlaw must be submitted to support@everlaw.com in order to attempt resolution through discussion. Everlaw will negotiate with Customer in good faith in an effort to resolve such Dispute without the necessity of any formal proceeding.

3. **Arbitration.** In the unlikely event that the Dispute cannot be resolved in accordance with Section 11.2 (Informal Resolution) and within 30 business days of Everlaw's first communication with Customer after Customer's written submission to Everlaw under Section 11.2 (Informal Resolution), then the parties must submit the Dispute to binding arbitration as stated in this Section 11.3. Except as stated in Section 11.4 (Exception to Arbitration), the parties agree that the Dispute will be settled by arbitration administered by the American Arbitration Association under its Commercial Arbitration Rules and that judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction. The arbitration will be held in Oakland, California, or any other location both parties agree to in writing. The prevailing party will be entitled to costs and attorneys' fees. Except as may be required by law or as necessary to enforce the respective award in a court of law, neither party, nor the mediator or arbitrator, may disclose the existence, content, or results of any mediation or arbitration without the prior written consent of both parties.
4. **Exception to Arbitration.** Without first engaging in the informal dispute process described in Section 11.2 (Informal Resolution) or by submitting to arbitration under Section 11.3 (Arbitration), either party may bring a lawsuit solely for injunctive relief to stop unauthorized use or abuse of the Service or its infringement of a third-party's Intellectual Property Rights, in the federal or state courts of Alameda County, California, and each party irrevocably submits to the venue and jurisdiction of such applicable courts.
5. **Class Actions.** Customer may only resolve Disputes with Everlaw on an individual basis and will not bring a claim in a class, consolidated, or representative action. Class arbitrations, class actions, private attorney general actions, and consolidation with other arbitrations are prohibited.

12. TERM; TERMINATION.

1. **Term.** These Terms apply if an effective Order Form exists between Customer and Everlaw, or until otherwise terminated.
2. **Automatic Renewal.** Unless a party provides written notice of non-renewal at least 30 days before the end of the then current Term on an applicable Order Form, Order Forms automatically renew for: (A) 12-month periods in the case of annual or multi-year subscriptions; or (B) successive terms of 1 month.

3. **Temporary Suspension.** Everlaw may temporarily suspend Customer's, Reseller's, or Authorized User's access to the Service if Everlaw reasonably determines that: (A) Customer's use of the Service disrupts or creates a security risk to the Service or Everlaw systems; (B) Customer is using the Service in violation of any applicable law or regulation or this Agreement; or (C) Customer fails to pay fees owed to Everlaw in accordance with this Agreement.
4. **Termination for Cause.** Either party may terminate the Agreement if the other party: (A) is in material breach of the Agreement and then fails to cure that breach within 30 days after receipt of written notice; or (B) ceases its business operations or becomes subject to insolvency proceedings and such proceedings are not dismissed within 90 days.
5. **Effect of Termination.** If the Agreement terminates or expires, then all Order Forms terminate or expire. 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 Service will terminate (including access to Case Materials); and (B) Everlaw will send Customer a final invoice (if applicable) for payment obligations under that Order Form.
6. **Survival.** Sections 4 (Fees and Billing), 5 (Intellectual Property Rights & Restrictions), 6 (Data Protection), 7 (Confidentiality), 8 (Representations and Warranties), 9 (Indemnification), 10 (Limitation of Liability), 11 (Governing Law; Dispute Resolution), 12.6 (Survival), and 13 (Miscellaneous) will survive the end of the Agreement.

13. MISCELLANEOUS.

1. **Beta Services.** Everlaw sometimes releases products and features that require testing and evaluation ("Beta Services"). Everlaw designates Beta Services as "alpha," "beta," "early access," or "evaluation" (or with words or phrases with similar meanings) and may not be as reliable as Everlaw's other services. Everlaw makes Beta Services available to collect Feedback, and by using the Beta Services, Customer agrees that Everlaw may contact Customer to collect such Feedback. Beta Services may be subject to additional terms and may be presented at the time Customer is given access to the Beta Services. BETA SERVICES ARE PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR REPRESENTATIONS OF ANY KIND. Everlaw may change, suspend, or discontinue Beta Services at any time

without prior notice to Customer. Everlaw's indemnity obligations under Section 9.1 do not apply to Beta Services. EVERLAW'S MAXIMUM AGGREGATE LIABILITY WITH RESPECT TO BETA SERVICES WILL NOT EXCEED \$100.

2. **Free Trial.** Everlaw may make one or more feature of the Service available to Customer on a trial basis free of charge ("Free Trial Service") until the earlier of (A) the end of the free trial period for which Customer agreed to use such Free Trial Service, (B) the start date of any Subscription purchased by Customer for such Free Trial Service, or (C) termination of the Free Trial Service by Everlaw in its sole discretion. Free Trial Services may be subject to additional terms and may be presented at the time Customer is given access to the Free Trial Service. FREE TRIAL SERVICES ARE PROVIDED "AS IS" WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES OR REPRESENTATIONS OF ANY KIND. Everlaw may change, suspend, or discontinue Free Trial Services at any time without prior notice to Customer. Everlaw's indemnity obligations under Section 9.1 do not apply to Free Trial Services. EVERLAW'S MAXIMUM AGGREGATE LIABILITY WITH RESPECT TO FREE TRIAL SERVICES WILL NOT EXCEED \$100.
3. **Modifications.** Everlaw may update these Terms and will notify Customer of any changes by posting new Terms at <https://www.everlaw.com/customer-terms-of-service/> and updating the "Last Updated" date. Everlaw will notify Customer of material changes by sending an email to Commercial Contact's address and such changes will be effective 30 calendar days following notification, except to the extent the changes are required by applicable laws, rules, or regulations, in which case they will be effective immediately. Continued use of the Service following such changes will indicate Customer's acknowledgement of such changes and agreement to be bound by the updated version of these Terms.
4. **Assignment.** Neither party may assign the Agreement, except to an Affiliate, without the written consent of the other, except that Everlaw may assign this Agreement in connection with a merger, sale of substantially all of its stock or assets, or other change in Control. Any other attempt to assign is void.
5. **Notices.** All notices and other communications will be in writing and given when sent by email.

6. **No Agency.** The Agreement does not create any agency, partnership, or joint venture between the parties.
7. **Severability.** If any provision in the Agreement is invalid, illegal, or unenforceable, the rest of the Agreement will remain in effect.
8. **Force Majeure.** Except for payment obligations under the Agreement, 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.
9. **Entire Agreement.** The Agreement states all terms agreed between the parties, and supersedes any prior or contemporaneous agreements between the parties relating to the subject matter of the Agreement. In entering into the Agreement, neither party has relied on, and neither party will have any right or remedy based on, any statement, representation, or warranty (whether made negligently or innocently), except those expressly described in the Agreement. The Agreement includes URL links to other terms, which are incorporated by reference into the Agreement.

14. DEFINITIONS.

1. **Account Information** means information about a Customer that it provides to Everlaw in connection with the creation, administration, or updating of its account. For example, Account Information includes names, usernames, phone numbers, email addresses, and billing information associated with Customer's account.
2. **Administrator Access** means the level of access that allows an individual to administer the Service by having the ability to select organization settings and permissions on the Service.
3. **Affiliate** means any entity that directly or indirectly Controls, is Controlled by, or is under common Control with a party.
4. **Annual Fee** means an annual fee based on a Minimum Commitment.
5. **Authorized User(s)** means anyone whom the (A) Customer or Reseller, or (B) a person with Administrator Access on a Customer's account, has invited to join Customer's account on the Service. Authorized Users act on behalf of Customer and may be employees, contractors, or agents of Customer or Reseller, including attorneys representing Customer.

6. **Case Materials** means the Documents uploaded or submitted to the Service and any content created in the Service by Customer or Authorized Users, or applicable Reseller. Case Materials include Input and Output but do not include: (A) Account Information; (B) Service-Generated Data, or (C) Project and Database names and labels, though Project and Database names and labels are considered Proprietary Information subject to Section 7 (Confidentiality).
7. **Claim** means, collectively, any third-party claims, demands, and actions.
8. **Commercial Contact** means the individual designated in the applicable Order Form who is authorized to purchase the Service on behalf of Customer.
9. **Control** means control of greater than 50% of the voting rights or equity interests of a party.
10. **Database** means the repository where a discrete collection of Customer's Case Materials are uploaded and stored within the Service.
11. **DPA** means Everlaw's Data Processing Addendum, available at <https://www.everlaw.com/customer-data-processing-addendum/>.
12. **Disclosing Party** means the party that discloses Proprietary Information to the other party.
13. **Dispute** means any controversy, claim, or dispute arising out of or relating to this Agreement, or the alleged breach of the Agreement.
14. **Document** means the reviewable object in its uncompressed, unpacked format. It may include any combination of text, images, and/or native files.
15. **Documentation** means the Everlaw documentation (as may be updated from time to time) in the form generally made available by Everlaw to its customers for use with the Service at <https://support.everlaw.com/hc/en-us> (which URL link may be updated from time to time).
16. **Everlaw AI Assistant** means any machine learning capability or functionality made available by Everlaw, including without limitation any capability or functionality labeled or otherwise identified by Everlaw as AI-powered.
17. **Feedback** means ideas, suggestions, feedback, recommendations, or improvements pertaining to the Service provided by Customer and Authorized Users.

18. **HIPAA** means the U.S. Health Insurance Portability and Accountability Act of 1996.
19. **Input** means any text, information, or other content Customer provides or makes available to Everlaw AI Assistant for processing.
20. **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 similar rights (registered or unregistered).
21. **Minimum Commitment** means a Subscription that comes with either: (A) a fixed minimum Storage Capacity reserved for Customer's use; or (B) an amount of Storage Usage that, when calculated, is an amount equal to the minimum recurring fee Everlaw charges the Customer.
22. **Monthly Unit Price** means a price per gigabyte of Storage Usage per month.
23. **Native Data** means the Documents within the Case Materials the Customer or an Authorized User uploads via the native uploader functionality or created and processed by the Service.
24. **Order Form** means the document incorporated into these Terms and stating Customer's Subscription.
25. **Output** means any text, information, or other content that Everlaw AI Assistant generates based on Input and returns to Customer and Authorized Users.
26. **Privacy Notice** means Everlaw's Privacy Notice, available at <https://www.everlaw.com/legal/privacy-notice/>.
27. **Processed Data** means the Documents within the Case Materials Customer or an Authorized User uploads via the processed uploader functionality or created by the Service.
28. **Projects** mean the repositories created within a Database where Customer and Authorized Users, or applicable Reseller, utilize the Service.
29. **Proprietary Information** means all information that is designated as confidential and/or proprietary or that should reasonably be understood to be confidential given the nature of the information and the circumstances of disclosure, including: (A) with respect to Customer, the Case Materials, and

Project and Database names and labels; and (B) with respect to Everlaw, the pricing offered to Customer by Everlaw.

- 30. **Recipient** means the party that receives Proprietary Information from the other party.
- 31. **Reseller** means an authorized Everlaw reseller.
- 32. **Service** means the applicable Everlaw hosted eDiscovery and document management platform procured in the Order Form, as described in the Documentation.
- 33. **Service-Generated Data** means all data generated or derived from a Customer's and Authorized Users' interaction with the Service, including data such as crash history, time the Service takes to load, configuration data; and diagnostic, capacity, and usage information to determine storage requirements.
- 34. **Service Specific Terms** means the then-current terms specific to one or more Everlaw or third party services contained within the Service available at <https://www.everlaw.com/legal/service-specific-terms/>.
- 35. **Storage Capacity** means the minimum commitment storage amount that Customer purchases stated in the applicable Order Form.
- 36. **Storage Usage** means the actual number of bytes of data Customer uses on the Service, calculated on a monthly basis by the method stated in the applicable Order Form.
- 37. **Subscription** means access to and usage of the Service subject to these Terms and referenced on the applicable Order Form.
- 38. **Terms of Use** refers to the then-current Everlaw Terms of Use available at <https://everlaw.com/legal/global-terms-of-use>.
- 39. **Trademark Policy** refers to the then-current Everlaw Trademark Policy available at <https://everlaw.com/legal/trademark-policy>.
- 40. **TSS** means the then-current Everlaw technical support services associated with the Service under the TSS Guidelines.
- 41. **TSS Guidelines** means the then-current Everlaw technical support services guidelines for the Service. TSS Guidelines are available at <https://everlaw.com/legal/everlaw-tss-guidelines>.

42. **Unpaid Subscription** means access to and use of the Service, or components of the Service, without payment.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.:

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

- | | |
|--|--|
| <input checked="" type="checkbox"/> Addendum No. 1 | <input type="checkbox"/> Addendum No. 6 |
| <input checked="" type="checkbox"/> Addendum No. 2 | <input type="checkbox"/> Addendum No. 7 |
| <input type="checkbox"/> Addendum No. 3 | <input type="checkbox"/> Addendum No. 8 |
| <input type="checkbox"/> Addendum No. 4 | <input type="checkbox"/> Addendum No. 9 |
| <input type="checkbox"/> Addendum No. 5 | <input type="checkbox"/> Addendum No. 10 |

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Carahsoft Technology Corporation

Company



Authorized Signature

03/05/25

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: Carahsoft Technology Corporation

Name of Agency: State of WV Department of Administration Purchasing Division

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?

Yes ☐
No ☒

2. If yes to #1, does the restricted information include personal data?

Yes ☐
No ☐

3. If yes to #1, does the restricted information include non-public data?

Yes ☐
No ☐

4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?

Yes ☐
No ☐

5. Provide name and email address for the Department privacy officer:

Name: _____

Email address: _____

Vendor/Service Provider's required information:

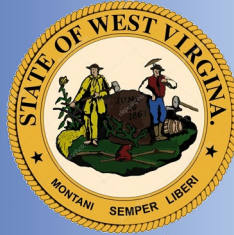
6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

Name: John Dutton

Email address: john.dutton@everlaw.com

Phone Number: 703.225.8142

Carahsoft's Response to the
State of West Virginia



Request for Quote

Cybersecurity e-Discovery Software

Solicitation Number: CRFQ 0231 OOT2500000017

Friday,
March 07, 2025

Solution Provided By



Carahsoft Technology Corporation

11493 Sunset Hills Road, Suite 100
Reston, VA 20190

888.662.2724 | www.carahsoft.com

Primary Point of Contact

Lexi Sutton | Senior Account Representative
571.662.3802 | Lexi.Sutton@carahsoft.com

Secondary Point of Contact

Proposals@carahsoft.com

March 07, 2024

State of West Virginia
Bid Clerk
Department of Administration Purchasing Division
2019 Washington St. E
Charleston, WV 25305

Re: Carahsoft's Response to the State of West Virginia's Request for Quote: Cybersecurity e-Discovery Software, Solicitation Number: CRFQ 0231 OOT2500000017

Dear Contracting Officer,

Carahsoft Technology Corp. appreciates the opportunity to respond to the State of West Virginia (WV)'s Request for Quote (RFQ): Cybersecurity e-Discovery Software. Carahsoft is proposing an Everlaw solution which fully meets WV's requirements. Our team has reviewed and considered WV's requirements outlined in the RFQ and has carefully put together a solution that will best meet your needs.

Carahsoft, The Trusted Government IT Solutions Provider®, is responding as the GSA Multiple Award Schedule (MAS) contractor (47QSWA18D008F) and reseller for Everlaw. As the Master Government Aggregator® for our vendor partners, 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.

Please feel free to contact me directly at 571.662.3802/Lexi.Sutton@carahsoft.com or Ryan Odom at 703.889.9811/Ryan.Odom@carahsoft.com with any questions or communications that will assist WV 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,

Lexi Sutton

Lexi Sutton
Senior Account Representative

Table of Contents

Introduction..... 4

 The Everlaw Difference 6

Solution Details..... 8

 3. Qualifications 9

 4. Mandatory Requirements 9

 Additional Everlaw Solution Highlights 42

Pricing 47

 Everlaw Standard Pricing Model 47

 Everlaw AI Assistant - Generative AI Pricing..... 47

 Included Everlaw Features and Functionality..... 48

Contract Manager..... 48

Everlaw Implementation and Support..... 49

 Technical Deployment Overview 49

 Everlaw Support Model 50

Training Plan 51

 On-demand Training..... 52

 Live and Virtual Live Training..... 52

 On-platform Walkthroughs 53

 Training Documentation..... 53

 Training Certifications 53

Security Details 53

 Product Security Features 54

 Data Security 55

 Data Rights and Accessibility 56

 Identity, Authorization and Access Management (IdAAM)..... 57

 Operational FISMA Compliance..... 57

 Sensitive and Embargoed Data..... 57

 Confidentiality and Non-Disclosure..... 58

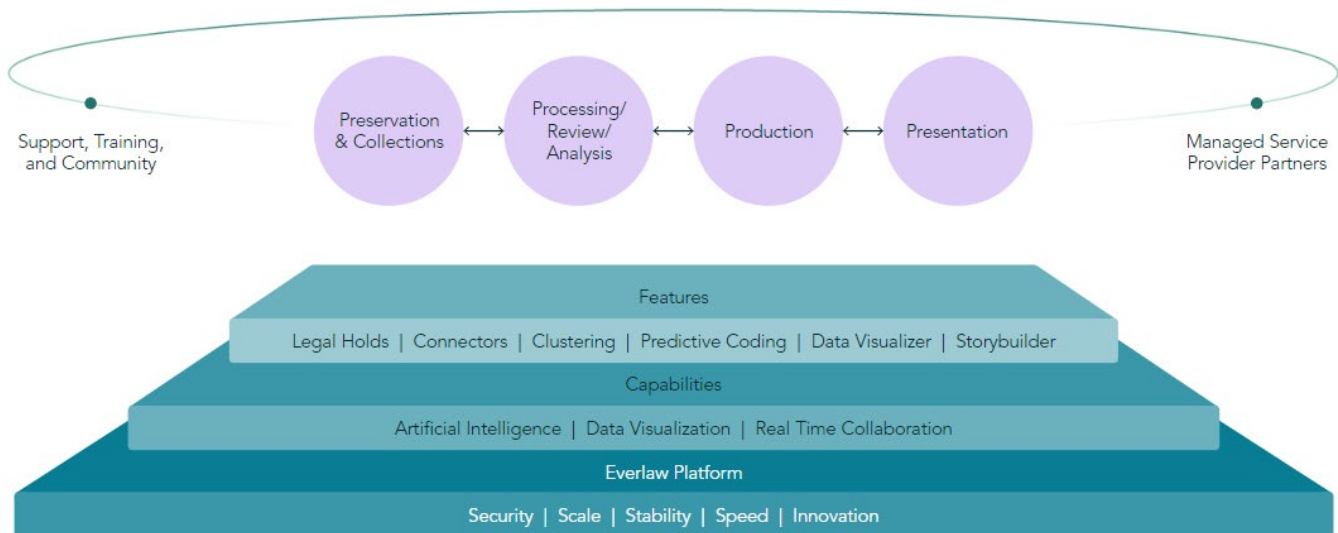
Everlaw Standard Service Level Agreements..... 58

Exceptions to Terms and Conditions 59

Attachments 60

Introduction

West Virginia Office of Technology (the “Agency”) deserves a modern and intuitive ediscovery platform. Everlaw is trusted by the Federal, State and Local Government enterprise customers across the U.S. to streamline their ediscovery experience. As technology has reduced complexity and replaced labor intensive tasks with a more consumer like experience, Everlaw has been the leader in bringing the power of ediscovery to users without the need for contractors, data scientists and large support staff. Everlaw is ready to bring West Virginia into the future of ediscovery.



Everlaw feels strongly that its enterprise-grade, “all-in-one” technology will empower Agency case teams to become future-ready and streamline the full range of litigation support needed for their matters, including ingestion (processing), capture, organization, search, review, analysis, and production of ESI.

Everlaw is committed to supporting our federal clients for the long term and has assigned dedicated resources and built our FedRAMP-Moderate authorized, Software as a Service on top of AWS-Govcloud to create a secure space to address the unique needs, make our technology more accessible, and help build professional efficiencies to empower government teams.

It is harder than it has ever been before to operate as a federal agency when you have to contend with:

- / Rising taxpayer expectations and growing amounts of work to be done, despite security risks that continue to increase and compound.
- / Rising complexity of work thanks to more data and an ever-growing variety of data types.

- / Rising internal pressures, including fewer resources to do more work, budgetary constraints, increasingly distributed workforce, and heightened employee expectations.

Everlaw believes that there's a different way to contend with these challenges and come out ahead – to achieve outcomes like employee efficiency gains that enable matters to be addressed more quickly, less time spent reviewing docs and more time spent crafting a winning strategy, internal recognition that agencies can in fact both lower costs and get to key insights sooner, the ability to better attract top talent, or – all of which agencies and organizations – like the US DOJ and US DOI – are achieving with Everlaw.

We believe getting your technology strategy right is no longer a nice-to-have, but rather the difference-maker in who comes out ahead and who falls behind in this new era, and we believe Everlaw is uniquely positioned to play a critical role in which organizations come out ahead for 3 key reasons: Everlaw offers the best technology on the market, is dedicated to helping clients achieve business outcomes, and is the right partner to help the Agency become future-ready.

Best Technology

For one, Everlaw is objectively the best tech option. Our platform helps to amplify your existing strengths and has emerged as the preeminent tech option on the market. Everlaw is easy to adopt by both tech savvy and tech-averse legal professionals, and it's well-suited in terms of capabilities, speed, and level of Support you get from Everlaw for matters of all sizes and degrees of complexity. Additionally, Everlaw was fully built in the cloud and is a truly unified solution – not an on-prem solution that's been retrofitted to be accessible via the cloud or one that's made up of acquired platforms strung together. All of this means that the benefits you get from reducing the time it takes to start matters, uncover key insights, and start on post-review are readily scaled across your business.

Business Outcomes Orientation

Everlaw also excels in delivering measurable business outcomes as trusted partners to clients; we're not just here to solve technical needs. One private sector client, for instance, brought 70% more work in-house in their first year with Everlaw while the U.S. Department of Justice ("DOJ") has been able to greatly reduce the amount of time spent on matters.

Right Partnership

While customers agree that Everlaw is great today, no one knows exactly how the unprecedented tech and industry evolution we find ourselves embarking on will continue to change how legal work is done. However, we're confident that our track record of innovation (including strides we've already made in

generative AI); thoughtful and disciplined Engineering function, formed by a CEO and founder with a PhD in computer science; and the fact that we've designed our business for the long-term – we're not beholden to private equity trying to make a quick profit or looking for a quick exit ourselves, but rather geared toward becoming the market leader for the next few decades – make us the right partner to save you money, reduce risk, and improve the outcomes your agency is able to deliver.

The Everlaw Difference

Everlaw's mission is to promote justice by illuminating truth. We take our federal customer needs seriously, and we work together with our users to continuously improve their experience and add value to the mission. Everlaw consistently strives to achieve our own company mission by delivering on our core values of transparency, respect for users, affinity for speed, rapid innovation, and security. Our focus on these values ensures that Everlaw will provide an effective solution and exceptional experience to the Agency.



Transparency

Our commitment to transparency manifests most obviously in the product, providing audit trails and reporting on data uploads, early case assessment ("ECA"), and review decisions for accountability and transparency purposes. Beyond the actual product, we're committed to a pricing model that's easy to understand and predictable, based on the amount of data hosted, with unlimited user licenses, processing, and productions.



Respect for Users

The Everlaw approach to building software is to deliver elegant solutions with thoughtful design that makes for happy software users who can not only get their jobs done, but also find enjoyment in the process. We are focused on long-term success with our partners rather than making quick changes to the platform that don't provide utility or align with long term strategies. We are confident Agency users will find our ease-of-use to be superior to any of our competitors.



Affinity for Speed

Everlaw automates or streamlines every step of the discovery process, whether it's ingesting, searching, reviewing, or producing documents. The ingestion engine achieves processing and production speeds of 900K+ documents per hour. Blink-speed search provides instant results with even the most complex search strings. Everlaw's proprietary PDF viewer saves our users thousands of hours of review time, navigating between documents in 1/8 of a second.



Rapid Innovation

Everlaw's commitment to innovation consistently propels us forward. We release new features roughly every four weeks, and our release cycle keeps us "close to the code" so that bugs don't linger. As a cloud-native solution, we have the advantage of instantly deploying our innovations and enhancements to all customers. All cases are up to date with the latest

technology, all the time. Everlaw also keeps up with emerging data sources to handle modern file types. The magnitude and velocity of our feature innovation can be observed by reviewing our release notes on our website. These release updates occur on schedule, at no additional cost, with no required action for installation or updating, and no maintenance burden for our customers. Agency users will simply log on to their secure URL to find new innovations every four weeks. Prior to making a release, the Agency will be informed of any anticipated changes and after release, a walkthrough of the changes will appear on the home screen.















Security

Everlaw employs extensive security measures to protect customers' data and is built on AWS-GovCloud to ensure U.S. Person only support. Everlaw is one of the first ediscovery platforms to achieve FedRAMP authorization, with sponsorship from the U.S. DOJ. Everlaw was also one of the first cloud ediscovery platforms to successfully obtain a SOC 2 Type II security certification along with HIPAA compliance and has conducted several third-party security audits and penetration tests to demonstrate compliance. Furthermore, Everlaw has both SSO and Multi-factor authentication (MFA) options available and integrates with most major authentication platforms including Okta and Active Directory.

Solution Details

Everlaw's cloud-based, ediscovery platform for legal professionals enables teams to manage, analyze, and collaborate on information across a geographically dispersed user base. Everlaw combines speed, security, and ease-of-use into a unified, comprehensive solution that unlocks the collaborative power of teams and allows them to investigate issues more thoroughly, uncover truth more quickly, and present their findings more clearly.

Manage	Analyze	Collaborate
 Upload	 Data visualization	 Legal holds
 Search	 Predictive coding	 Narrative building
 Review	 Advanced analytics	 Depositions
 Productions	 Clustering	 Secure collaboration

Unlike our competitors, the Agency can expect no hidden charges from Everlaw. All of our features and functionality are fully integrated, including processing, analytics and production, with no plug-ins or additional products required to gain the full benefit of the Everlaw platform, in a secure environment. To complement our modern technology, Everlaw offers unlimited users, projects, and its thoughtful onboarding, training and ongoing customer success support at no additional cost. Everlaw believes its unique, user-centered approach will simplify and streamline each matter.

Everlaw delivers on all required and desired functionality for the Agency and the following summarizes how Everlaw addresses the specific solution requirements provided in Agency CRFQ.

3. Qualifications

Vendor, or Vendor's staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

3.1 The Vendor must be compliant with Internal Revenue Service (IRS) 1075, Section AC-17 Remote Access, and Section 3.3.1. Cloud Computing.

Everlaw's FedRAMP and StateRAMP authorized solution complies with Internal Revenue Service (IRS) 1075, Section AC-17 Remote Access, and Section 3.3.1. Cloud Computing in the Government Community Cloud (GCC) environment.

4. Mandatory Requirements

4.1 Mandatory Contract Services Requirements and Deliverables

Req #	Requirement	Everlaw Solution
4.1.1 General Requirements - ediscovery System		
4.1.1.1	The vendor must provide an ediscovery system that is cloud-based (Software as a Service Model), as well as support Automated Cloud Data Collections and Connectors	<p>▼ Everlaw is a collaborative, cloud-based litigation platform that enables teams to discover, illuminate, and act on information to better drive internal investigations and positively impact the outcome of litigation and investigations. Unlike legacy platforms, which can be slow and unwieldy, only Everlaw combines speed, security, and ease-of-use into a unified, comprehensive solution that unlocks the collaborative power of teams and enables them to investigate issues more thoroughly, uncover truth more quickly, and present their findings more clearly.</p> <p>Everlaw delivers a comprehensive, tightly-coupled ediscovery solution from ingestion through production in a far more elegant and efficient manner than other tools on the market. The solution was created with thoughtful design and affinity for speed; this is especially apparent when compared to legacy platforms.</p> <p>Everlaw's self-serve upload and automated processing feature set streamlines the ingestion and processing of both native and processed data. Traditionally this has been one of the most complicated elements of the EDRM, but with Everlaw's wizard-driven process, even novice users can ingest and process data with a few simple steps. Everlaw can process more file types than most platforms on the market today, and at unparalleled speeds (benchmarked at 900,000 documents per hour). Behind the scenes, Everlaw does all the heavy lifting of automatically: extracting metadata and text, OCR-ing documents without extractable text, creating searchable color PDFs for all documents (except types like spreadsheets and A/V) to optimize the reviewer experience, identifying PDFs of emails as emails and extracting their metadata, threading emails, identifying Non-English Languages, transcoding and transcribing audio video files, and optimizing documents for analytics and search. At the conclusion of processing, Everlaw delivers a concise report of the file types, data size and errors (if any) for review and validation purposes.</p>
4.1.1.2	The system must contain the following capabilities within a single platform that does not require integration with other software: self-service data loading, self-service data processing, client administration, self-service, productions, review, and analytics capabilities.	<p>▼ <u>Self Service Data Loading and Processing</u></p> <p>Everlaw is a fully self-service platform and Everlaw's customers are empowered to manage all aspects of the platform. Everlaw's support team is available to assist with any questions that arise when using the platform. Please refer to the response to 4.1.1.1 above as well as</p>

Req #	Requirement	Everlaw Solution
		<p>Section 4.1.2 for information regarding Data Loading and Processing.</p> <p><u>Client Administration</u></p> <p>Everlaw's platform provides administrators with fine-grained permission settings, allowing precise control over user access and maintaining workflow transparency throughout a case's life cycle. Role-Based Access Control enables administrators to manage project access and permissions by group. Project administrators can create security groups (e.g., Administrators, Project Manager, Reviewer) with customizable permissions, even down to individual document or code levels.</p> <p>Administrators can also create custom categories and codes (tags), such as "Hot Docs", for document designation. Additionally, Everlaw's granular permissions groups allow administrators to strictly control ESI uploading and processing through Project and Database Administrator rights, among other features and tasks.</p> <p><u>Productions</u></p> <p>Everlaw's production wizard allows users to customize all elements needed for production or export. The wizard provides a user-friendly interface to assist users and make all selections transparent, ensuring the user produces in the format required. Everlaw includes both DOJ and SEC-compliant protocols (templates) for production, and further allows users to customize additional protocols for future use.</p> <p>Please refer to the responses to Section 4.1.6 below for more detailed information regarding Productions in Everlaw.</p> <p><u>Review</u></p> <p>Everlaw's innovative features make document review faster and more effective than ever. Everlaw offers users an inherently customizable document review experience that has built-in collaboration into every element of the platform to help reduce information silos and help teams surface key information faster. Users can easily share and collaborate on everything from searches to depositions, testimony or trial preparation.</p> <p>Furthermore, as an eDiscovery platform that was designed with the scalability of the cloud in mind,</p>

Req #	Requirement	Everlaw Solution
		<p>Everlaw gives our clients near limitless scaling potential. We have hosted matters that have had hundreds of concurrent users reviewing tens of millions of documents with no discernible performance issues. Please refer to the responses to Section 4.1.3 below for information regarding Review in Everlaw.</p> <p><u><i>Analytics</i></u></p> <p>Everlaw's analytics tools are an integrated element of the Everlaw platform. For instance, Everlaw's Project Analytics provides extensive performance reports that are configurable and filterable based upon different user activities within the platform. Everlaw also automatically creates email threads and performs a near duplicate analysis upon ingestion and both are displayed within the context panel of the review window. Near duplicates will display down to a 95th percentile. Email threads can be easily filtered based on inclusiveness.</p> <p>Additionally, analytics can be used to prioritize important documents for faster review. Everlaw utilizes TAR 2.0 technology for Predictive Coding based on term frequency inverse document frequency (tf-idf). Models are set up in just three quick steps and a customizable dashboard will populate as soon as at least 200 unique documents have been reviewed and coded (with at least 100 in both of the binary decision categories for the model). Everlaw's clustering capability is also based on a tf-idf calculation. Clustering displays down to the document level and users can layer on predictive coding or review decisions on clusters to see trends. Clusters can also be visualized through the data visualizer interface displayed on the right hand screen of the clustering interface.</p> <p>Please refer to the responses to Section 4.1.4 below for further information regarding Analytics in Everlaw.</p>

Req #	Requirement	Everlaw Solution
4.1.1 General Requirements - ediscovery System		
4.1.1.1	The vendor must provide an ediscovery system that is cloud-based (Software as a Service Model), as well as support Automated Cloud Data Collections and Connectors	<p>▼ Everlaw is a collaborative, cloud-based litigation platform that enables teams to discover, illuminate, and act on information to better drive internal investigations and positively impact the outcome of litigation and investigations. Unlike legacy platforms, which can be slow and unwieldy, only Everlaw combines speed, security, and ease-of-use into a unified, comprehensive solution that unlocks the collaborative power of teams and enables them to investigate issues more thoroughly, uncover truth more quickly, and present their findings more clearly.</p> <p>Everlaw delivers a comprehensive, tightly-coupled ediscovery solution from ingestion through production in a far more elegant and efficient manner than other tools on the market. The solution was created with thoughtful design and affinity for speed; this is especially apparent when compared to legacy platforms.</p> <p>Everlaw's self-serve upload and automated processing feature set streamlines the ingestion and processing of both native and processed data. Traditionally this has been one of the most complicated elements of the EDRM, but with Everlaw's wizard-driven process, even novice users can ingest and process data with a few simple steps. Everlaw can process more file types than most platforms on the market today, and at unparalleled speeds (benchmarked at 900,000 documents per hour). Behind the scenes, Everlaw does all the heavy lifting of automatically: extracting metadata and text, OCR-ing documents without extractable text, creating searchable color PDFs for all documents (except types like spreadsheets and A/V) to optimize the reviewer experience, identifying PDFs of emails as emails and extracting their metadata, threading emails, identifying Non-English Languages, transcoding and transcribing audio video files, and optimizing documents for analytics and search. At the conclusion of processing, Everlaw delivers a concise report of the file types, data size and errors (if any) for review and validation purposes.</p>
4.1.1.2	The system must contain the following capabilities within a single platform that does not require integration with other software: self-service data loading, self-service data processing, client administration, self-service, productions, review, and analytics capabilities.	<p>▼ <u>Self Service Data Loading and Processing</u></p> <p>Everlaw is a fully self-service platform and Everlaw's customers are empowered to manage all aspects of the platform. Everlaw's support team is available to assist with any questions that arise when using the platform. Please refer to the response to 4.1.1.1 above as well as</p>

Req #	Requirement	Everlaw Solution
		<p>Section 4.1.2 for information regarding Data Loading and Processing.</p> <p><u>Client Administration</u></p> <p>Everlaw's platform provides administrators with fine-grained permission settings, allowing precise control over user access and maintaining workflow transparency throughout a case's life cycle. Role-Based Access Control enables administrators to manage project access and permissions by group. Project administrators can create security groups (e.g., Administrators, Project Manager, Reviewer) with customizable permissions, even down to individual document or code levels.</p> <p>Administrators can also create custom categories and codes (tags), such as "Hot Docs", for document designation. Additionally, Everlaw's granular permissions groups allow administrators to strictly control ESI uploading and processing through Project and Database Administrator rights, among other features and tasks.</p> <p><u>Productions</u></p> <p>Everlaw's production wizard allows users to customize all elements needed for production or export. The wizard provides a user-friendly interface to assist users and make all selections transparent, ensuring the user produces in the format required. Everlaw includes both DOJ and SEC-compliant protocols (templates) for production, and further allows users to customize additional protocols for future use.</p> <p>Please refer to the responses to Section 4.1.6 below for more detailed information regarding Productions in Everlaw.</p> <p><u>Review</u></p> <p>Everlaw's innovative features make document review faster and more effective than ever. Everlaw offers users an inherently customizable document review experience that has built-in collaboration into every element of the platform to help reduce information silos and help teams surface key information faster. Users can easily share and collaborate on everything from searches to depositions, testimony or trial preparation.</p> <p>Furthermore, as an eDiscovery platform that was designed with the scalability of the cloud in mind,</p>

Req #	Requirement	Everlaw Solution
		<p>Everlaw gives our clients near limitless scaling potential. We have hosted matters that have had hundreds of concurrent users reviewing tens of millions of documents with no discernible performance issues. Please refer to the responses to Section 4.1.3 below for information regarding Review in Everlaw.</p> <p><u><i>Analytics</i></u> Everlaw's analytics tools are an integrated element of the Everlaw platform. For instance, Everlaw's Project Analytics provides extensive performance reports that are configurable and filterable based upon different user activities within the platform. Everlaw also automatically creates email threads and performs a near duplicate analysis upon ingestion and both are displayed within the context panel of the review window. Near duplicates will display down to a 95th percentile. Email threads can be easily filtered based on inclusiveness.</p> <p>Additionally, analytics can be used to prioritize important documents for faster review. Everlaw utilizes TAR 2.0 technology for Predictive Coding based on term frequency inverse document frequency (tf-idf). Models are set up in just three quick steps and a customizable dashboard will populate as soon as at least 200 unique documents have been reviewed and coded (with at least 100 in both of the binary decision categories for the model). Everlaw's clustering capability is also based on a tf-idf calculation. Clustering displays down to the document level and users can layer on predictive coding or review decisions on clusters to see trends. Clusters can also be visualized through the data visualizer interface displayed on the right hand screen of the clustering interface.</p> <p>Please refer to the responses to Section 4.1.4 below for further information regarding Analytics in Everlaw.</p>
4.1.1.3	The vendor must provide an ediscovery system with unlimited user seats for a minimum of 12 months from date of award.	<p>▼ Everlaw provides unlimited user seats at no additional charge. Everlaw is designed to facilitate collaboration with other agencies, internal divisions, outside counsel, or expert witnesses in a highly secure environment. Any number of users with any email domain can be invited to the projects designated by the Agency, utilizing Everlaw's unique no-cost unlimited users policy. The Agency will then have the option to restrict their document access and other permissions in the main review project / workspace.</p> <p>Alternatively, Agency Project Administrators can also</p>

Req #	Requirement	Everlaw Solution
		take advantage of Everlaw's unique, no-cost unlimited projects model to create separate partial (sub) projects / workspaces, eliminating the risk of providing complete access to the entire document corpus. Please refer to the Pricing section of this document for additional information.
4.1.1.4	The system must allow client administrators to have the ability to set up new users or workspaces and assign roles and permissions to new users.	<p>▼ Everlaw's platform allows customers to manage access to their accounts and projects, including adding or removing projects, users or groups at any time. Customers' assigned administrators can utilize fine-grained permission settings and role-based access controls (RBAC) to precisely grant user groups the necessary access to perform their jobs effectively. Through customizable RBAC, administrators can determine granular permissions or restrictions for user groups throughout the platform, and even refine or restrict access within and among matters. Please refer to https://support.everlaw.com/hc/en-us/articles/205583355-User-Groups-and-Project-Permissions for further information.</p>
4.1.1.5	The system must allow a user to have multiple roles and toggle between roles. For example, a client administrator can toggle between user roles to validate user permissions and provide users support.	<p>▼ Everlaw provides admins with granular control over permissions for different roles. Admins can toggle between roles and modify permissions for specific user groups in the "Permissions" tab of the "Project Settings" page, accessible via the Project Management tab. Additionally, user roles within a project can be changed by adjusting their user group level, along with their access to features and objects within Everlaw.</p>
4.1.1.6	The system must not require additional licenses and/or software from third parties.	<p>▼ Everlaw is a fully cloud-based platform supported by any modern web browser, including Microsoft Internet Explorer version 10 and version 11, Google Chrome, Edge, and Safari. No other software (including third-party applications) is required in order to access the platform..</p>
4.1.1.7	The system must allow the customer/client administrators the ability to remove/delete documents and create archives from the platform.	<p>▼ Admins and users with the proper permission levels are able to remove/delete documents from the platform. Everlaw's User Activity report logs all user activity including adding or deleting any document in the platform.</p> <p>For a full case archive, Everlaw has a simple one-click export that allows an administrator to export all data and work product from a case that can be imported back in at a later time if necessary. Data is exported in an industry standard format with a .DAT file for metadata, .OPT for images, and all accompanying data</p>

Req #	Requirement	Everlaw Solution
		<p>files.</p> <p>Everlaw also provides a case suspension option, which moves a case to near-line storage. This makes it inaccessible to the client, but billed at a significantly lower hosting rate. Users with appropriate permissions can quickly reactivate suspended databases or projects with one click to regain access to a case.</p>
4.1.1.8	The system must be accessible to an unlimited number of users and allow access to at least 50 concurrent cases each having at least one million documents without degradation to speed.	<p>▼ As an ediscovery platform that was designed with the scalability of the cloud in mind, Everlaw gives our clients near limitless scaling potential. We have hosted matters that have had hundreds of concurrent users reviewing tens of millions of documents with no discernable performance issues.</p>
4.1.1.9	The system must be a configurable platform that allows the administrators to configure applications like request tracking and FOIA requests.	<p>▼ Everlaw provides lightning-fast data-ingestion speeds, seamless connections to common cloud-storage platforms, powerful search, and integrated collaborative capabilities, all within one intuitive and easy-to-use platform that allows Agencies to respond more quickly and with more confidence. Please refer to https://www.everlaw.com/foia-public-records-requests/ for additional information.</p>
4.1.1.10	The system must be built on scalable architecture.	<p>▼ As a cloud-native platform, Everlaw is highly scalable and can easily support projects with hundreds of users and millions of documents with no performance impact. Everlaw is hosted by AWS, which assigns processing resources as required to allow near limitless scaling potential.</p>
4.1.1.11	The vendor must provide an ediscovery system that features the following:	
4.1.1.11.1	A system that has two-factor authentication access.	<p>▼ Everlaw offers multi-factor authentication (MFA) at no additional cost for all customer accounts, which can be enforced at the organization level. Please refer to the Security Details section of this document for further information.</p>
4.1.1.11.2	A system that allows the Agency to have 100% data input automation. The Vendor must not have access to Agency-owned data.	<p>▼ Everlaw's customers manage access to their account and projects and can create and remove user accounts. Everlaw's role based access controls allow Everlaw's customers to finely control their access to individual projects and elements within those projects, including individual document level access within each project. Clients are responsible for the data they upload to the platform. Client data is only accessed upon client request during troubleshooting of issues.</p>
4.1.1.11.3	A system that provides 256-bit encryption to the data when at rest and in transit.	<p>▼ Everlaw customers' data is encrypted, whether it is in transit or at rest. We use hybrid encryption techniques</p>

Req #	Requirement	Everlaw Solution
		<p>that constitute software-based encryption, hosting solutions (AWS), and self-encrypting drives to align with NIST Special Publication 800-53.</p> <p>Encryption In Transit: Everlaw serves application data using HTTPS to ensure encryption in transit of all customer data. The Everlaw application uses Transport Layer Security (TLS) version 1.2 or higher to protect HTTPS communications. For email security, our platform leverages opportunistic TLS encryption (OE) by default.</p> <p>Encryption At Rest: Everlaw leverages the default encryption-at-rest provided by AWS, which protects the data on disk with AES-256 encryption. We also configure all snapshots to encrypt backup data. Additionally, Everlaw encrypts data at rest using AES-256 to secure inactive data stored on any device or network.</p>
4.1.1.11.4	A system that scans files for viruses.	<p>▼ Everlaw automatically scans for malicious files during processing and will flag them during processing, during review, and production.</p>
4.1.1.11.5	A system that allows for load file import and export.	<p>▼ Everlaw accepts industry standard load file formats for loading previously processed / production data (.DAT and .OPT), as well as .CSV or .TXT files with consistent delimiters. In addition, Everlaw can load .PDF productions that lack load files and maintain their bates numbering in the system (assuming the files are named after their bates number).</p> <p>Productions in Everlaw can include the following load files: DAT, OPT, LST, LFP, and DII. Everlaw's production wizard contains options for load file creation and customization (options to rename fields, combine text fields, combine or separate date and time fields, and include code, code category, and freeform code fields, and empty / custom fields).</p>
4.1.2 Data Loading & Processing - ediscovery System		
4.1.2.1	The system must allow the Agency to have 100% data input automation.	<p>▼ Please refer to the response to 4.1.1.11.2 above.</p>
4.1.2.2	The system must allow the user to load raw data such as PSTs, zip files, and other ESI for processing.	<p>▼ Everlaw has an integrated cloud-processing system that will automatically extract and process native files for ingestion into the platform. Data can be ingested through a direct connection with one of our cloud APIs (such as OneDrive, O365, SharePoint and more) or pulled directly from the user's file explorer.</p> <p>Users can input any anticipated passwords and the</p>

Req #	Requirement	Everlaw Solution
		<p>processing engine will use these to unlock any password-protected documents. Everlaw supports a wide variety of file types such as .PST, Microsoft Office files, .ZIP files, .PDF and .HTML, in addition to less common file types like .CAD, DICOM, A/V files, Slack and other short message format type files. During processing, files are automatically de-NISTed and deduped. Searchable transcripts are generated for A/V files, email threads and near duplicates are automatically identified, as well as any present Non-English language. Everlaw's processing tool generates searchable text (including OCR for files without extracted text), metadata, and images. Everlaw also has an easy, wizard driven process for the ingestion of pre-processed data (either with a load file or without).</p>
4.1.2.3	<p>The system must allow the client administrator to move data between data stores and conduct early case assessment, including running search terms, and listing and counting file types reports, prior to making the data available to reviewers.</p>	<p>▼ Everlaw has built-in, advanced-functionality Early Case Assessment (ECA) tools that can be leveraged for the purposes of culling down large document sets easily or storing a comprehensive, searchable dataset affordably over the life of a case. Data can be loaded either into an ECA project or an active review project. ECA projects include deduplication and email threading as well as Everlaw's full set of search and data visualization tools, including Search Term Reports, Concept Clustering AI, the Cluster Map, and Communication Visualizer. Users can view searchable PDFs, as well as view AI-identified "more documents like this one" from the review window while still in ECA. Data in ECA can be organized in binders, and priority data easily promoted to "active review" for coding, predictive coding, or production. Data housed in an ECA environment is billed at a greatly reduced rate.</p> <p>ECA projects also include functionality to run search terms and list/count file type reports</p>
4.1.2.4	<p>The system must allow the customer to create, save, and upload templates for data processing.</p>	<p>▼ Everlaw's processing engine automatically extracts and processes native files for ingestion into the platform, obviating the need for a template during the ingestion and processing steps.</p> <p>Everlaw automatically recommends field mapping for the most common metadata fields during a processed data upload. An Everlaw user can customize this field mapping and save it as a template. Additional details on the most common metadata fields that Everlaw will detect and map are located at https://support.everlaw.com/hc/en-us/articles/208407963-Standard-Fields</p>

Req #	Requirement	Everlaw Solution
4.1.2.5	The system must have pre-built utilities to support processing for various files including imaging, loading and text files.	<p>▼ Everlaw supports automatic native uploading and processing for most common file types out of the box.</p> <p>Once processed, Everlaw provides users with a near native, imaged file, and text file for review.</p> <p>Please refer to https://support.everlaw.com/hc/en-us/articles/360026908431-Supported-Native-Data-Types for a list of compatible file types within Everlaw.</p>
4.1.2.6	The system must support up to 10 GB of data directly from web-browser via “drag and drop.”	<p>▼ Everlaw accelerates document review by providing multiple document upload options. Users can drag and drop files from their local machine, browse to a network-connected location using the file explorer, or utilize one of our third-party API's cloud connectors for direct uploads. For drag-and-drop uploads, the maximum size limits are as follows: 5 TB for the top-level container file, 2 GB for an individual PDF, 50 loose files (not in a folder or container file) can be uploaded at once, and 5000 for loose PDFs uploaded without a load file.</p>
4.1.2.7	The system must allow loading and processing of a data set that has at least 1 terabyte of documents, data, or ESI, into the review tool.	<p>▼ There is no practical limit to the size of the data set that can be ingested and processed in Everlaw. However, as mentioned above in the response to 4.1.2.6, the maximum size of the top level container file is 5 TB. The maximum size of an individual PDF is 2 GB. The maximum number of loose files (not in a folder or container file) that can be uploaded at a time is 50, and the maximum number of loose PDFs without a load file is 5000.</p>
4.1.2.8	The system must support data reduction and culling (De-NIST; custodial and global deduplication; filtering by Custodian, file type, date; keyword searching) during processing.	<p>▼ <u>DeNISTing</u> Everlaw's processing engine will automatically deNIST all documents upon ingestion and creates a record within the processing report of which files have been deNISTed.</p> <p><u>Deduplication</u> Everlaw's native uploads offer the following Hash-based deduplication options: global, within-custodian, none. Upload deduplication always respects families (i.e. does not deduplicate attachments that are part of different families) and automatically populates "all custodians" and "all file paths" fields to maintain a record of all deduplicated documents for production.</p> <p>For documents not deduplicated in a native upload, Everlaw offers search-based deduplication and a review window duplicates view to identify duplicates.</p> <p>Since duplicate emails stored in different email clients</p>

Req #	Requirement	Everlaw Solution
		<p>often have different Hash values and so are notoriously difficult to deduplicate, Everlaw includes a proprietary email threading deduplication tool (turned on by default) allowing the identification of email duplicates with different hashes after upload.</p> <p><u>Filtering by Custodian, File type, Date</u> Everlaw's Data Visualizer allows users to interactively visualize and filter documents on dozens of document properties, metadata fields, and review values (ex., filtering by Custodian, file type, date, etc.) and convert those filters into searches. Filters can be combined. Results can be exported to CSV. Email contact fields are filterable by domain, contact name, and/or email address. The File Path view allows users to explore documents' original folder structure.</p> <p><u>Keyword Searching</u> Everlaw contains three primary search tools:</p> <p>The Search Term Report feature allows users to run lists of terms or search strings. Unique or rare functionality includes:</p> <ul style="list-style-type: none"> / high speed of running STRs / option to auto-refresh daily / per term hit reporting that additionally includes hits with family members and unique hits for each term / hyperlinked results for easy document set access / the option to search across document contents, text metadata fields (specific or all), or both / easy creation of project-wide persistent highlights from search terms / easy PDF and CSV reports for download <p>Everlaw's Instant Visual Search builder allows users to visually construct powerful searches combining terms, metadata and other document properties without the need to craft complex boolean search syntax. Unique or rare functionality includes:</p> <ul style="list-style-type: none"> / Searching for who applied codes at custom date-time ranges

Req #	Requirement	Everlaw Solution
		<ul style="list-style-type: none"> / Efficient email metadata search option to select a Contact, which automatically includes all email addresses associated with the contact name. / Efficient "Parties" and "Recipients" metadata search terms that combine email metadata fields. / Deduplication options (within search, project wide, remove non-inclusive documents from email threads while deduplicating) / Step-by-step deduplication and grouping reporting prior to running a search <p>Everlaw's Data Visualizer allows users to interactively visualize and filter documents on dozens of document properties, metadata fields, and review values and convert those filters into searches. Filters can be combined. Results can be exported to CSV. Email contact fields are filterable by domain, contact name, and/or email address. The File Path view allows users to explore documents' original folder structure.</p>
4.1.2.9	The system must include built-in ESI processing capabilities (extraction of text and metadata, imaging, numbering, OCR, load file creation).	<p>▼ When native data is uploaded to Everlaw, the following are run automatically: deduplication (global, within custodian, none), deNISTing, unpacking of container files (ZIP, PST, etc), extraction of attachments, processing / text extraction, OCR (70+ languages), search indexing, metadata extraction, PDF imaging (can be turned off), media file transcoding and transcribing (English, Spanish), language detection, email threading.</p> <p>Everlaw will maintain the integrity of all metadata processed into the platform and this metadata will be viewable and searchable.</p> <p>Everlaw automatically OCRs documents during the ingest process. For pages of native data TIFF or PDF files where no or very little (less than 50 non-white-space characters) of extractable text is found, Everlaw will automatically OCR those upon ingestion. Other images can be OCR'ed after upload by reprocessing. Non-English language detection and OCR takes place at the time of document upload. Everlaw has the ability to OCR for English and Non-English language simultaneously per page. OCR throughput is roughly 200,000 pages per hour.</p> <p>Everlaw's document export feature and production wizard includes options for load file creation.</p>

Req #	Requirement	Everlaw Solution
		Productions and exports in Everlaw can include the following load files: DAT, OPT, LST, LFP, and DII.
4.1.2.10	The system must keep emails and families together and locate orphaned documents during processing.	<p>▼ Everlaw email family relationships (also known as attachments) are preserved during processing. Documents and document families can be searched, grouped for review and produced within their family relationship. Nested container files are also extracted and unpacked.</p> <p>Threading: Everlaw's processing performs email threading automatically upon ingestion. This includes both the ability to search for only the most inclusive email in a thread, as well as the ability to display on the most inclusive email(s) from within the review window.</p> <p>Everlaw's linked documents context addresses the challenge of modern communication, where documents often reference cloud-hosted documents or objects via links. Unlike attachments, these documents are not contained within the email or document itself (i.e., orphaned documents) but are stored elsewhere, such as Google Drive or Box.</p> <p>Everlaw identifies links within the text of newly uploaded documents for specific applications. The "Linked Documents" section of the context panel displays the relationships between documents. If the linked document has been collected through an Everlaw connector, it will be linked via the context panel; otherwise, a placeholder will appear. For more information about the linked documents context, please refer to https://support.everlaw.com/hc/en-us/articles/205541875-Context-Panel-View-and-Batch-Code-Related-Documents-in-Review-Window#01HZ800PDF1TF6TJ429VWVG8J54</p>
4.1.2.11	The system must support extraction and processing of files within container files such as zip and rar, and support the processing of files in nested containers or folders.	<p>▼ Everlaw automatically extracts the individual documents within container files, meaning it unpacks and unzips the file, allowing users to access and search each document separately within the platform. This process also includes extracting metadata and generating images/text for each document if applicable.</p>
4.1.2.12	The system must have the ability to ingest, process, and view multiple file types.	<p>▼ Everlaw supports automatic native uploading and processing for a wide variety of file types.</p> <p>Once processed, Everlaw provides users with a near native, imaged file, and text file for review.</p> <p>Please refer to https://support.everlaw.com/hc/en-</p>

Req #	Requirement	Everlaw Solution
		us/articles/360026908431-Supported-Native-Data-Types for a list of compatible file types within Everlaw.
4.1.2.13	The system must allow for load file import and export.	<p>▼ As mentioned in the response to 4.1.1.11.5 above, Everlaw accepts industry standard load file formats for loading previously processed / production data (.DAT and .OPT), as well as .CSV or .TXT files with consistent delimiters. In addition, Everlaw can load .PDF productions that lack load files and maintain their bates numbering in the system (assuming the files are named after their bates number).</p> <p>Productions in Everlaw can include the following load files: DAT, OPT, LST, LFP, and DII. Everlaw's production wizard contains options for load file creation and customization (options to rename fields, combine text fields, combine or separate date and time fields, and include code, code category, and freeform code fields, and empty / custom fields).</p>
4.1.2.14	The system must allow the user the ability to create templates for processing, production, import and export.	<p>▼ As mentioned in the response to 4.1.2.4 above, Everlaw's processing engine automatically extracts and processes native files for ingestion into the platform, obviating the need for a template during the ingestion and processing steps.</p> <p>Everlaw automatically recommends field mapping for the most common metadata fields during a processed data upload. An Everlaw user can customize this field mapping and save it as a template. Additional details on the most common metadata fields that Everlaw will detect and map are located at https://support.everlaw.com/hc/en-us/articles/208407963-Standard-Fields</p> <p>Everlaw allows for multiple production protocols to be created that can be templated across cases, including SEC and DOJ compliant protocols. The protocol (or template) allows users to retain commonly selected options from the production wizard. Please refer to the response to 4.1.6.2 below for additional information regarding the Everlaw production wizard.</p>
4.1.2.15	The system must be able to securely transfer ESI to the review tool.	<p>▼ As mentioned in the response to 4.1.1.11.3 above, Everlaw customers' data is encrypted, whether it is in transit or at rest. We use hybrid encryption techniques that constitute software-based encryption, hosting solutions (AWS), and self-encrypting drives to align with NIST Special Publication 800-53.</p> <p>Encryption In Transit: Everlaw serves application data using HTTPS to ensure encryption in transit of all</p>

Req #	Requirement	Everlaw Solution
		<p>customer data. The Everlaw application uses Transport Layer Security (TLS) version 1.2 or higher to protect HTTPS communications. For email security, our platform leverages opportunistic TLS encryption (OE) by default.</p> <p>Encryption At Rest: Everlaw leverages the default encryption-at-rest provided by AWS, which protects the data on disk with AES-256 encryption. We also configure all snapshots to encrypt backup data. Additionally, Everlaw encrypts data at rest using AES-256 to secure inactive data stored on any device or network.</p> <p>Please refer to the Security Details section of this document for additional information.</p>
4.1.3 Review - ediscovery System		
4.1.3.1	The system must allow users to review and analyze ESI productions.	<p>▼ Everlaw accepts industry standard load file formats for loading previously processed / production data (.DAT and .OPT), as well as .CSV or .TXT files with consistent delimiters. In addition, Everlaw can load .PDF productions that lack load files and maintain their bates numbering in the system (assuming the files are named after their bates number).</p>
4.1.3.2	The system must allow users to identify and remove duplicate documents and data.	<p>▼ As mentioned in the response to 4.1.2.8 above, Everlaw's native uploads offer the following Hash-based deduplication options: global, within-custodian, none. Upload deduplication always respects families (i.e. does not deduplicate attachments that are part of different families) and automatically populates "all custodians" and "all file paths" fields to maintain a record of all deduplicated documents for production.</p> <p>For documents not deduplicated in a native upload, Everlaw offers search-based deduplication and a review window duplicates view to identify duplicates.</p> <p>Since duplicate emails stored in different email clients often have different Hash values and so are notoriously difficult to deduplicate, Everlaw includes a proprietary email threading deduplication tool (turned on by default) allowing the identification of email duplicates with different hashes after upload.</p>
4.1.3.3	The system must allow users to redact and highlight portions of the document.	<p>▼ Everlaw offers a variety of redactions that will help streamline the review process, including but not limited to:</p> <p>/ Box redactions that are drawn over a specific area</p>

Req #	Requirement	Everlaw Solution
		<ul style="list-style-type: none"> / Text selected redactions. These can be applied by highlighting various words or sentences in a PDF to redact. / Search and redact. This includes searching for specific words or phrases, use of regular expressions, built-in PII detection, and the option to redact all instances in the document. / Full/multi-page redactions / Inverse redactions / Metadata redactions can be bulk-applied on specified fields for any set of documents. Text metadata fields will receive any specified endorsement (redaction stamp) in the production loadfile; other metadata fields types (e.g. number, date/time) will remain blank. If a user draws a redaction box over email header metadata, Everlaw will automatically detect that that metadata is intended for redaction and will prompt the user to deselect (if desired) any corresponding document metadata fields automatically identified for metadata redaction, saving the user considerable time (no need to manually redact metadata fields when redacting email headers). / Native spreadsheet redactions, including cell, cell block, row, column, and sheet redactions. Redacting a cell automatically gives the user options to redact all dependent cells. Redact all cells in a document that contain a specified term or phrase. Native spreadsheets are produced as redacted natives to maximize ease of use. / Native audio/video redactions, which can be applied either to the transcribed text that is generated or by specifying time ranges to be redacted. / Batch redactions, i.e. applying mass redactions across a given set of documents from the results table. Redact one or several search terms or phrases at once or existing persistent highlight

Req #	Requirement	Everlaw Solution
		<p>lists. Redact specific metadata fields. Prior to applying the batch redaction, see a report of how many documents will be redacted for each term, phrase, or metadata field.</p> <p>/ Batch redaction deletion, i.e. selectively remove redactions of certain terms, phrases, or metadata fields across a set of documents. Term or phrase redaction deletion is limited to text redactions (does not apply to drawn box redactions).</p> <p>All redactions include the option to add configurable redaction stamps (abbreviated for small redactions). In addition, Everlaw's processing will automatically create searchable, color PDF images for all documents upon ingestion (with the exception of spreadsheets and other file types that don't convert well to imaged form), which gives users the ability to apply redactions to documents as they encounter them, without the need to subsequently image on the fly. The generation and hosting of these images is free of charge, so there is no downside to clients for this approach to processing.</p> <p><u>Native Spreadsheet Redactions</u></p> <p>Obviating the need for imaging spreadsheets, Everlaw's native spreadsheet redaction tools include the ability to navigate spreadsheets in an interactive native viewer (see cell formulas, move between worksheets, etc), search for / highlight cells containing a certain term or phrase, bulk apply redactions to all such highlighted cells, and select among options for redacting auto-detected dependent formula cells (to prevent reverse-engineering of redacted values). A new, redacted "native" version will be created on production.</p>
4.1.3.4	The system must allow users to search, tag, index, and code information and provide advance search features including but not limited to keyword, Boolean, stemming, wildcard, fuzzy, proximity and other search types.	<p>▼ Everlaw's data processing engine is able to OCR and index text, extrapolate metadata for searching, and provide reporting if a document is corrupted. To optimize efficient review, Everlaw allows users to create custom tags/codes, apply them to individual documents or multiple documents via a "batch modify" action and search based upon these tags. Additionally, Everlaw offers extensive review tools, including but not limited to the ability to apply manual notes, codes and highlights, redactions, hit highlights, unitization, automatic language translation, and more advanced features such as Predictive Coding and Concept clustering.</p> <p>Furthermore, Everlaw supports keyword, Boolean,</p>

Req #	Requirement	Everlaw Solution
		<p>stemming, wildcard, fuzzy and proximity searches.</p> <p>As mentioned in the response to 4.1.2.8 above, Everlaw contains three primary search tools:</p> <p>The Search Term Report feature allows users to run lists of terms or search strings. Unique or rare functionality includes:</p> <ul style="list-style-type: none"> / high speed of running STRs / option to auto-refresh daily / per term hit reporting that additionally includes hits with family members and unique hits for each term / hyperlinked results for easy document set access / the option to search across document contents, text metadata fields (specific or all), or both / easy creation of project-wide persistent highlights from search terms / easy PDF and CSV reports for download <p>Everlaw's Instant Visual Search builder allows users to visually construct powerful searches combining terms, metadata and other document properties without the need to craft complex boolean search syntax. Unique or rare functionality includes:</p> <ul style="list-style-type: none"> / Searching for who applied codes at custom date-time ranges / Efficient email metadata search option to select a Contact, which automatically includes all email addresses associated with the contact name. / Efficient "Parties" and "Recipients" metadata search terms that combine email metadata fields. / Deduplication options (within search, project wide, remove non-inclusive documents from email threads while deduplicating) / Step-by-step deduplication and grouping reporting prior to running a search

Req #	Requirement	Everlaw Solution
		Everlaw's Data Visualizer allows users to interactively visualize and filter documents on dozens of document properties, metadata fields, and review values and convert those filters into searches. Filters can be combined. Results can be exported to CSV. Email contact fields are filterable by domain, contact name, and/or email address. The File Path view allows users to explore documents' original folder structure.
4.1.3.5	The system must process searches, display documents, and allow users to perform document review with minimal loading times.	<p>▼ Everlaw has benchmarked our processing speed throughput at rates as high as 900,000 documents/hour. This process is inclusive of all native data processing, metadata extraction, and PDF image generation. Documents are processed and PDF-imaged upfront, meaning that there is next to zero latency when moving from doc-to-doc.</p> <p>Everlaw expects our search and document load speeds to be among the fastest available on the market for all sizes of documents and document sets.</p>
4.1.3.6	The system must include a file viewer that easily and quickly opens files without needing to install additional applications. Supported files must include: .docx, .xlsx, .pdf, .jpg, .jpeg, .mov, avi, .rtf, .txt., pub, .pptx.	<p>▼ Everlaw users can view any document in its native, text, or PDF image format (where any of these exist for a document), and any of these files can be downloaded on the fly as needed. However, review in Everlaw is optimized for review in the searchable PDF image view, which allows for advantages like rapid loading, hit highlighting, and immediate mass redaction across the vast majority of common file types. Everlaw also has proprietary native spreadsheet and native media (audio/video) viewers for optimized review of those file types.</p> <p>Please refer to https://support.everlaw.com/hc/en-us/articles/360026908431-Supported-Native-Data-Types for the list of supported native data types within Everlaw.</p> <p>As mentioned in the response to 4.1.1.6, no 3rd party applications, licences, or plug-ins are required to access and use the Everlaw Platform.</p>
4.1.3.7	The system must support searching on tags/codes and metadata.	<p>▼ Users can search on document contents, tags/codes, or any available metadata fields and save results in one or more binders (folders) in Everlaw.</p> <p>Please refer to https://support.everlaw.com/hc/en-us/articles/205466935-Searching-Categories-Codes-and-Annotations-notes-highlights-redactions and https://support.everlaw.com/hc/en-us/articles/205466875-Searching-Metadata for</p>

Req #	Requirement	Everlaw Solution
		additional information.
4.1.3.8	The system must allow the user the option to assign and self-assign batches for review.	<p>▼ Everlaw's Assignments functionality provides the ability to create one-off batch or automated workflows for users. A user with the necessary permissions to assign work (either to themselves or to other users) is able to create an assignment either from the home screen or after a search has returned results. The user simply needs to follow a wizard-driven workflow to assign the set of documents to the reviewer and opt to make the assignment either "static" or "dynamic". The "static" assignment restricts the assigned data set to documents either assigned as part of the creation of the workflow or those manually appended to the assignment thereafter. "Dynamic" assignments will automatically pull in documents as they are added to the system or when they match the designated criteria (for example, the assignment could pull from documents that have high prediction scores associated with them using Everlaw's predictive coding). These setups can further be templated across projects for easy reuse.</p>
4.1.3.9	The system must provide search engines that support both Elasticsearch and dtSearch indexing and searching options within a single matter.	<p>▼ Everlaw utilizes Lucene. Most, but not all, dtSearch search syntax is supported for automatic conversion into Lucene search syntax within Everlaw. Boolean Search terms, proximity search and nested proximity search terms are supported. The W/P, W/S, PRE, XFIRSTWORD and XLASTWORD search terms are not supported.</p>
4.1.3.10	The system must allow the user to create workspaces, folders, etc., for customizable document organization.	<p>▼ Each Everlaw matter is organized by project or matter, selectable from a drop-down menu at the top of the screen.</p> <p>Everlaw supports foldering/binding and subfoldering. Every project within Everlaw has it's own homescreen, which is unique to every user. The homescreen is made up of columns and cards. Columns are related to functionality within the platform (Assignments, Searches, Binders, Storybuilder, and Document Sets), and Cards, which are work product that fall under those columns.</p> <p>Users can create folders on their personal homescreen on a per project basis that allows them to store any combination of cards in them. While these are private by default, they can instantly be shared with other users. When sharing, permissions are customizable.</p> <p>Binders can be thought of as folders of documents.</p>

Req #	Requirement	Everlaw Solution
		<p>Binders are static tags, similar to codes that are applied to documents, except that a code is applied to a document (e.g. Responsiveness) where a Binder may represent a collection of documents comprised of several codes. Binders are also private by default until shared. When sharing, permissions are customizable.</p>
4.1.3.11	<p>The system must provide full administrator rights to the customer, including the ability to assign roles/permissions, create review assignments and/ or review batches for reviewers.</p>	<p>▼ Everlaw is a fully self-service platform and Everlaw's customers are empowered to manage all aspects of the platform. Everlaw's support team is available to assist with any questions that arise when using the platform.</p> <p>Everlaw's role based access controls allow Everlaw's customers to finely control their access to individual projects and elements within those projects, including individual document level access within each project.</p> <p>As mentioned in the response to 4.1.3.8 above, Everlaw's Assignments functionality provides the ability to create one-off batch or automated workflows for users. A user with the necessary permissions to assign work (either to themselves or to other users) is able to create an assignment either from the home screen or after a search has returned results. The user simply needs to follow a wizard-driven workflow to assign the set of documents to the reviewer and opt to make the assignment either "static" or "dynamic". The "static" assignment restricts the assigned data set to documents either assigned as part of the creation of the workflow or those manually appended to the assignment thereafter. "Dynamic" assignments will automatically pull in documents as they are added to the system or when they match the designated criteria (for example, the assignment could pull from documents that have high prediction scores associated with them using Everlaw's predictive coding). These setups can further be templated across projects for easy reuse.</p> <p>Review progress can be monitored from the assignments group dashboard, which tracks the overall progress of the entire assignment group as well as progress by individual reviewers within the group.</p>
4.1.3.12	<p>The system must allow for the customization of coding panels.</p>	<p>▼ Everlaw allows for detailed coding layout customization, including</p> <ul style="list-style-type: none"> / the inclusion / exclusion of tool icons: zoom and orientation options, text selector, text wrapping, highlight, redact, undo, share, download, print, add to Storybuilder, processing status, document

Req #	Requirement	Everlaw Solution
		<p>access log)</p> <ul style="list-style-type: none"> / the inclusion / exclusion of "tabs": Codes, Coding Presets, Metadata, Hit Highlights (custom, search, and persistent highlight hits, redact all), Annotations (add notes, view and jump to highlights and redactions), Language and translation, Document History, Predictive Coding weighting / grouping tabs into tab groups for optimal access / expanding and collapsing a tab group for easy focus on a single tab / the inclusion / exclusion and ordering of fields within a single tab, for example displaying priority coding categories and codes at the top of the Codes tab / custom keyboard shortcuts (Coding Presets) for common combinations of codes, enabling very fast review <p>Users can share their saved layouts, Project Administrators can set or change default layouts for a project, and Assignment Administrators can set or change default layouts for assignment batches.</p>
4.1.4 Advanced Analytics - ediscovery System		
4.1.4.1	The system must include the following content & context analysis capabilities: topic clustering, email threading, near-duplicate analysis, entities recognition.	<p>▼ Topic Clustering</p> <p>Everlaw's clustering, based on a tf-idf calculation, can be accessed in review and via an interactive cluster graph. In review, users can find and review the most conceptually similar documents to the current one via the context panel on the left. The multifunction cluster graph</p> <ul style="list-style-type: none"> / displays down to the document level (including individual document viewing) / includes the ability to drill down into subclusters (up to five levels) / incorporates a search interface to narrow down visible documents and clusters / displays top ten cluster-defining terms and customizable data visualizations for selected

Req #	Requirement	Everlaw Solution
		<p>clusters</p> <ul style="list-style-type: none"> / allows fast, one-click access to the documents list for selected clusters to enable easy assignment or review / allows color layering of predictive coding scores or coding decisions onto clustered documents to spot trends and anomalies, aiding review prioritization or quality control / is supported for up to 25 million documents. <p>Everlaw's Clustering visualizes documents in a dataset by conceptual similarity, empowering users to find documents by concept. It generates insights about concepts in documents without requiring any user input (though users can specify which documents to include in clustering). On the cluster map page, users can input a term and all clusters with that term as a top-three cluster-defining term will automatically be selected and can easily be opened for review. In the Review Window, users can also see and navigate through the documents most conceptually similar to the document in view, or open them all as a search in a new Results Table.</p> <p>In the cluster map documents are represented as a dot / data point, and each document belongs to a document cluster of the same color with a conceptual-space-defining polygon. The cluster-defining terms associated with each cluster can give the user an understanding of the concepts within the documents, and users can drill down into multiple levels of subtopics / subclusters. Users can layer on color coding to see things like reviewer coding consistency across a cluster, or the predictive coding model's relevance scores for documents in the cluster. This can be valuable information for prioritization and quality control.</p> <p>Everlaw also offers the ability to filter the cluster map by a wide variety of search options, and to select clusters and visualize properties such as custodians, date ranges and file types within that cluster from a histogram on the right hand panel of the screen.</p> <p><u>Email Threading and Near-duplicate Analysis</u> Email threading and near duplicate analysis occurs automatically every time documents are added to a</p>

Req #	Requirement	Everlaw Solution
		<p>project. Both are displayed for a document in the context panel of the Review Window. Non-inclusive documents can be removed from threads. Near duplicates will display down to 95% similarity.</p> <p>For additional information on email threading, please refer to https://support.everlaw.com/hc/en-us/articles/360001906052-Email-Threading-and-Reviewing-Emails</p> <p><u>Entities Recognition</u></p> <p>When data is uploaded, Everlaw automatically identifies all email addresses and their associated names (e.g. “Shelley Corman <shelley.corman@email.com>”) as individual contacts. This information is then stored as searchable email metadata. From this data, Everlaw compiles what we refer to as entities — collections of one or more contacts tied to an individual. For two contacts to be grouped into an entity, there must be at least one email address that is associated with both contacts. Everlaw matches words shared between contacts while also taking into consideration common non-name words to prevent incorrect grouping.</p> <p>Entities can be used throughout the platform, such as when using email search terms (e.g. From, To, Cc, Bcc, Recipients, Parties) and Data Visualizer.</p>
4.1.4.2	The system must provide predictive coding, advanced artificial intelligence (AI) and Technology Assisted Review (TAR) technologies including TAR 1.0 and TAR 3.0.	<p>▼ Everlaw utilizes TAR 2.0 technology for Predictive Coding based on term frequency inverse document frequency (tf-idf). Models are set up in three quick steps, with options for custom review and relevance criteria and documents to exclude from the model. Prediction scores will populate as soon as 200 documents have been coded (with at least 50 in both of the binary decision categories for the model). Models can be improved by using a unique coverage graph and / or weighted terms to train the model. Model performance can be measured against a holdout set using Recall, Precision, and F1 scores. Everlaw also allows for Predictive Coding Models to be preserved and redeployed with our new Multi-Matter Models feature. This new feature will allow users to continue to see value from prior review work.</p>
4.1.4.3	The system must provide Active Learning (story builder with continuous active learning analytics).	<p>▼ As mentioned in the response to 4.1.4.2 above, Everlaw leverages TAR 2.0 Continuous Active Learning in an intuitive and easy-to-use predictive coding tool. Everlaw’s wizard-driven process empowers both novice and power users to quickly create predictive coding</p>

Req #	Requirement	Everlaw Solution
		<p>models based on any pertinent binary coding category. Every case in Everlaw comes with a pre-built model based on our rating system (Hot, Warm, Cold). As soon as the first 200 documents in a case have a rating applied the model becomes functional and ready to use. The predictive coding dashboard provides users with a clear menu of tasks to perform to optimize and leverage the model. Everlaw's predictive coding can be applied to a variety of use cases, including surfacing the most relevant predictions or helping to ensure quality control in a collaborative document review.</p> <p>Storybuilder, Everlaw's narrative building toolkit, allows review teams to seamlessly move between their review and post-review workflows. All Storybuilder capabilities and tools can be used via a single object called a Story. Within a Story, relevant documents and testimony from deposition transcripts can be labeled by people, critical events, or other relevant issues related to the case via a Timeline view. You can also prepare for a deposition or presentation by creating a Deposition in Everlaw, or a Draft that lives as a separate collaborative tool for written work product.</p> <p>Within Storybuilder, users can create depositions and drafts in which exhibits may be embedded/linked within the line of questioning. Exhibit lists can also be exported directly from here as well. Exhibits received afterwards can also be imported and linked directly to transcripts. Everlaw is capable of synchronizing the videos and transcripts of depositions together to allow for seamless review.</p>
4.1.5 Security - ediscovery System		
4.1.5.1	The system must provide secure authorized access and have multi- factor authentication for each user to prevent unauthorized access.	<p>▼ Everlaw's security posture is a core part of the business, as one of the first ediscovery platforms to achieve FedRAMP Moderate authorization (sponsored by the US DOJ). Everlaw offers MFA as requested. Please refer to the Security Details section of this document as well as https://www.everlaw.com/security/ for additional information.</p>
4.1.5.2	The systems must provide automatic session termination if no activity with a prescribed period of time.	<p>▼ Project Administrators will be automatically logged out after 15 minutes of idle time. All other users will be automatically logged out after 30 minutes of idle time.</p>
4.1.5.3	The system must allow a client administrator to restrict security rights at the individual, group or role level.	<p>▼ Everlaw utilizes Role-Based Access Control (RBAC) for access to projects and functionality.</p> <p>Within the platform, Everlaw uses group-based security to control access to projects and permissions. The</p>

Req #	Requirement	Everlaw Solution
		<p>Project Administrators will have the ability to create security groups (such as Administrators, Project Manager and Reviewer) and customize these groups' security down to individual document or code levels. There can be multiple Administrators or "Managers" on projects if needed. Customers will have full control over which users have access to any project.</p> <p>Project permissions control access to features and tools within projects. These tools include codes, assignment groups, and Storybuilder objects (e.g., Depositions, Drafts). By contrast, the permissions governing document uploads, document deletions, and project creation are called database permissions. All Everlaw users belong to one or more permission groups, controlled by the Organization Administrator(s). If a user is in multiple groups, their permissions will be a combination of both groups' permissions, always favoring the least restrictive permission option. The database administrator controls database permissions for user groups. Those groups feature role-based access controls and each group can be configured to give the appropriate access to platform features as well as specific documents within a project.</p>
4.1.5.4	The system must provide a security level that allows system administrators to add new users to the system and edit existing user permissions.	<p>✓ Any number of new users may be added to the system at any time by system admins, and existing user permissions can be modified in the admin dashboard. Please refer to the response to 4.1.5.3 above for additional information regarding RBAC in Everlaw.</p>
4.1.5.5	The vendor must provide regular maintenance including new releases and updates.	<p>✓ Everlaw operates on a standard 4 week release schedule for planned releases, which deploys the newest version of Everlaw to all users and typically results in less than 30 minutes of downtime for users. When significant issues require urgent off-cycle resolution, Everlaw may initiate a hotfix which results in a short period of downtime for end users. Users are alerted to any upcoming releases by an in-platform banner, and can choose to receive email notifications as well.</p>
4.1.5.6	The system must provide at least 256-bit encryption to the data when at rest and in transit.	<p>✓ As mentioned in the response to 4.1.1.11.3 above, Everlaw customers' data is encrypted, whether it is in transit or at rest. We use hybrid encryption techniques that constitute software-based encryption, hosting solutions (AWS), and self-encrypting drives to align with NIST Special Publication 800-53.</p> <p>Encryption In Transit: Everlaw serves application data using HTTPS to ensure encryption in transit of all</p>

Req #	Requirement	Everlaw Solution
		<p>customer data. The Everlaw application uses Transport Layer Security (TLS) version 1.2 or higher to protect HTTPS communications. For email security, our platform leverages opportunistic TLS encryption (OE) by default.</p> <p>Encryption At Rest: Everlaw leverages the default encryption-at-rest provided by AWS, which protects the data on disk with AES-256 encryption. We also configure all snapshots to encrypt backup data. Additionally, Everlaw encrypts data at rest using AES-256 to secure inactive data stored on any device or network.</p>
4.1.6 Production - ediscovery System		
4.1.6.1	The system must provide production of the ESI in a variety of formats including as searchable PDF, native or images and text with a load file.	<p>▼ Everlaw's standard production format produces native, text, and/or image (color PDF, black-and-white TIFF, or b&w TIFF with subset in color JPG) files for every document, grouped into corresponding native, text, and image folders. Standard productions are also accompanied by DAT, OPT, LST, LFP, and DII metadata loadfiles. This production format is best handled by an ediscovery platform.</p> <p>Everlaw additionally enables non-standard productions for easy offline review by providing document export options for produced documents, including:</p> <ul style="list-style-type: none"> / export to searchable PDF, with options to include slipsheets with select metadata / export to ZIP (image, text, and/or native files) with native filenames options (Bates number, original filename, or both) and loadfile and work product CSV options / export to CSV for configurable metadata and/or coding and work product reports
4.1.6.2	The system must have a wizard-driven production process.	<p>▼ Everlaw's production wizard contains seven steps which allow users to customize everything needed in a production, including:</p> <ul style="list-style-type: none"> / Bates number - prefix, padding, page-level vs document level numbering (suffixing for pages) / Image formats (PDF, TIFF, TIFF with color JPG subset) along with location of various endorsements (metadata, code, custom)

Req #	Requirement	Everlaw Solution
		<ul style="list-style-type: none"> / Inclusion of redactions, native files (options to designate subsets of documents, add endorsement to filename, and strip attachments from email parents), and/or text (including audio transcriptions created by Everlaw) / Withholding of privilege documents and privilege placeholder configuration / Placeholder configuration for documents produced in native / Load file creation and customization (options to rename fields, combine text fields, combine or separate date and time fields, and include code, code category, and freeform code fields, and empty / custom fields) / Built-in privilege log creation and customization, including different field inclusion for withheld vs redacted documents / Packaging: folder naming and encryption / ZIP file encryption options (none, AES-256, ZipCrypto) <p>Everlaw productions include an automated check of twenty common production mistakes with easy options for addressing or ignoring document inclusion warnings (e.g. broken families) and configuration warnings (e.g. missing privilege rule). Productions can be modified by altering the production configuration and rerunning the production for some or all documents, with the option to rerun only metadata. Virtually all settings can be changed and rerun for an existing production except Bates numbering. Production modifications automatically identify documents for clawback. Each production includes a history of configurations and downloadable ZIPs for each rerun modification. Each production includes options for direct download, download via SFTP, and sharing via link or emailed link. Each production includes access logs for both in-platform downloads and downloads via shared link.</p>
4.1.6.3	The system must have self-service production capabilities to allow the user to prepare and export from start to finish/download.	<p>▼ Everlaw is fully self service. However, Everlaw's customer success rep will be available to assist users as needed with any production workflows. Please refer to the response to 4.1.6.2 above for additional</p>

Req #	Requirement	Everlaw Solution
		information.
4.1.6.4	The system must allow the user to view all productions for a single file in the review platform.	<ul style="list-style-type: none"> Everlaw maintains a record of all past productions which can be viewed as needed.
4.1.7 Professional Services and Training - ediscovery		
4.1.7.1	The vendor must provide live training (which may be virtual).	<ul style="list-style-type: none"> All training, live or virtual, is unlimited and is included at no extra cost with an Everlaw agreement. Please refer to the Training Plan section of this document for additional information.
4.1.7.2	The vendor must provide reviewer training and client administrator/ organization administrator training.	<ul style="list-style-type: none"> Everlaw offers a wide range of training options, including reviewer training and project admin/org admin training, available either as recorded sessions, virtual sessions, or in-person training as desired. Please refer to the Training Plan section of this document as well as https://www.everlaw.com/training/ for additional information.
4.1.7.3	The vendor must record live training and provide recorded training to the client at no additional cost.	<ul style="list-style-type: none"> As mentioned above in the responses to 4.1.7.1 and 4.1.7.2, Everlaw provides live training and recorded training as needed at no additional cost. Everlaw takes no issues with recording these live training sessions as desired by the Agency.
4.1.7.4	The system must provide access to a knowledge base or help center, technical documentation, and online support resources.	<ul style="list-style-type: none"> Everlaw has a dedicated Knowledge Base portal (https://support.everlaw.com/hc/en-us), which includes documentation on all features/functionality in the platform, links to video walk throughs, technical documentation and release notes for all platform updates. <p>Everlaw's support and training can be accessed online. Please refer to https://www.everlaw.com/customer-resources/ for information regarding Everlaw technical support. Please refer to https://www.everlaw.com/training/ for information regarding Everlaw's training.</p>
4.1.7.5	The vendor must provide support services for the initial setup.	<ul style="list-style-type: none"> Everlaw is fully committed to assisting the Agency with deployment, including offering data migration assistance at no additional charge. Please refer to the Everlaw Implementation and Support section of this document for additional information.
4.1.7.6	The vendor must provide support services for the duration of the contract for ongoing maintenance.	<ul style="list-style-type: none"> Everlaw provides support throughout the duration of an Everlaw agreement for ongoing maintenance as well as
4.1.7.7	The vendor must offer client services support including project management and technical	<ul style="list-style-type: none"> Everlaw's Customer Success team, included at no additional charge, partners with clients throughout the

Req #	Requirement	Everlaw Solution
	support services.	<p>engagement, offering strategic guidance on best practices, workflow optimization, and implementation planning. For large-scale or complex matters, Everlaw's support ensures smooth onboarding, data migration, and workflow configuration tailored to client needs.</p> <p>Please refer to the Everlaw Implementation and Support and Training Plan sections of this document for additional information.</p>
4.1.8 Support - ediscovery		
4.1.8.1	Support by telephone, online, in-app, and email 24 hours-a-day, 7 days-a-week, 365 days-a-year for troubleshooting technical issues	<p>▼ Everlaw offers support via telephone, online, in-app and email during the following times:</p> <ul style="list-style-type: none"> / Monday – Friday from 9am – 1am ET (via phone, support tickets, in-platform) / Saturday & Sunday from 9am – 1am ET (via support tickets and in-platform) <p>Please refer to https://www.everlaw.com/customer-resources/ for additional information.</p>
4.1.8.2	A response time of a minimum of 1 day to request for technical support.	<p>▼ Everlaw maintains 4 severity levels for support requests with robust definitions describing each one. Those severity levels are:</p> <ol style="list-style-type: none"> 1. Critical/S1 for those issues that render the system inoperable or create risks of breaching known regulations and may cause legal consequences, security issues, login problems. 2. High/S2 for those issues that cause significant impact to product functionality and other widespread issues with no known resolution. 3. Medium/S3 for those issues that impact user experience and platform performance and sub-features. 4. Operational/S4 for those issues that have little or no business impact, such as enhancement requests or cosmetic issue <p>Our SLAs for response time are:</p> <ul style="list-style-type: none"> / Severity 1: response time of 30 minutes / Severity 2: response time of 60 minutes (within

Req #	Requirement	Everlaw Solution
		<p>support hours)</p> <p>/ Severity 3: response time of 2 hours (within support hours)</p> <p>/ Severity 4: response time of 4 hours (within support hours)</p> <p>Our SLAs for resolution time are:</p> <p>/ Severity 1: 8 hours (most are resolved in a few minutes)</p> <p>/ Severity 2: end of next business day</p> <p>/ Severity 3: next scheduled release cycle (releases generally every four weeks)</p> <p>/ Severity 4: at Everlaw's discretion</p>
4.1.8.3	Access to knowledgebase, technical documentation, and online support resources.	<p>▼ As mentioned in the response to 4.1.7.4 above, Everlaw has a dedicated Knowledge Base portal (https://support.everlaw.com/hc/en-us), which includes documentation on all features/functionality in the platform, links to video walk throughs, technical documentation and release notes for all platform updates.</p> <p>Everlaw's support and training can be accessed online. Please refer to https://www.everlaw.com/customer-resources/ for information regarding Everlaw technical support. Please refer to https://www.everlaw.com/training/ for information regarding Everlaw's training.</p>
4.1.9 Billing - ediscovery		
4.1.9.1	Vendor will round up to the nearest next whole gigabyte (GB) for billing and auditing purposes. (Example 1.2GB will be billed at 2.0 GB)	▼
4.1.9.2	Vendor will invoice monthly and bill at the maximum gigabyte (GB) capacity used by the state.	▼
4.1.9.3	Vendor's proposed solution must provide billing capabilities designed to simplify the procedures of a chargeback model, as well as provide a holistic view of service. The state desires the billing detail to include but not be limited to billing by agency, consumption usage by each agency.	▼
4.1.10 Software as a Service Addendum		

Req #	Requirement	Everlaw Solution
4.1.10.1	Vendor must sign the attached Software as a Service Addendum prior to award.	▼ Please refer to <i>[Everlaw Response] Software as a Service Addendum</i>
4.1.11 Optional Renewals		
4.1.11.1	Vendor will include in their bid the cost of optional Annual renewals for years 2, 3, and 4. These optional Annual renewals will be initiated on Agency request authorized under the authority of the Purchasing Division.	▼ Please refer to <i>[Everlaw Response] Exhibit A - Pricing Page</i>

Additional Everlaw Solution Highlights

Exception reporting

Everlaw will flag any documents where an exception occurred during processing. This is displayed both in the post processing report, as well as in a special field that can be searched and displayed in the document list screen. How exceptions are handled will naturally vary on a case-by-case basis (such as dealing with password protected documents, where such documents can be reprocessed in platform assuming the correct password is obtained).

Email/text/instant messenger threading

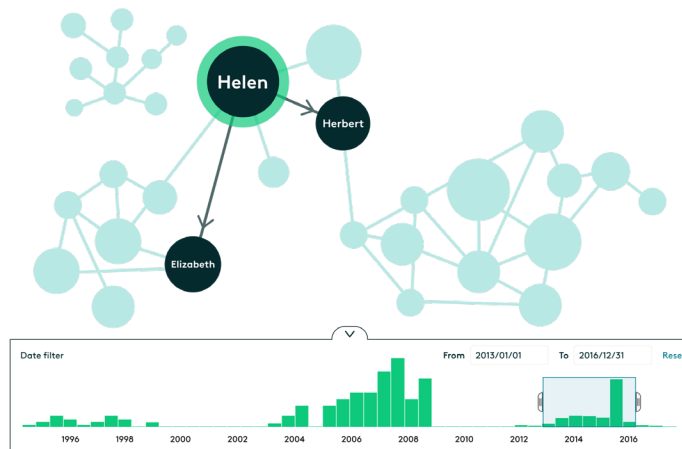
Everlaw's processing performs email threading automatically upon ingestion. This includes both the ability to search for only the most inclusive email in a thread, as well as the ability to display on the most inclusive email(s) from within the review window.

Everlaw automatically processes short message format documents including text messages, iMessage, MS Teams, Slack, tweets, Bloomberg Messages, Instant Bloomberg, instant messages, etc. Conversations are segmented into documents for review (e.g. by 24 hour period) and rendered in near-to-original PDF and native views for user-friendly review, allowing reviewers to see who was talking to whom and in what context. Threaded messages are kept together (e.g. for Slack data), and emojis and reactions are preserved and searchable. For mobile devices, Everlaw supports native uploads of Cellebrite UFDR files and automatically creates near-to-original text message and chat documents for review. In addition, significant native chat improvements currently in active development will include the abilities to search at the message level, automatically scroll from segment to segment for seamless conversation review, create filtered views within a segment by author(s), keyword(s), etc., and produce only desired messages, further enhancing review and production.

Communication Visualizer

Everlaw's Communication Visualizer is an interactive and filterable network graph of email addresses, domains, and names that helps users gather insights into communication patterns, understanding who

was communicating with whom, with what frequency, and how those communication patterns evolved over time.



Generative Artificial Intelligence (GAI)

Everlaw is excited to introduce its Generative AI functionality, Everlaw AI Assistant, which is designed to enhance the efficiency and accuracy of legal workflows. Now available for general release after a full year of Beta testing with live clients, this advanced feature leverages state-of-the-art AI technologies to streamline document review, automate routine tasks, and generate insightful summaries of complex case materials. By integrating Generative AI into our platform, we aim to provide users with powerful tools that not only accelerate case preparation but also support strategic decision-making with AI-driven insights. This innovative functionality is a key addition to Everlaw's suite of ediscovery solutions, reinforcing our commitment to delivering cutting-edge technology to our clients.

Everlaw firmly believes that AI, and Generative AI in particular, will change the landscape of how legal professionals are using tools like Everlaw in the near future. Please refer to the following article regarding our Gen AI offering: (<https://www.everlaw.com/product/everlaw-ai-assistant/>).

Additionally, please refer to the following article regarding Everlaw's Generative AI Principles: www.everlaw.com/blog/ai-and-law/generative-ai-principles/.

Native format viewing including emojis

Everlaw renders chat data in a form that approximates their appearance in their native applications (time stamped, text bubbles color-coded by user, emojis, etc), as well as extracting relevant metadata, such as chat participants, start date, end date, and application. Please refer to the [Email/text/instant messenger threading](#) section of this document above for further information regarding native format viewing of chat formats.

Translation capabilities

Everlaw automatically detects Non-English languages upon upload. Project admins can select the languages they wish to be searchable for their users, or these settings can be included in project templates. Common latin-based and CJK languages are automatically detected for OCR, while other languages can be specified by the user (e.g. Cyrillic-based languages, Arabic). Non-English language characters, words, and phrases are searchable. Reviewers can also instantly translate a document into English via Everlaw's secure, in-region integration with AWS Translate.

Legal Holds

Through Everlaw's legal hold notification features, the Agency can make legal holds simple, bolster your defensibility, and proactively mitigate risk. Everlaw's legal hold feature allows users to either add custodians manually or integrate with their organization's Active Directory to identify and pull in custodian information.

The Agency can issue holds to custodians to preserve potential evidence quickly, confidently, and reliably with a simple and straightforward user interface. The feature provides the Agency with the ability to create custom hold templates, send notifications to custodians, track custodian acknowledgment of legal holds, reissue periodic reminders, as well as escalate holds to managers. All correspondence relating to legal holds within Everlaw is preserved, including the hold notice, any acknowledgement, any automated reminder or escalation and the notice of the removal or release of the hold. This information is retained even after the release of the hold. Everlaw's Legal Hold tool is fully integrated with the rest of the platform at no additional cost, helping the Agency avoid legal software fragmentation.

Additionally, Everlaw supports Microsoft Office 365 collection including Outlook, OneNote, Teams, and Calendar data by both custodian and/or date range. During processing, the initiator can select to associate the collected or uploaded data with a particular custodian under legal hold. The legal hold dashboard will then update automatically to reflect the number of documents uploaded to Everlaw that are linked to the custodian. All data will be preserved in our system until a user with the appropriate permissions performs deletions or the matter is closed.

Furthermore, Everlaw has the ability to issue silent holds with Preservation-in-place for Microsoft 365. Users with the proper permissions can create, track, and release Microsoft Purview holds on custodian data within Everlaw via Microsoft 365 cloud connector. These new preservation-in-place objects are displayed alongside hold notices pertaining to the same matter, without ever having to leave the Everlaw platform.

Tagging/Coding

Everlaw allows users to create custom tags, apply them to individual documents, and search based upon these tags. Tags can be created at the project level or on the fly during review by users with the appropriate permissions. Multiple documents can be bulk tagged or otherwise modified via a "batch

modify" action. Specific documents within the Results Table can be deselected / reselected to further specify which documents should receive a bulk action. Additionally, tag(s) assigned to documents are visible in the review window (list of documents in the project or search) and are fully visible without having to open the document.

Storybuilder

Storybuilder, Everlaw's narrative building toolkit, allows review teams to seamlessly move between their review and post-review workflows. All Storybuilder capabilities and tools can be used via a single object called a Story. Within a Story, relevant documents and testimony from deposition transcripts can be labeled by people, critical events, or other relevant issues related to the case via a Timeline view. You can also prepare for a deposition or presentation by creating a Deposition in Everlaw, or a Draft that lives as a separate collaborative tool for written work product.

Within Storybuilder, users can create depositions and drafts in which exhibits may be embedded/linked within the line of questioning. Exhibit lists can also be exported directly from here as well. Exhibits received afterwards can also be imported and linked directly to transcripts. Everlaw is capable of synchronizing the videos and transcripts of depositions together to allow for seamless review.

Review Workflows

Everlaw's integrated and flexible platform provides case teams with an array of simple and effective ways to organize and conduct review within the platform. There are countless ways that workflows can be customized to fit the needs of each individual team. Permissions in Everlaw are administered by group and workflow administrators can establish permission groups for each level of review (such as first level review or QC) and tailor the rights of those groups to just those functionalities of the platform required for users to perform their designated tasks. Everlaw's assignment group feature can be used to create assignments for individual users, or groups of users, based on the static or dynamic criteria determined by the workflow administrator. Any search or binder created within Everlaw can be shared with one or more users in Everlaw, as a way to identify document subsets for review. A set of binders, assignment groups, assignment batches, and/or searches can further be grouped together / categorized in shareable "Folders." Everlaw supports up to four layers of folders, inclusive of the top-level folder. Each folder layer can contain as many folders as desired (e.g., specific productions that can be viewed and reviewed individually). Additionally, within the document review window, the workflow administrator can create custom coding layouts for each review group or individual as required, meaning only the selected codes and information necessary for that review function would be displayed.

Everlaw also simplifies the creation of coding categories and choices, and users can easily create custom coding layouts for different review groups. Persistent highlights can be created quickly directly from a Search Term Report or from the project settings page. These highlights empower reviewers to quickly identify key terms within the review. Additionally, reviewers can perform bulk redactions on things like privilege terms or PII (which Everlaw automatically detects) directly from the results table of any search.

Within a document all instances of a term can be redacted with a click of a button and customizable stamps can be applied. Everlaw has a proprietary native spreadsheet redaction tool built directly into the platform that allows reviewers to redact spreadsheets without the need to create cumbersome Excel images. Automated email threading and near duplicate analysis gives users greater visibility into related documents, and our Non-English language translation tool helps reviewers quickly scan documents in numerous languages for relevance. Everlaw even supports audio/video files, and automatically creates searchable transcripts upon data ingestion. Analytics can be used to prioritize important documents for faster review and assignment groups can be created to provide control and visibility into the review workflow. Everlaw's innovative features make document review faster and more effective than ever. Furthermore, Everlaw offers users an inherently customizable document review experience. Finally, Everlaw's Customer Success team or Everlaw certified partners offer support and training for case teams to uncover the most effective ways to utilize the platform for their needs.

Collaboration with other Entities

Everlaw is designed to facilitate collaboration with other agencies, internal divisions, or expert witnesses in a highly secure environment. Any number of users with any email domain can be invited to the projects designated by the Agency, utilizing Everlaw's unique no-cost unlimited users policy. The Agency will then have the option to restrict their document access and other permissions in the main review project / workspace. Alternatively, Agency Project Administrators can also take advantage of Everlaw's unique, no-cost unlimited projects model to create separate partial (sub) projects / workspaces, eliminating the risk of providing complete access to the entire document corpus. Copy the desired documents into the partial (sub) projects, and invite the reviewers / users (i.e., other agencies, internal divisions, or expert witnesses) using Role-based Access Controls (RBAC). The documents loaded into a partial (sub) projects are only stored once in the underlying Everlaw database, but each project can have separate users, permissions, and work product, as well as access to Everlaw's full platform functionality. Additionally, users with appropriate rights can easily copy work product from a partial / sub project back into the main project when desired.

Furthermore, all user actions including on documents, as well as other kinds of activity are logged and auditable (e.g., login / logout, searches run, documents viewed, documents coded / tagged, downloads, document deletions, etc.). Also, project analytics tracks the amount of time each user has spent on different types of platform activities (e.g., Review time, Uploads, Production, Project Management, Storybuilder, etc.) within configurable date ranges.

Everlaw also has built-in collaboration into every element of the platform to help reduce information silos and help teams surface key information faster. Users can easily share and collaborate on everything from document review to depositions, testimony or trial preparation. In-platform messaging allows users to share documents, searches, dashboard visualizations, predictive coding (TAR) models results and custom communications securely within the platform. They will receive messages in their project inboxes, and can even set up notifications alerts in their agency email to alert them to new activity within Everlaw.

Pricing

Please refer to the attached document **[Everlaw Response] Exhibit A - Pricing Page**.

Everlaw Standard Pricing Model

Everlaw's straightforward pricing model is storage based, so clients only pay for the data they host on the Everlaw platform. Data storage pricing is tailored to the type of usage/storage needed by the client, which can include active review databases, early case assessment databases, as well as data placed in a suspended state/near line storage. Subscription options are offered on a per-matter or minimum spend basis to best align with the Agency's needs.

The Agency should expect no hidden charges from Everlaw. All of our features and functionality are fully integrated, including Advanced Data Analytics, Redactions (including A/V), Legal Holds and Processing, with no plug-ins or additional products required to gain the full benefit of the Everlaw platform, in a secure environment. To compliment our cloud-native technology, we offer unlimited users and our thoughtful onboarding, training and ongoing customer success support at no additional cost.

Everlaw AI Assistant - Generative AI Pricing

Available as an add-on to our standard annual subscriptions, pricing for EverlawAI Assistant is based on usage of credits consumed per task. Customers get started by purchasing a minimum number of credits.

Tasks available through the Everlaw Review Assistant include summarization, topic analysis, document Q&A, coding suggestions, and extractions. The Writing Assistant creates fact-based memos, outlines and lists based on the key evidence in your matter in Storybuilder.

Included Everlaw Features and Functionality

Features	Everlaw	Industry Standard
Data Migration	✓ Included	\$\$ Extra Charge
Unlimited User Licences	✓ Included	\$\$ Extra Charge
Onboarding	✓ Included	\$\$ Extra Charge
Customer Support	✓ Included	\$\$ Extra Charge
Customer Training	✓ Included	\$\$ Extra Charge
Processing and Imaging	✓ Included	\$\$ Extra Charge
Advanced Analytics	✓ Included	\$\$ Extra Charge

Features	Everlaw	Industry Standard
Predictive Coding	✓ Included	\$\$ Extra Charge
Unlimited Productions	✓ Included	\$\$ Extra Charge
Non-English Language Translation	✓ Included	\$\$ Extra Charge
Audio/Video Transcriptions	✓ Included	\$\$ Extra Charge
Post-review Case building & Deposition tools	✓ Included	\$\$ Extra Charge

Contract Manager

During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager	Joshua Harvey, Director, Customer Success - Public Sector
Telephone Number	510.390.5616
Fax Number	n/a
Email Address	joshua.harvey@everlaw.com

Everlaw Implementation and Support

Deploying and implementing a cloud-native, Software-as-a-Service (SaaS) solution takes far fewer resources and less effort from the customer than traditional on-premises deployments. Unlike on-premises applications that would require a heavy server footprint, various software licenses, necessary integrations, and a small army of IT staff that have been vetted to access the federal physical environment, with SaaS solutions all of that effort happens “as a Service” and is simply not required.

Everlaw is a FedRAMP-authorized, cloud-native SaaS solution that was introduced in 2011 with the purpose of modernizing the ediscovery market and bringing discovery into the future. To complement our modern, intuitive platform and promote a more contemporary, sustainable, self-service model, Everlaw offers custom onboarding, training, and ongoing customer success support entirely free of charge to ensure user success. We do this to disrupt the “service wrapper” that has become standard

for many ediscovery solutions and providers. We believe that services in the field of ediscovery software can have unintended negative impacts on user experience in two ways. 1) It can inhibit user empowerment and product feedback by creating extra layers of communication to navigate between the ediscovery software provider and the customer, and 2) If the customer is charged for the time spent supporting adoption of the technology, adoption and product development are both slowed. As a result, customer satisfaction and product functionality can suffer. By contrast, Everlaw's cloud-native, SaaS offering is built to empower its users and onboard them smoothly. We offer a complimentary, comprehensive package to support user success and are deeply committed to their immediate and future success on the platform, with a track record of onboarding hundreds of customers successfully, including government agencies.

We believe our unique approach to building intuitive software and pairing it with robust, personalized, free onboarding, training, and educational services will increase Agency adoption of Everlaw, and will create a stronger partnership to continuously improve our product and the services we provide to empower our customers to do more with less and maximize your return on investment. From data migrations to custom training sessions, the Everlaw team of product experts, skilled data operations managers, and seasoned ediscovery support staff are there for Agency teams every step of the way.

Technical Deployment Overview

Everlaw is a Software-as-a-Service ("SaaS") solution, which means that there will be no hardware for Agency to purchase or maintain. Built on AWS GovCloud East, the Everlaw platform can scale up or down in an instant to accommodate unlimited users, cases, and documents. As part of our FedRAMP- and StateRAMP- authorized solution, the Agency will have unique subcomponent organizations in our Government Community Cloud (where Agency will still be logically separate from all other government entities, without needing to carry the expense of a Virtual Private Cloud).

All of our customers are operating on the most up-to-date version of Everlaw. Our product team is constantly innovating and improving the platform. New features are delivered every four weeks, and automatically deploy to the platform at no cost and with no maintenance requirements. Last year alone, we released more than 230 new features and improvements to the platform to make sure our customers are future-ready and at the forefront of innovation. All of this happens quickly during non-business hours, which means that we are able to deliver this high level of innovation while still maintaining an industry-leading uptime higher than 99.5%, including scheduled maintenance. Each release is accompanied by a set of detailed release notes, and a walkthrough of the new features will appear automatically on the home page for each user so they can stay up to date on the changes. We believe innovation is critical in the ever-evolving digital landscape but should never come at the expense of user experience.

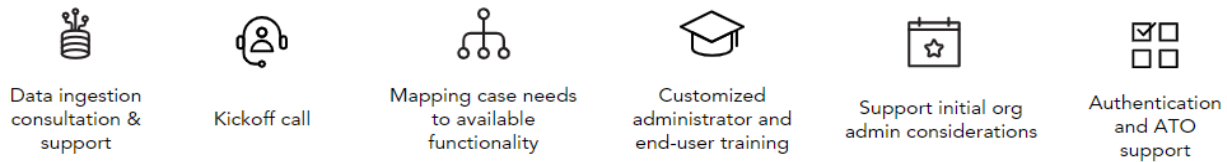
Everlaw Support Model

Everlaw provides an integrated and intuitive discovery platform. The product is so easy to use that users can perform most tasks without additional assistance. However, Everlaw will assign an experienced

Customer Success Manager (“CSM”) to this engagement, who will lead the onboarding and ongoing technical support. The Agency CSM will have the full backing and support of the company’s customer success and user education teams.

Onboarding Assistance (Complimentary)

Everlaw understands how important a good start is and wants to help lay the groundwork for a successful case. Everlaw will offer complimentary onboarding for each new Agency matter, which can include:



The Everlaw Customer Success team will engage with Agency users to understand their current case needs and map them to available functionality. The Everlaw Customer Success team will coordinate customized, objective-based training paths to help users to be Everlaw proficient as quickly as possible. As a supplement to live training, Everlaw also hosts a number of virtual standing training sessions every weekday that are free and available to anyone who would like to hop on for an introduction or refresher. At the completion of the onboarding process, Agency users should feel very comfortable navigating Everlaw and executing their required tasks.

Ongoing Training and Support (Complimentary)

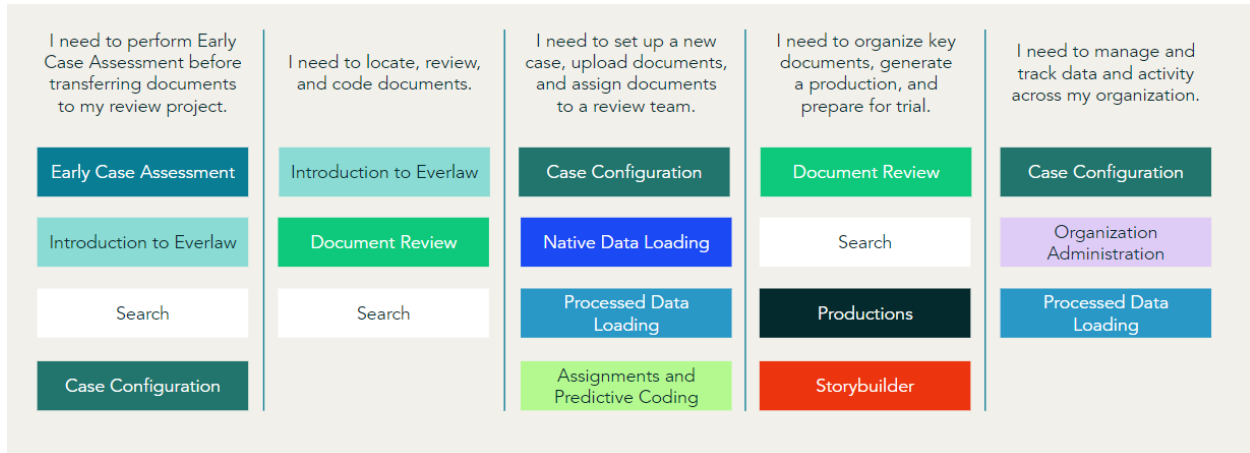
After initial onboarding, Everlaw’s Customer Success Team, led by the assigned CSM will continue to provide support to users throughout the life of the contract at no additional charge. The team will be available to help walk users through any area of the platform and answer any technical questions related to Everlaw’s various features. Agency users will always be able to quickly connect with the team via email, in-platform messaging or telephone. Additionally, the Everlaw team can work with the Agency to schedule in-person training on a case-by-case situation, depending on geographic location. Additionally, any user can attend online, standing trainings with a live instructor which are objective based and include live Q&A with Everlaw, or request a virtual training session customized to Agency needs. For detailed insights into product features and functionality, Agency users and admins can access Everlaw’s online Knowledge Base at any time, which is continuously updated with relevant and useful tips and walkthrough videos. See additional details in the draft Training Plan. Everlaw can customize the proposed training plan based on the Agency guidance and user needs.

Training Plan

Everlaw has a robust and modern training program ready to empower Agency users that includes our expansive Knowledge Base, Training Center, live and virtual live training sessions, all available at no

extra cost. We deliver our training across several channels to make our training accessible to busy legal professionals, some of whom may only need limited or short term access for an ad-hoc activity, while others may spend most of their day on the platform.

The Everlaw team will deliver a customized training program based on the Agency case team's defined objectives, which may look something like the following figure.



This objective-based approach to training includes custom onboarding live and virtual training and ongoing periodic live training sessions, scheduled to accommodate geographically dispersed resources.

On-demand Training

Everlaw's Training Center is the Agency's one stop shop for recorded training to support the office or case team training requirements and to make onboarding of new users (both Agency and outside parties) simple. Available online at any time, Agency users don't even need to log in to access the content. They can simply visit the website and follow a training path that makes sense for them. Additional training resources and the latest feature release specific videos are also available through the Training Center, to ensure users are kept constantly up-to-date with the latest features and remain "Future Ready."

Live and Virtual Live Training

Everlaw will offer unlimited custom training across Agency offices during the life of the contract, ensuring that each session has multiple times to accommodate time zones and schedules, through Everlaw's user education team.

Because it is likely that the majority of the upfront training needs will be needed based on Agency case team demand, getting users up and running on the platform our User Education team will schedule objective-based training courses and Question and Answer sessions to ensure the reviewers and system administrator are product experts and certified as needed to be successful in their roles as quickly as required.

Each week, Everlaw’s User Education team also offers a variety of free live standing training sessions designed to help any Everlaw user learn, understand, and master the Everlaw platform. These sessions cover everything from introductory sessions designed to help new users get started navigating and using Everlaw, to advanced sessions focused on specific complex features (like Predictive Coding).

Monday	Tuesday	Wednesday	Thursday	Friday
Search	Intro to Everlaw <i>or</i> Document Review	Release Training	Native Data Loading <i>or</i> Processed Data <i>or</i> Productions <i>or</i> Case Configuration	Storybuilder <i>or</i> Assignment and Predictive Coding <i>or</i> Visualizing Your Data
	Organization Administration training is offered as a private, custom session. All sessions are available as recordings and/or live custom sessions.			

On-platform Walkthroughs

Across the platform, Everlaw users have access to instant on-platform support. All Agency users need to do is click the question mark at the top of any page they are on in the Everlaw platform and a new window opens that gives them relevant articles and video tutorials to the area of the platform they are in, as well as the ability to send a message directly to our customer support team to provide answers to specific questions. Throughout this process, Everlaw’s dedicated team will be available to assist.

Training Documentation

Everlaw offers a constantly updated library of articles and videos that support our customers ongoing product understanding, we call the Knowledge Base. This library is available to all users (and non-users) and accessible online.

Training Certifications

Agency users that complete our Everlaw Certified Pro modules and pass the module exams will receive the designation of “Certified Professional” in Everlaw and provided certifications. The Agency, as an organization, will have the ability to have unlimited users go through the certification program at no additional cost, and may be a good option for Agency “train-the-trainer” interest and team member(s) who will be responsible for data management and system ownership.

Security Details

Everlaw prioritizes data security and privacy with enterprise-class security protocols and privacy standards because we understand that hosting sensitive client data on a SaaS ediscovery platform

requires an established compliance program and rigorous controls. Everlaw's security and compliance program is holistic and part of our core philosophy. It demonstrates our commitment to ethics and our company values, as well as compliance with our security, privacy, and confidentiality commitments to customers, and applicable laws and regulations. Our program is built on top of federal guidance on effective compliance programs because we believe that security, privacy, and compliance go hand-in-hand.

Everlaw's ediscovery solutions meet rigorous security, privacy, and compliance standards, and validated by third party audits.



FedRAMP
Authorized



SOC 2 Type 2
Certified



ISO
27001:2013



Cyber
Essentials Plus

Adding value for our customers

Everlaw delivers value to users instantly and scales on-demand thanks to its secure-by-design, cloud-native architecture built on Amazon Web Services (AWS) GovCloud. Security and compliance are a critical part of our core philosophy, and influence all aspects of our business, from product design and development, marketing, sales, and customer service.

Product Security Features

Everlaw has a variety of product security features. We have highlighted a few below for Agency consideration:

- / Single Sign-On (SSO): Everlaw supports single sign-on (SSO) via the SAML 2.0 protocol, allowing customers to log into Everlaw via their organization's existing LDAP or other SSO system.
- / Multi-Factor Authentication (MFA): Additionally, Everlaw offers multi-factor authentication (MFA) at no additional cost for all customer accounts, which can be enforced at the organization level. Multi-factor authentication increases your account's security by requiring a second method for logging in, such as access to your email or mobile device.
- / Granular Permissions: The ability to specify access to tools, data, and work products is crucial to secure and efficient review. On Everlaw, admins can use fine-grained permission settings to precisely grant users access to what they need to do their jobs well.

- / Analytics & Monitoring: The Everlaw Analytics page gives you a view of all user activity on your project. From here, you can monitor live and historic activity of all users on your project, as well as all administrative activity.
- / Secure In-Platform Sharing: Everlaw's in-platform project messaging allows for direct sharing and secure communication between users, enabling users to bypass the typical process of downloading and sharing documents with colleagues via email and other forms of workplace communication.
- / Flexible Sharing Options: Often, a review requires a third-party expert or co-counsel to access documents in order to complete a review project, offer an expert opinion, or manage project consultants. Everlaw users can organize, create, and share an appropriate subset of documents in a secure project, eliminating the risk of providing complete access to the entire document corpus.
- / Location Approval Lists (IP Range Blocking): With the increase of remote work, security concerns have become more top-of-mind for legal and IT professionals. Everlaw gives organizations more control over who has access to projects by allowing project admins to restrict access based on a user's IP address and country. This feature helps organizations better protect their data and, as a result, their clients.

Data Security

Everlaw customers' data is encrypted, whether it is in transit or at rest. We use hybrid encryption techniques that constitute software-based encryption, hosting solutions (AWS), and self-encrypting drives to align with NIST Special Publication 800-53.

Encryption In Transit: Everlaw serves application data using HTTPS to ensure encryption in transit of all customer data. The Everlaw application uses Transport Layer Security (TLS) version 1.2 or higher to protect HTTPS communications. For email security, our platform leverages opportunistic TLS encryption (OE) by default.

Encryption At Rest: Everlaw leverages the default encryption-at-rest provided by AWS, which protects the data on disk with AES-256 encryption. We also configure all snapshots to encrypt backup data. Additionally, Everlaw encrypts data at rest using AES-256 to secure inactive data stored on any device or network.

As part of our system of internal control and SLDC, Everlaw implements data protection and privacy by design principles. When developing a new feature or a new product, we implement the appropriate organizational and technical safeguards to ensure that personal data is only processed for a specific purpose. At Everlaw, we follow our strict information security policies and procedures encompassing the security, availability, processing, integrity, and confidentiality of our customer data.

Data Rights and Accessibility

At project kickoff, Everlaw will work with Agency to define the level of access required for technical support from Everlaw, and establish the resources needed to support the engagement. Everlaw adheres to a least privileged-based access control model. Per Everlaw policies, our government systems may only be accessed by employees who are U.S. Persons located within the United States. Any employee supporting our government customers must undergo specific training and checks before being granted access to any customer data. Even those employees who meet these qualifications must still have a specific need and request approval before being granted access to customer data. Additionally, several of our employees have active BI's or clearances with other government agencies.

Everlaw complies with NIST 800-53 and has dedicated General Risk & Compliance and Security Engineering teams who are responsible for developing and maintaining security processes and documentation. As a FedRAMP Moderate authorized platform, we regularly conduct the required testing and monitoring activities, and can provide updates to Agency as requested. Everlaw can coordinate with Agency POC should an on-site assessment be required.

Everlaw can display an Agency approved banner that warns users at logon that they are accessing a monitored government system, with no expectation of privacy. Users will be required to acknowledge this warning prior to logging into the system. All files imported into Everlaw are scanned for malicious code during processing.

Everlaw has a robust incident management program. Our incident response SLA's are as follows:

- / Severity 1: response time of 30 minutes (within support hours)
- / Severity 2: response time of 60 minutes (within support hours)
- / Severity 3: response time of 2 hours (within support hours)
- / Severity 4: response time of 4 hours (within support hours)

Resolution time depends on the root cause of the incident.

There are no user or software licenses required for Everlaw. Our pricing model is based solely on hosted data size. Everlaw asserts that all platform development performed during the execution of any customer contract remains the intellectual property of the company.

Identity, Authorization and Access Management (IdAAM)

As previously mentioned, Everlaw supports SSO via the SAML 2.0 protocol which means we can integrate with any platform that supports SAML. This includes Active Directory (among many others). Everlaw also supports PIV/CAC authentication. Everlaw has worked with other government agencies to integrate into their authentication platforms of choice and has a clear set of instructions it will provide

to Agency to help initiate the process. We can also help Agency establish Multi-factor Authentication for external collaborators, as needed.

Within the platform, Everlaw uses group-based security to control access to projects and permissions. The Agency Project Administrators will have the ability to create security groups (such as Administrators, Project Manager and Reviewer) and customize these groups' security down to individual document or code levels. There can be multiple Administrators or "Managers" on projects if needed. Agency will have full control over which users have access to any project. Because we do not charge for user licenses, there should not be a concern that an Admin can inadvertently incur extraneous charges through this process.

Operational FISMA Compliance

Everlaw is FedRAMP authorized since January 2020 and meets the requirements listed under NIST 800-53 framework, and thus meets the FISMA security and privacy requirements. Since achieving authorization in 2020, Everlaw has not exceeded two (2) incidents of non-compliance per fiscal year. We comply with FedRAMP mandates to protect and defend information systems from recurring security threats or in response to real-time vulnerabilities and have had no more than one (1) non-compliant incident per fiscal year. is Everlaw's standard to provide and apply security patches against all known high-risk vulnerabilities within thirty (30) days from date of discovery; moderate risk vulnerabilities mitigated within ninety (90) days from date of discovery; low risk vulnerabilities mitigated within one hundred and eighty (180) days from date of discovery, in accordance with an organizational assessment of risk.

Sensitive and Embargoed Data

Everlaw understands the importance of protecting sensitive government data. We have established internal controls to assure the security of confidential information and limit access to sensitive client data. Everlaw provides comprehensive training to our employees about data security and secure communications. We work from a least privilege-based access model to restrict access to government systems to only U.S. Persons with the appropriate training and certifications. We maintain a system of record that provides oversight into all employees with access to government data and the validation of their completion of the full approval process.

Confidentiality and Non-Disclosure

Everlaw will regard all information produced or received in response to this contract as sensitive and confidential, and that information will only be used in performance of the task order. As discussed above, Everlaw has a comprehensive security training and authorization process for any employees that will be accessing Agency data.

Everlaw Standard Service Level Agreements

Everlaw is the fastest ediscovery platform on the market and looks forward to delivering our cloud-native solution and ensuring our performance meets or exceeds Agency customers expectations. With our self-service optimized processing tool, new data can be rapidly added to the platform at speeds benchmarked between 500-900K documents per hour. Additionally, we propose the following SLA around availability and access as a starting point to negotiate and formalize final SLA's upon award:

Everlaw SLA. During the term of a Subscription under the applicable Everlaw Agreement (the "Agreement"), the Service will have a Monthly Availability of at least 99.5% of the time in any calendar month (the "Service Level Objective" or "SLO"). If Everlaw does not meet the SLO and Customer meets its obligations described in this SLA and the Agreement (including payment obligations), Customer will be eligible to receive SLA Credits. This SLA is the sole and exclusive remedy for any failure by Everlaw to meet the SLO. Capitalized terms used but not defined in this SLA will have the meanings given to them in the Agreement. All references to Customer in this SLA also mean Partner or Reseller (as applicable), and SLA Credits will apply for impacted Partner or Reseller order(s) under the Agreement.

Definitions. The following definitions apply to the Everlaw SLA.

"Downtime" means the total number of minutes for which customers are unable to login to the Service during the applicable calendar month. Downtime that occurs for less than one minute will not be counted towards any Downtime.

"Monthly Availability" is calculated by subtracting from 100% the percentage of Downtime minutes during the applicable calendar month.

"Scheduled Maintenance" means downtime periods scheduled to perform service maintenance, upgrades, and testing of failover capabilities.

"SLA Credit" means the following:

Monthly Availability	Percentage of monthly bill which does not meet SLO that will be credited to future monthly bills
99%-99.4%	5%
98%-98.9%	10%
95%-97.9%	25%
<95%	50%

SLA Credit. In order to receive SLA Credits, Customer must notify Everlaw by emailing support@everlaw.com within 30 days from the time Customer becomes eligible to receive SLA Credits. Failure to comply with this requirement will forfeit Customer's right to receive SLA Credits. If a dispute arises with respect to this SLA, Everlaw will make a determination in good faith based on its system logs, monitoring reports, configuration records, and other available information.

Maximum SLA Credits. The total maximum number of SLA Credits to be issued by Everlaw to Customer for Downtime that occurs in a single billing month will not exceed 50% of the amount payable by Customer for the applicable month. SLA Credits will be made in the form of a monetary credit applied to future use of the Service and will be applied within 60 days after the SLA Credit was requested.

Everlaw SLA Exclusions. The Everlaw SLA does not apply to any performance issues: (i) caused by factors described in the "Force Majeure" section of the Agreement; (ii) that resulted from Customer's software or hardware or third party software or hardware, or both (not within the primary control of Everlaw); (iii) that resulted from Customer's acts or omissions, including violations of the Agreement; (iv) general internet outages affecting multiple third parties; (v) network or services availability issues related to denial of service attacks and other flooding techniques; or (vi) Scheduled Maintenance.

Attachments

Please see additional attachments at the end of this document.

IN SUMMARY

Carahsoft Technology Corporation and Everlaw appreciate the opportunity to offer this solution for WV's initiative.

The Carahsoft Team has proposed a superior and cost-effective solution that fully complies with WV's requirements set forth in Cybersecurity e-Discovery Software Solicitation Number: CRFQ 0231 OOT2500000017. 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 State of West Virginia on this project.



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Info Technology

Proc Folder: 1619676			Reason for Modification:
Doc Description: Cybersecurity e-Discovery Software as a Service (OT25112)			
Proc Type: Central Contract - Fixed Amt			
Date Issued	Solicitation Closes	Solicitation No	Version
2025-02-06	2025-02-26 13:30	CRFQ 0231 OOT2500000017	1

BID RECEIVING LOCATION
BID CLERK DEPARTMENT OF ADMINISTRATION PURCHASING DIVISION 2019 WASHINGTON ST E CHARLESTON WV 25305 US

VENDOR
Vendor Customer Code: 000000195808
Vendor Name : Carahsoft Technology Corp.
Address : 11493 Sunset Hills Rd Suite 100
Street :
City : Fairfax
State : Virginia
Country : United States
Zip : 20190
Principal Contact :
Vendor Contact Phone: 703-871-8500
Extension:

FOR INFORMATION CONTACT THE BUYER Toby L Welch (304) 558-8802 toby.l.welch@wv.gov
Carahsoft Technology Corp.
Vendor Signature X <i>Natalie LeMay</i>
FEIN# 52-2189693
DATE 03/06/2025

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

The West Virginia Purchasing Division is soliciting bids on behalf of West Virginia Office of Technology to establish a contract for an e-Discovery software as a service. This software will be used for discovery in legal proceedings to process emails and other files. The software will facilitate keyword searching, document review, privilege report creation, data tagging and redaction prior to final report being released per the terms and conditions and specifications as attached.

INVOICE TO

DEPARTMENT OF
ADMINISTRATION
OFFICE OF TECHNOLOGY
1900 KANAWHA BLVD E,
BLDG 5 10TH FLOOR
CHARLESTON WV
US

SHIP TO

WV OFFICE OF
TECHNOLOGY
BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E
CHARLESTON WV
US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Contract Services: e-Discovery System				

Comm Code	Manufacturer	Specification	Model #
43231511			

Extended Description:

Please see the attached Exhibit A Pricing Page

Please note: Vendor must provide Exhibit A Pricing Page with their submitted bid response. Failure to do so will result in disqualification of your bid.

SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions are due by 3:00 p.m.	2025-02-18

	Document Phase	Document Description	Page 3
OOT2500000017	Draft	Cybersecurity e-Discovery Software as a Service (OT25112)	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

INSTRUCTIONS TO VENDORS SUBMITTING BIDS

1. REVIEW DOCUMENTS THOROUGHLY: The attached documents contain a solicitation for bids. Please read these instructions and all documents attached in their entirety. These instructions provide critical information about requirements that if overlooked could lead to disqualification of a Vendor's bid. All bids must be submitted in accordance with the provisions contained in these instructions and the Solicitation. Failure to do so may result in disqualification of Vendor's bid.

2. MANDATORY TERMS: The Solicitation may contain **mandatory** provisions identified by the use of the words "**must**," "**will**," and "**shall**." Failure to comply with a mandatory term in the Solicitation will result in bid disqualification.

3. PRE-BID MEETING: The item identified below shall apply to this Solicitation.

☒ A pre-bid meeting will not be held prior to bid opening

☐ A **MANDATORY PRE-BID** meeting will be held at the following place and time:

All Vendors submitting a bid must attend the **mandatory** pre-bid meeting. Failure to attend the **mandatory** pre-bid meeting shall result in disqualification of the Vendor's bid. No one individual is permitted to represent more than one vendor at the pre-bid meeting. Any individual that does attempt to represent two or more vendors will be required to select one vendor to which the individual's attendance will be attributed. The vendors not selected will be deemed to have not attended the pre-bid meeting unless another individual attended on their behalf.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. Any person attending the pre-bid meeting on behalf of a Vendor must list on the attendance sheet his or her name and the name of the Vendor he or she is representing. It is the Vendor's responsibility to locate the attendance sheet and provide the required information. Failure to complete the attendance sheet as required may result in disqualification of Vendor's bid.

Vendors who arrive after the starting time but prior to the end of the pre-bid will be permitted to sign in but are charged with knowing all matters discussed at the pre-bid.

Any discussions or answers to questions at the pre-bid meeting are preliminary in nature and are non-binding. Official and binding answers to questions will be published in a written addendum to the Solicitation prior to bid opening.

4. VENDOR QUESTION DEADLINE: Vendors may submit questions relating to this Solicitation to the Purchasing Division. Questions must be submitted in writing. All questions **must be submitted on or before the date listed below and to the address listed below to be considered.** A written response will be published in a Solicitation addendum if a response is possible and appropriate. Non-written discussions, conversations, or questions and answers regarding this Solicitation are preliminary in nature and are non-binding.

Submitted emails should have the solicitation number in the subject line. Question

Submission Deadline: Tuesday February 18, 2025 @3:00 p.m

Submit Questions to: Toby L Welch
2019 Washington Street, East Charleston, WV 25305
Fax: (304) 558-3970
Email: Toby.L.Welch@wv.gov

5. VERBAL COMMUNICATION: Any verbal communication between the Vendor and any State personnel is not binding, including verbal communication at the mandatory pre-bid conference. Only information issued in writing and added to the Solicitation by an official written addendum by the Purchasing Division is binding.

6. BID SUBMISSION: All bids must be submitted on or before the date and time of the bid opening listed in section 7 below. Vendors can submit bids electronically through wvOASIS, in paper form delivered to the Purchasing Division at the address listed below either in person or by courier, or in facsimile form by faxing to the Purchasing Division at the number listed below. Notwithstanding the foregoing, the Purchasing Division may prohibit the submission of bids electronically through wvOASIS at its sole discretion. Such a prohibition will be contained and communicated in the wvOASIS system resulting in the Vendor's inability to submit bids through wvOASIS. The Purchasing Division will not accept bids or modification of bids via email.

Bids submitted in paper, facsimile, or via wvOASIS must contain a signature. Failure to submit a bid in any form without a signature will result in rejection of your bid.

A bid submitted in paper or facsimile form should contain the information listed below on the face of the submission envelope or fax cover sheet. Otherwise, the bid may be rejected by the Purchasing Division.

VENDOR NAME:

BUYER: Toby L Welch

SOLICITATION NO.: CRFQ OOT2500000017

BID OPENING DATE: Wednesday February 26, 2025

BID OPENING TIME: 1:30 p.m.

FAX NUMBER: 304-558-3970

Any bid received by the Purchasing Division staff is considered to be in the possession of the Purchasing Division and will not be returned for any reason.

Bid Delivery Address and Fax Number:

Department of Administration, Purchasing Division 2019 Washington Street East

Charleston, WV 25305-0130

Fax: 304-558-3970

7. BID OPENING: Bids submitted in response to this Solicitation will be opened at the location identified below on the date and time listed below. Delivery of a bid after the bid opening date and time will result in bid disqualification. For purposes of this Solicitation, a bid is considered delivered when confirmation of delivery is provided by wvOASIS (in the case of electronic submission) or when the bid is time stamped by the official Purchasing Division time clock (in the case of hand delivery or via delivery by mail).

Bid Opening Date and Time: 02/26/25 @ 1:30 p.m.

Bid Opening Location:

Department of Administration, Purchasing Division

2019 Washington Street East

Charleston, WV 25305-0130

8. ADDENDUM ACKNOWLEDGEMENT: Changes or revisions to this Solicitation will be made by an official written addendum issued by the Purchasing Division. Vendor should acknowledge receipt of all addenda issued with this Solicitation by completing an Addendum Acknowledgement Form. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

9. BID FORMATTING: Vendor should type or electronically enter the information onto its bid to prevent errors in the evaluation. Failure to type or electronically enter the information may result in bid disqualification.

10. ALTERNATE MODEL OR BRAND: Unless the box below is checked, any model, brand, or specification listed in this Solicitation establishes the acceptable level of quality only and is not intended to reflect a preference for, or in any way favor, a particular brand or vendor. Vendors may bid alternates to a listed model or brand provided that the alternate is at least equal to the model or brand and complies with the required specifications. The equality of any alternate being bid shall be determined by the State at its sole discretion. Any Vendor bidding an alternate model or brand **shall** clearly identify the alternate items in its bid and should include manufacturer's specifications, industry literature, and/or any other relevant documentation demonstrating the equality of the alternate items. Failure to provide information for alternate items **may** be grounds for rejection of a Vendor's bid.

☐ This Solicitation is based upon a standardized commodity established under W. Va. Code § 5A-3-61. Vendors are expected to bid the standardized commodity identified. Failure to bid the standardized commodity will result in your firm's bid being rejected.

11. COMMUNICATION LIMITATIONS: In accordance with West Virginia Code of State Rules §148-1-6.6.2, communication with the State of West Virginia or any of its employees regarding this Solicitation during the solicitation, bid, evaluation or award periods, except through the Purchasing Division, is strictly prohibited without prior Purchasing Division approval. Purchasing Division approval for such communication is implied for all agency delegated and exempt purchases.

12. REGISTRATION: Prior to Contract award, the apparent successful Vendor **must** be properly registered with the West Virginia Purchasing Division and must have paid the \$125 fee, if applicable.

13. UNIT PRICE: Unit prices **shall** prevail in cases of a discrepancy in the Vendor's bid.

14. PREFERENCE: Vendor Preference may be requested in purchases of motor vehicles or construction and maintenance equipment and machinery used in highway and other infrastructure projects. Any request for preference must be submitted in writing with the bid, must specifically identify the preference requested with reference to the applicable subsection of West Virginia Code § 5A-3-37, and must include with the bid any information necessary to evaluate and confirm the applicability of the requested preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

15A. RECIPROCAL PREFERENCE: The State of West Virginia applies a reciprocal preference to all solicitations for commodities and printing in accordance with W. Va. Code § 5A-3-37(b). In effect, non-resident vendors receiving a preference in their home states, will see that same preference granted to West Virginia resident vendors bidding against them in West Virginia. Any request for reciprocal preference must include with the bid any information necessary to evaluate and confirm the applicability of the preference. A request form to help facilitate the request can be found at: www.state.wv.us/admin/purchase/vrc/Venpref.pdf.

15. SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES:

For any solicitations publicly advertised for bid, in accordance with West Virginia Code § 5A-3-37 and W. Va. CSR § 148-22-9, any non-resident vendor certified as a small, women-owned, or minority-owned business under W. Va. CSR § 148-22-9 shall be provided the same preference made available to any resident vendor. Any non-resident small, women-owned, or minority-owned business must identify itself as such in writing, must submit that writing to the Purchasing Division with its bid, and must be properly certified under W. Va. CSR § 148-22-9 prior to contract award to receive the preferences made available to resident vendors.

16. WAIVER OF MINOR IRREGULARITIES: The Director reserves the right to waive minor irregularities in bids or specifications in accordance with West Virginia Code of State Rules § 148-1-4.7.

17. ELECTRONIC FILE ACCESS RESTRICTIONS: Vendor must ensure that its submission in wvOASIS can be accessed and viewed by the Purchasing Division staff immediately upon bid opening. The Purchasing Division will consider any file that cannot be immediately accessed and viewed at the time of the bid opening (such as, encrypted files, password protected files, or incompatible files) to be blank or incomplete as context requires and are therefore unacceptable. A vendor will not be permitted to unencrypt files, remove password protections, or resubmit documents after bid opening to make a file viewable if those documents are required with the bid. A Vendor may be required to provide document passwords or remove access restrictions to allow the Purchasing Division to print or electronically save documents provided that those documents are viewable by the Purchasing Division prior to obtaining the password or removing the access restriction.

18. NON-RESPONSIBLE: The Purchasing Division Director reserves the right to reject the bid of any vendor as Non-Responsible in accordance with W. Va. Code of State Rules § 148-1-5.3, when the Director determines that the vendor submitting the bid does not have the capability to fully perform or lacks the integrity and reliability to assure good-faith performance.”

19. ACCEPTANCE/REJECTION: The State may accept or reject any bid in whole, or in part in accordance with W. Va. Code of State Rules § 148-1-4.6. and § 148-1-6.3.”

20. WITH THE BID REQUIREMENTS: In instances where these specifications require documentation or other information with the bid, and a vendor fails to provide it with the bid, the Director of the Purchasing Division reserves the right to request those items after bid opening and prior to contract award pursuant to the authority to waive minor irregularities in bids or specifications under W. Va. CSR § 148-1-4.7. This authority does not apply to instances where state law mandates receipt with the bid.

21. EMAIL NOTIFICATION OF AWARD: The Purchasing Division will attempt to provide bidders with e-mail notification of contract award when a solicitation that the bidder participated in has been awarded. For notification purposes, bidders must provide the Purchasing Division with a valid email address in the bid response. Bidders may also monitor *wvOASIS* or the Purchasing Division's website to determine when a contract has been awarded.

22. EXCEPTIONS AND CLARIFICATIONS: The Solicitation contains the specifications that **shall** form the basis of a contractual agreement. **Vendor shall clearly mark any exceptions, clarifications, or other proposed modifications in its bid.** Exceptions to, clarifications of, or modifications of a requirement or term and condition of the Solicitation may result in bid disqualification.

GENERAL TERMS AND CONDITIONS:

1. CONTRACTUAL AGREEMENT: Issuance of an Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance by the State of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid, or on the Contract if the Contract is not the result of a bid solicitation, signifies Vendor's agreement to be bound by and accept the terms and conditions contained in this Contract.

2. DEFINITIONS: As used in this Solicitation/Contract, the following terms shall have the meanings attributed to them below. Additional definitions may be found in the specifications included with this Solicitation/Contract.

2.1. "Agency" or "Agencies" means the agency, board, commission, or other entity of the State of West Virginia that is identified on the first page of the Solicitation or any other public entity seeking to procure goods or services under this Contract.

2.2. "Bid" or "Proposal" means the vendors submitted response to this solicitation.

2.3. "Contract" means the binding agreement that is entered into between the State and the Vendor to provide the goods or services requested in the Solicitation.

2.4. "Director" means the Director of the West Virginia Department of Administration, Purchasing Division.

2.5. "Purchasing Division" means the West Virginia Department of Administration, Purchasing Division.

2.6. "Award Document" means the document signed by the Agency and the Purchasing Division, and approved as to form by the Attorney General, that identifies the Vendor as the contract holder.

2.7. "Solicitation" means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

2.8. "State" means the State of West Virginia and/or any of its agencies, commissions, boards, etc. as context requires.

2.9. "Vendor" or "Vendors" means any entity submitting a bid in response to the Solicitation, the entity that has been selected as the lowest responsible bidder, or the entity that has been awarded the Contract as context requires.

3. CONTRACT TERM; RENEWAL; EXTENSION: The term of this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below:

☒ **Term Contract**

Initial Contract Term: The Initial Contract Term will be for a period of One (1) Year. The Initial Contract Term becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and the Initial Contract Term ends on the effective end date also shown on the first page of this Contract.

Renewal Term: This Contract may be renewed upon the mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any request for renewal should be delivered to the Agency and then submitted to the Purchasing Division thirty (30) days prior to the expiration date of the initial contract term or appropriate renewal term. A Contract renewal shall be in accordance with the terms and conditions of the original contract. Unless otherwise specified below, renewal of this Contract is limited to Three (3) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed the total number of months available in all renewal years combined. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

☐ **Alternate Renewal Term** – This contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's office (Attorney General approval is as to form only)

Delivery Order Limitations: In the event that this contract permits delivery orders, a delivery order may only be issued during the time this Contract is in effect. Any delivery order issued within one year of the expiration of this Contract shall be effective for one year from the date the delivery order is issued. No delivery order may be extended beyond one year after this Contract has expired.

☐ **Fixed Period Contract:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and must be completed within _____ days.

☐ **Fixed Period Contract with Renewals:** This Contract becomes effective upon Vendor's receipt of the notice to proceed and part of the Contract more fully described in the attached specifications must be completed within _____ days. Upon completion of the work covered by the preceding sentence, the vendor agrees that:

☐ the contract will continue for _____ years;

☐ the contract may be renewed for _____ successive _____ year periods or shorter periods provided that they do not exceed the total number of months contained in all available renewals. Automatic renewal of this Contract is prohibited. Renewals must be approved by the Vendor, Agency, Purchasing Division and Attorney General's Office (Attorney General approval is as to form only).

☐ **One-Time Purchase:** The term of this Contract shall run from the issuance of the Award Document until all of the goods contracted for have been delivered, but in no event will this Contract extend for more than one fiscal year.

☐ **Construction/Project Oversight:** This Contract becomes effective on the effective start date listed on the first page of this Contract, identified as the State of West Virginia contract cover page containing the signatures of the Purchasing Division, Attorney General, and Encumbrance clerk (or another page identified as _____), and continues until the project for which the vendor is providing oversight is complete.

☐ **Other:** Contract Term specified in _____

4. AUTHORITY TO PROCEED: Vendor is authorized to begin performance of this contract on the date of encumbrance listed on the front page of the Award Document unless either the box for "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked in Section 3 above. If either "Fixed Period Contract" or "Fixed Period Contract with Renewals" has been checked, Vendor must not begin work until it receives a separate notice to proceed from the State. The notice to proceed will then be incorporated into the Contract via change order to memorialize the official date that work commenced.

5. QUANTITIES: The quantities required under this Contract shall be determined in accordance with the category that has been identified as applicable to this Contract below.

☒ **Open End Contract:** Quantities listed in this Solicitation/Award Document are approximations only, based on estimates supplied by the Agency. It is understood and agreed that the Contract shall cover the quantities actually ordered for delivery during the term of the Contract, whether more or less than the quantities shown.

☐ **Service:** The scope of the service to be provided will be more clearly defined in the specifications included herewith.

☐ **Combined Service and Goods:** The scope of the service and deliverable goods to be provided will be more clearly defined in the specifications included herewith.

☐ **One-Time Purchase:** This Contract is for the purchase of a set quantity of goods that are identified in the specifications included herewith. Once those items have been delivered, no additional goods may be procured under this Contract without an appropriate change order approved by the Vendor, Agency, Purchasing Division, and Attorney General's office.

☐ **Construction:** This Contract is for construction activity more fully defined in the specifications.

6. EMERGENCY PURCHASES: The Purchasing Division Director may authorize the Agency to purchase goods or services in the open market that Vendor would otherwise provide under this Contract if those goods or services are for immediate or expedited delivery in an emergency. Emergencies shall include, but are not limited to, delays in transportation or an unanticipated increase in the volume of work. An emergency purchase in the open market, approved by the Purchasing Division Director, shall not constitute of breach of this Contract and shall not entitle the Vendor to any form of compensation or damages. This provision does not excuse the State from fulfilling its obligations under a One-Time Purchase contract.

7. REQUIRED DOCUMENTS: All of the items checked in this section must be provided to the Purchasing Division by the Vendor as specified:

☒ **LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section of the General Terms and Conditions entitled Licensing, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits upon request and in a form acceptable to the State. The request may be prior to or after contract award at the State's sole discretion.

WV Software as a Service Addendum Attached as Appendix A. See specification 4.1.10



The apparent successful Vendor shall also furnish proof of any additional licenses or certifications contained in the specifications regardless of whether or not that requirement is listed above.

8. INSURANCE: The apparent successful Vendor shall furnish proof of the insurance identified by a checkmark below prior to Contract award. The insurance coverages identified below must be maintained throughout the life of this contract. Thirty (30) days prior to the expiration of the insurance policies, Vendor shall provide the Agency with proof that the insurance mandated herein has been continued. Vendor must also provide Agency with immediate notice of any changes in its insurance policies, including but not limited to, policy cancelation, policy reduction, or change in insurers. The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether that insurance requirement is listed in this section.

Vendor must maintain:

☒ **Commercial General Liability Insurance** in at least an amount of: \$1,000,000.00 per occurrence.

☐ **Automobile Liability Insurance** in at least an amount of: _____ per occurrence.

☐ **Professional/Malpractice/Errors and Omission Insurance** in at least an amount of: _____ per occurrence. Notwithstanding the forgoing, Vendor's are not required to list the State as an additional insured for this type of policy.

☐ **Commercial Crime and Third Party Fidelity Insurance** in an amount of: _____ per occurrence.

☒ **Cyber Liability Insurance** in an amount of: \$1,000,000.00 per occurrence.

☐ **Builders Risk Insurance** in an amount equal to 100% of the amount of the Contract.

☐ **Pollution Insurance** in an amount of: _____ per occurrence.

☐ **Aircraft Liability** in an amount of: _____ per occurrence.

☐

☐

☐

☐

9. WORKERS' COMPENSATION INSURANCE: Vendor shall comply with laws relating to workers compensation, shall maintain workers' compensation insurance when required, and shall furnish proof of workers' compensation insurance upon request.

10. VENUE: All legal actions for damages brought by Vendor against the State shall be brought in the West Virginia Claims Commission. Other causes of action must be brought in the West Virginia court authorized by statute to exercise jurisdiction over it.

11. LIQUIDATED DAMAGES: This clause shall in no way be considered exclusive and shall not limit the State or Agency's right to pursue any other available remedy. Vendor shall pay liquidated damages in the amount specified below or as described in the specifications:

☐ _____ for _____.

☐ Liquidated Damages Contained in the Specifications.

☒ Liquidated Damages Are Not Included in this Contract.

12. ACCEPTANCE: Vendor's signature on its bid, or on the certification and signature page, constitutes an offer to the State that cannot be unilaterally withdrawn, signifies that the product or service proposed by vendor meets the mandatory requirements contained in the Solicitation for that product or service, unless otherwise indicated, and signifies acceptance of the terms and conditions contained in the Solicitation unless otherwise indicated.

13. PRICING: The pricing set forth herein is firm for the life of the Contract, unless specified elsewhere within this Solicitation/Contract by the State. A Vendor's inclusion of price adjustment provisions in its bid, without an express authorization from the State in the Solicitation to do so, may result in bid disqualification. Notwithstanding the foregoing, Vendor must extend any publicly advertised sale price to the State and invoice at the lower of the contract price or the publicly advertised sale price.

14. PAYMENT IN ARREARS: Payments for goods/services will be made in arrears only upon receipt of a proper invoice, detailing the goods/services provided or receipt of the goods/services, whichever is later. Notwithstanding the foregoing, payments for software maintenance, licenses, or subscriptions may be paid annually in advance.

15. PAYMENT METHODS: Vendor must accept payment by electronic funds transfer and P-Card. (The State of West Virginia's Purchasing Card program, administered under contract by a banking institution, processes payment for goods and services through state designated credit cards.)

16. TAXES: The Vendor shall pay any applicable sales, use, personal property or any other taxes arising out of this Contract and the transactions contemplated thereby. The State of West Virginia is exempt from federal and state taxes and will not pay or reimburse such taxes.

17. ADDITIONAL FEES: Vendor is not permitted to charge additional fees or assess additional charges that were not either expressly provided for in the solicitation published by the State of West Virginia, included in the Contract, or included in the unit price or lump sum bid amount that Vendor is required by the solicitation to provide. Including such fees or charges as notes to the solicitation may result in rejection of vendor's bid. Requesting such fees or charges be paid after the contract has been awarded may result in cancellation of the contract.

18. FUNDING: This Contract shall continue for the term stated herein, contingent upon funds being appropriated by the Legislature or otherwise being made available. In the event funds are not appropriated or otherwise made available, this Contract becomes void and of no effect beginning on July 1 of the fiscal year for which funding has not been appropriated or otherwise made available. If that occurs, the State may notify the Vendor that an alternative source of funding has been obtained and thereby avoid the automatic termination. Non-appropriation or non-funding shall not be considered an event of default.

19. CANCELLATION: The Purchasing Division Director reserves the right to cancel this Contract immediately upon written notice to the vendor if the materials or workmanship supplied do not conform to the specifications contained in the Contract. The Purchasing Division Director may also cancel any purchase or Contract upon 30 days written notice to the Vendor in accordance with West Virginia Code of State Rules § 148-1-5.2.b.

20. TIME: Time is of the essence regarding all matters of time and performance in this Contract.

21. APPLICABLE LAW: This Contract is governed by and interpreted under West Virginia law without giving effect to its choice of law principles. Any information provided in specification manuals, or any other source, verbal or written, which contradicts or violates the West Virginia Constitution, West Virginia Code, or West Virginia Code of State Rules is void and of no effect.

22. COMPLIANCE WITH LAWS: Vendor shall comply with all applicable federal, state, and local laws, regulations and ordinances. By submitting a bid, Vendor acknowledges that it has reviewed, understands, and will comply with all applicable laws, regulations, and ordinances.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to comply with all applicable laws, regulations, and ordinances. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

23. ARBITRATION: Any references made to arbitration contained in this Contract, Vendor's bid, or in any American Institute of Architects documents pertaining to this Contract are hereby deleted, void, and of no effect.

24. MODIFICATIONS: This writing is the parties' final expression of intent. Notwithstanding anything contained in this Contract to the contrary no modification of this Contract shall be binding without mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office (Attorney General approval is as to form only). Any change to existing contracts that adds work or changes contract cost, and were not included in the original contract, must be approved by the Purchasing Division and the Attorney General's Office (as to form) prior to the implementation of the change or commencement of work affected by the change.

25. WAIVER: The failure of either party to insist upon a strict performance of any of the terms or provision of this Contract, or to exercise any option, right, or remedy herein contained, shall not be construed as a waiver or a relinquishment for the future of such term, provision, option, right, or remedy, but the same shall continue in full force and effect. Any waiver must be expressly stated in writing and signed by the waiving party.

26. SUBSEQUENT FORMS: The terms and conditions contained in this Contract shall supersede any and all subsequent terms and conditions which may appear on any form documents submitted by Vendor to the Agency or Purchasing Division such as price lists, order forms, invoices, sales agreements, or maintenance agreements, and includes internet websites or other electronic documents. Acceptance or use of Vendor's forms does not constitute acceptance of the terms and conditions contained thereon.

27. ASSIGNMENT: Neither this Contract nor any monies due, or to become due hereunder, may be assigned by the Vendor without the express written consent of the Agency, the Purchasing Division, the Attorney General's office (as to form only), and any other government agency or office that may be required to approve such assignments.

28. WARRANTY: The Vendor expressly warrants that the goods and/or services covered by this Contract will: (a) conform to the specifications, drawings, samples, or other description furnished or specified by the Agency; (b) be merchantable and fit for the purpose intended; and (c) be free from defect in material and workmanship.

29. STATE EMPLOYEES: State employees are not permitted to utilize this Contract for personal use and the Vendor is prohibited from permitting or facilitating the same.

30. 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 www.state.wv.us/admin/purchase/privacy.

31. YOUR SUBMISSION IS A PUBLIC DOCUMENT: Vendor's entire response to the Solicitation and the resulting Contract are public documents. As public documents, they will be disclosed to the public following the bid/proposal opening or award of the contract, as required by the competitive bidding laws of West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq. and the Freedom of Information Act West Virginia Code §§ 29B-1-1 et seq.

DO NOT SUBMIT MATERIAL YOU CONSIDER TO BE CONFIDENTIAL, A TRADE SECRET, OR OTHERWISE NOT SUBJECT TO PUBLIC DISCLOSURE.

Submission of any bid, proposal, or other document to the Purchasing Division constitutes your explicit consent to the subsequent public disclosure of the bid, proposal, or document. The Purchasing Division will disclose any document labeled "confidential," "proprietary," "trade secret," "private," or labeled with any other claim against public disclosure of the documents, to include any "trade secrets" as defined by West Virginia Code § 47-22-1 et seq. All submissions are subject to public disclosure without notice.

32. LICENSING: In accordance with West Virginia Code of State Rules § 148-1-6.1.e, Vendor must be licensed and in good standing in accordance with any and all state and local laws and requirements by any state or local agency of West Virginia, including, but not limited to, the West Virginia Secretary of State's Office, the West Virginia Tax Department, West Virginia Insurance Commission, or any other state agency or political subdivision. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Upon request, the Vendor must provide all necessary releases to obtain information to enable the Purchasing Division Director or the Agency to verify that the Vendor is licensed and in good standing with the above entities.

SUBCONTRACTOR COMPLIANCE: Vendor shall notify all subcontractors providing commodities or services related to this Contract that as subcontractors, they too are required to be licensed, in good standing, and up-to-date on all state and local obligations as described in this section. Obligations related to political subdivisions may include, but are not limited to, business licensing, business and occupation taxes, inspection compliance, permitting, etc. Notification under this provision must occur prior to the performance of any work under the contract by the subcontractor.

33. 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.

34. VENDOR NON-CONFLICT: Neither Vendor nor its representatives are permitted to have any interest, nor shall they acquire any interest, direct or indirect, which would compromise the performance of its services hereunder. Any such interests shall be promptly presented in detail to the Agency.

35. VENDOR RELATIONSHIP: The relationship of the Vendor to the State shall be that of an independent contractor and no principal-agent relationship or employer-employee relationship is contemplated or created by this Contract. The Vendor as an independent contractor is solely liable for the acts and omissions of its employees and agents. Vendor shall be responsible for selecting, supervising, and compensating any and all individuals employed pursuant to the terms of this Solicitation and resulting contract. Neither the Vendor, nor any employees or subcontractors of the Vendor, shall be deemed to be employees of the State for any purpose whatsoever. Vendor shall be exclusively responsible for payment of employees and contractors for all wages and salaries, taxes, withholding payments, penalties, fees, fringe benefits, professional liability insurance premiums, contributions to insurance and pension, or other deferred compensation plans, including but not limited to, Workers' Compensation and Social Security obligations, licensing fees, etc. and the filing of all necessary documents, forms, and returns pertinent to all of the foregoing.

Vendor shall hold harmless the State, and shall provide the State and Agency with a defense against any and all claims including, but not limited to, the foregoing payments, withholdings, contributions, taxes, Social Security taxes, and employer income tax returns.

36. INDEMNIFICATION: The Vendor agrees to indemnify, defend, and hold harmless the State and the Agency, their officers, and employees from and against: (1) Any claims or losses for services rendered by any subcontractor, person, or firm performing or supplying services, materials, or supplies in connection with the performance of the Contract; (2) Any claims or losses resulting to any person or entity injured or damaged by the Vendor, its officers, employees, or subcontractors by the publication, translation, reproduction, delivery, performance, use, or disposition of any data used under the Contract in a manner not authorized by the Contract, or by Federal or State statutes or regulations; and (3) Any failure of the Vendor, its officers, employees, or subcontractors to observe State and Federal laws including, but not limited to, labor and wage and hour laws.

37. 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.

38. CONFLICT OF INTEREST: Vendor, its officers or members or employees, shall not presently have or acquire an interest, direct or indirect, which would conflict with or compromise the performance of its obligations hereunder. Vendor shall periodically inquire of its officers, members and employees to ensure that a conflict of interest does not arise. Any conflict of interest discovered shall be promptly presented in detail to the Agency.

39. REPORTS: Vendor shall provide the Agency and/or the Purchasing Division with the following reports identified by a checked box below:

☒ Such reports as the Agency and/or the Purchasing Division may request. Requested reports may include, but are not limited to, quantities purchased, agencies utilizing the contract, total contract expenditures by agency, etc.

☐ Quarterly reports detailing the total quantity of purchases in units and dollars, along with a listing of purchases by agency. Quarterly reports should be delivered to the Purchasing Division via email at purchasing.division@wv.gov.

40. 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.

41. PREFERENCE FOR USE OF DOMESTIC STEEL PRODUCTS: Except when authorized by the Director of the Purchasing Division pursuant to W. Va. Code § 5A-3-56, no contractor may use or supply steel products for a State Contract Project other than those steel products made in the United States. A contractor who uses steel products in violation of this section may be subject to civil penalties pursuant to W. Va. Code § 5A-3-56. As used in this section:

- a. "State Contract Project" means any erection or construction of, or any addition to, alteration of or other improvement to any building or structure, including, but not limited to, roads or highways, or the installation of any heating or cooling or ventilating plants or other equipment, or the supply of and materials for such projects, pursuant to a contract with the State of West Virginia for which bids were solicited on or after June 6, 2001.
- b. "Steel Products" means products rolled, formed, shaped, drawn, extruded, forged, cast, fabricated or otherwise similarly processed, or processed by a combination of two or more or such operations, from steel made by the open hearth, basic oxygen, electric furnace, Bessemer or other steel making process.
- c. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:
 1. The cost for each contract item used does not exceed one tenth of one percent (.1%) of the total contract cost or two thousand five hundred dollars (\$2,500.00), whichever is greater. For the purposes of this section, the cost is the value of the steel product as delivered to the project; or
 2. The Director of the Purchasing Division determines that specified steel materials are not produced in the United States in sufficient quantity or otherwise are not reasonably available to meet contract requirements.

42. PREFERENCE FOR USE OF DOMESTIC ALUMINUM, GLASS, AND STEEL: In Accordance with W. Va. Code § 5-19-1 et seq., and W. Va. CSR § 148-10-1 et seq., for every contract or subcontract, subject to the limitations contained herein, for the construction, reconstruction, alteration, repair, improvement or maintenance of public works or for the purchase of any item of machinery or equipment to be used at sites of public works, only domestic aluminum, glass or steel products shall be supplied unless the spending officer determines, in writing, after the receipt of offers or bids, (1) that the cost of domestic aluminum, glass or steel products is unreasonable or inconsistent with the public interest of the State of West Virginia, (2) that domestic aluminum, glass or steel products are not produced in sufficient quantities to meet the contract requirements, or (3) the available domestic aluminum, glass, or steel do not meet the contract specifications. This provision only applies to public works contracts awarded in an amount more than fifty thousand dollars (\$50,000) or public works contracts that require more than ten thousand pounds of steel products.

The cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than twenty percent (20%) of the bid or offered price for foreign made aluminum, glass, or steel products. If the domestic aluminum, glass or steel products to be supplied or produced in a “substantial labor surplus area”, as defined by the United States Department of Labor, the cost of domestic aluminum, glass, or steel products may be unreasonable if the cost is more than thirty percent (30%) of the bid or offered price for foreign made aluminum, glass, or steel products. This preference shall be applied to an item of machinery or equipment, as indicated above, when the item is a single unit of equipment or machinery manufactured primarily of aluminum, glass or steel, is part of a public works contract and has the sole purpose or of being a permanent part of a single public works project. This provision does not apply to equipment or machinery purchased by a spending unit for use by that spending unit and not as part of a single public works project.

All bids and offers including domestic aluminum, glass or steel products that exceed bid or offer prices including foreign aluminum, glass or steel products after application of the preferences provided in this provision may be reduced to a price equal to or lower than the lowest bid or offer price for foreign aluminum, glass or steel products plus the applicable preference. If the reduced bid or offer prices are made in writing and supersede the prior bid or offer prices, all bids or offers, including the reduced bid or offer prices, will be reevaluated in accordance with this rule.

43. INTERESTED PARTY SUPPLEMENTAL DISCLOSURE: W. Va. Code § 6D-1-2 requires that for contracts with an actual or estimated value of at least \$1 million, the Vendor must submit to the Agency a disclosure of interested parties prior to beginning work under this Contract. Additionally, the Vendor must submit a supplemental disclosure of interested parties reflecting any new or differing interested parties to the contract, which were not included in the original pre-work interested party disclosure, within 30 days following the completion or termination of the contract. A copy of that form is included with this solicitation or can be obtained from the WV Ethics Commission. This requirement does not apply to publicly traded companies listed on a national or international stock exchange. A more detailed definition of interested parties can be obtained from the form referenced above.

44. PROHIBITION AGAINST USED OR REFURBISHED: Unless expressly permitted in the solicitation published by the State, Vendor must provide new, unused commodities, and is prohibited from supplying used or refurbished commodities, in fulfilling its responsibilities under this Contract.

45. 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.

46. ISRAEL BOYCOTT: Bidder 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.

ADDITIONAL TERMS AND CONDITIONS (Construction Contracts Only)

1. CONTRACTOR'S LICENSE: Until June 15, 2021, West Virginia Code § 21-11-2, and after that date, § 30-42-2, requires that all persons desiring to perform contracting work in this state be licensed. The West Virginia Contractors Licensing Board is empowered to issue the contractor's license. Applications for a contractor's license may be made by contacting the West Virginia Contractor Licensing Board.

The apparent successful Vendor must furnish a copy of its contractor's license prior to the issuance of a contract award document.

2. BONDS: The following bonds must be submitted:

- ☐ **BID BOND:** Pursuant to the requirements contained in W. Va. Code § 5-22-1(c), All Vendors submitting a bid on a construction project shall furnish a valid bid bond in the amount of five percent (5%) of the total amount of the bid protecting the State of West Virginia. **THE BID BOND MUST BE SUBMITTED WITH THE BID OR VENDOR'S BID WILL BE DISQUALIFIED.**
- ☐ **PERFORMANCE BOND:** The apparent successful Vendor shall provide a performance bond in the amount of 100% of the contract. The performance bond must be received by the Purchasing Division prior to Contract award. (Attorney General requires use of the State approved bond forms found at: www.state.wv.us/admin/purchase/forms2.html)
- ☐ **LABOR/MATERIAL PAYMENT BOND:** The apparent successful Vendor shall provide a labor/material payment bond in the amount of 100% of the Contract value. The labor/material payment bond must be delivered to the Purchasing Division prior to Contract award. (Attorney General requires use of the State approved bond forms found at: www.state.wv.us/admin/purchase/forms2.html)
- ☐ **MAINTENANCE BOND:** The apparent successful Vendor shall provide a two (2) year maintenance bond covering the roofing system if the work impacts an existing roof. The amount of the bond must be equal to the price associated with the percentage of the project impacting the roof. The maintenance bond must be issued and delivered to the Purchasing Division prior to Contract award. (Attorney General requires use of the State approved bond forms found at: www.state.wv.us/admin/purchase/forms2.html)

At a minimum, all construction projects require a bid bond, performance bond, and labor/material payment bond. Failure on the part of the state of West Virginia to checkmark the required bonds above does not relieve the vendor from the legal requirement of providing these bonds.

In lieu of the Bid Bond, the Vendor may provide certified checks, cashier's checks, or irrevocable letters of credit. Any certified check, cashier's check, or irrevocable letter of credit provided in lieu of the bid bond must be of the same amount required of the Bid Bond and delivered with the bid.

3. DRUG-FREE WORKPLACE AFFIDAVIT: W. Va. Code § 21-1D-5 provides that any solicitation for a public improvement contract requires each Vendor that submits a bid for the work to submit an affidavit that the Vendor has a written plan for a drug-free workplace policy. If the affidavit is not submitted with the bid submission, the Purchasing Division shall promptly request by telephone and electronic mail that the low bidder and second low bidder provide the affidavit within one business day of the request. Failure to submit the affidavit within one business day of receiving the request shall result in disqualification of the bid. To comply with this law, Vendor should complete the enclosed drug-free workplace affidavit and submit the same with its bid. Failure to submit the signed and notarized drugfree workplace affidavit or a similar affidavit that fully complies with the requirements of the applicable code, within one business day of being requested to do so shall result in disqualification of Vendor's bid. Pursuant to W. Va. Code 21-1D-2(b) and (k), this provision does not apply to public improvement contracts the value of which is \$100,000 or less or temporary or emergency repairs.

3.1. DRUG-FREE WORKPLACE POLICY: Pursuant to W. Va. Code § 21-1D-4, Vendor and its subcontractors must implement and maintain a written drug-free workplace policy that complies with said article. The awarding public authority shall cancel this contract if: (1) Vendor fails to implement and maintain a written drug-free workplace policy described in the preceding paragraph, (2) Vendor fails to provide information regarding implementation of its drug-free workplace policy at the request of the public authority; or (3) Vendor provides to the public authority false information regarding the contractor's drug-free workplace policy.

Pursuant to W. Va. Code 21-1D-2(b) and (k), this provision does not apply to public improvement contracts the value of which is \$100,000 or less or temporary or emergency repairs.

4. DRUG FREE WORKPLACE REPORT: Pursuant to W. Va. Code § 21-1D-7b, no less than once per year, or upon completion of the project, every contractor shall provide a certified report to the public authority which let the contract. For contracts over \$25,000, the public authority shall be the West Virginia Purchasing Division. For contracts of \$25,000 or less, the public authority shall be the agency issuing the contract. The report shall include:

- (1) Information to show that the education and training service to the requirements of West Virginia Code § 21-1D-5 was provided;
- (2) The name of the laboratory certified by the United States Department of Health and Human Services or its successor that performs the drug tests;
- (3) The average number of employees in connection with the construction on the public improvement;
- (4) Drug test results for the following categories including the number of positive tests and the number of negative tests: (A) Pre-employment and new hires; (B) Reasonable suspicion; (C) Post-accident; and (D) Random.

Vendor should utilize the attached Certified Drug Free Workplace Report Coversheet when submitting the report required hereunder. Pursuant to W. Va. Code 21-1D-2(b) and (k), this provision does not apply to public improvement contracts the value of which is \$100,000 or less or temporary or emergency repairs.

5. AIA DOCUMENTS: All construction contracts that will be completed in conjunction with architectural services procured under Chapter 5G of the West Virginia Code will be governed by the attached AIA documents, as amended by the Supplementary Conditions for the State of West Virginia, in addition to the terms and conditions contained herein.

6. PROHIBITION AGAINST GENERAL CONDITIONS: Notwithstanding anything contained in the AIA Documents or the Supplementary Conditions, the State of West Virginia will not pay for general conditions, or winter conditions, or any other condition representing a delay in the contracts. The Vendor is expected to mitigate delay costs to the greatest extent possible and any costs associated with Delays must be specifically and concretely identified. The state will not consider an average daily rate multiplied by the number of days extended to be an acceptable charge.

7. GREEN BUILDINGS MINIMUM ENERGY STANDARDS: In accordance with § 22-29-4, all new building construction projects of public agencies that have not entered the schematic design phase prior to July 1, 2012, or any building construction project receiving state grant funds and appropriations, including public schools, that have not entered the schematic design phase prior to July 1, 2012, shall be designed and constructed complying with the ICC International Energy Conservation Code, adopted by the State Fire Commission, and the ANSI/ASHRAE/IESNA Standard 90.1-2007: Provided, That if any construction project has a commitment of federal funds to pay for a portion of such project, this provision shall only apply to the extent such standards are consistent with the federal standards.

8. LOCAL LABOR MARKET HIRING REQUIREMENT: Pursuant to West Virginia Code §21-1C-1 et seq., Employers shall hire at least seventy-five percent of employees for public improvement construction projects from the local labor market, to be rounded off, with at least two employees from outside the local labor market permissible for each employer per project.

Any employer unable to employ the minimum number of employees from the local labor market shall inform the nearest office of Workforce West Virginia of the number of qualified employees needed and provide a job description of the positions to be filled.

If, within three business days following the placing of a job order, Workforce West Virginia is unable to refer any qualified job applicants to the employer or refers less qualified job applicants than the number requested, then Workforce West Virginia shall issue a waiver to the employer stating the unavailability of applicant and shall permit the employer to fill any positions covered by the waiver from outside the local labor market. The waiver shall be in writing and shall be issued within the prescribed three days. A waiver certificate shall be sent to both the employer for its permanent project records and to the public authority.

Any employer who violates this requirement is subject to a civil penalty of \$250 per each employee less than the required threshold of seventy-five percent per day of violation after receipt of a notice of violation.

Any employer that continues to violate any provision of this article more than fourteen calendar days after receipt of a notice of violation is subject to a civil penalty of \$500 per each employee less than the required threshold of seventy-five percent per day of violation.

The following terms used in this section have the meaning shown below.

(1) The term “construction project” means any construction, reconstruction, improvement, enlargement, painting, decorating or repair of any public improvement let to contract in an amount equal to or greater than \$500,000. The term “construction project” does not include temporary or emergency repairs;

(2) The term “employee” means any person hired or permitted to perform hourly work for wages by a person, firm or corporation in the construction industry; The term “employee” does not include:(i) Bona fide employees of a public authority or individuals engaged in making temporary or emergency repairs;(ii) Bona fide independent contractors; or(iii) Salaried supervisory personnel necessary to assure efficient execution of the employee's work;

(3) The term “employer” means any person, firm or corporation employing one or more employees on any public improvement and includes all contractors and subcontractors;

(4) The term “local labor market” means every county in West Virginia and any county outside of West Virginia if any portion of that county is within fifty miles of the border of West Virginia;

(5) The term “public improvement” includes the construction of all buildings, roads, highways, bridges, streets, alleys, sewers, ditches, sewage disposal plants, waterworks, airports and all other structures that may be let to contract by a public authority, excluding improvements funded, in whole or in part, by federal funds.

9. DAVIS-BACON AND RELATED ACT WAGE RATES:

☐ The work performed under this contract is federally funded in whole, or in part. Pursuant to _____, Vendors are required to pay applicable Davis-Bacon wage rates.

☐ The work performed under this contract is not subject to Davis-Bacon wage rates.

10. SUBCONTRACTOR LIST SUBMISSION: In accordance with W. Va. Code § 5-22-1, the apparent low bidder on a contract valued at more than \$250,000.00 for the construction, alteration, decoration, painting or improvement of a new or existing building or structure shall submit a list of all subcontractors who will perform more than \$25,000.00 of work on the project including labor and materials. (This section does not apply to any other construction projects, such as highway, mine reclamation, water or sewer projects.) The subcontractor list shall be provided to the Purchasing Division within one business day of the opening of bids for review. If the apparent low bidder fails to submit the subcontractor list, the Purchasing Division shall promptly request by telephone and electronic mail that the low bidder and second low bidder provide the subcontractor list within one business day of the request. Failure to submit the subcontractor list within one business day of receiving the request shall result in disqualification of the bid.

If no subcontractors who will perform more than \$25,000.00 of work are to be used to complete the project, the apparent low bidder must make this clear on the subcontractor list, in the bid itself, or in response to the Purchasing Division's request for the subcontractor list.

a. Required Information. The subcontractor list must contain the following information:

- i. Bidder's name
- ii. Name of each subcontractor performing more than \$25,000 of work on the project.
- iii. The license number of each subcontractor, as required by W. Va. Code § 21-11-1 et. seq.
- iv. If applicable, a notation that no subcontractor will be used to perform more than \$25,000.00 of work. (This item iv. is not required if the vendor makes this clear in the bid itself or in documentation following the request for the subcontractor list.)

b. Subcontractor List Submission Form: The subcontractor list may be submitted in any form, including the attached form, as long as the required information noted above is included. If any information is missing from the bidder's subcontractor list submission, it may be obtained from other documents such as bids, emails, letters, etc. that accompany the subcontractor list submission.

c. Substitution of Subcontractor. Written approval must be obtained from the State Spending Unit before any subcontractor substitution is permitted. Substitutions are not permitted unless:

- i. The subcontractor listed in the original bid has filed for bankruptcy;
- ii. The subcontractor in the original bid has been debarred or suspended; or
- iii. The contractor certifies in writing that the subcontractor listed in the original bid fails, is unable, or refuses to perform his subcontract.

Subcontractor List Submission (Construction Contracts Only)

Bidder's Name: _____

☐ Check this box if no subcontractors will perform more than \$25,000.00 of work to complete the project.

Subcontractor Name	License Number if Required by W. Va. Code § 21-11-1 et. seq.

Attach additional pages if necessary

ADDITIONAL TERMS AND CONDITIONS
(Architectural and Engineering Contracts Only)

1. PLAN AND DRAWING DISTRIBUTION: All plans and drawings must be completed and available for distribution at least five business days prior to a scheduled pre-bid meeting for the construction or other work related to the plans and drawings.

2. PROJECT ADDENDA REQUIREMENTS: The Architect/Engineer and/or Agency shall be required to abide by the following schedule in issuing construction project addenda. The Architect/Engineer shall prepare any addendum materials for which it is responsible, and a list of all vendors that have obtained drawings and specifications for the project. The Architect/Engineer shall then send a copy of the addendum materials and the list of vendors to the State Agency for which the contract is issued to allow the Agency to make any necessary modifications. The addendum and list shall then be forwarded to the Purchasing Division buyer by the Agency. The Purchasing Division buyer shall send the addendum to all interested vendors and, if necessary, extend the bid opening date. Any addendum should be received by the Purchasing Division at least fourteen (14) days prior to the bid opening date.

3. PRE-BID MEETING RESPONSIBILITIES: The Architect/Engineer shall be available to attend any pre-bid meeting for the construction or other work resulting from the plans, drawings, or specifications prepared by the Architect/Engineer.

4. AIA DOCUMENTS: All construction contracts that will be completed in conjunction with architectural services procured under Chapter 5G of the West Virginia Code will be governed by the attached AIA documents, as amended by the Supplementary Conditions for the State of West Virginia, in addition to the terms and conditions contained herein. The terms and conditions of this document shall prevail over anything contained in the AIA Documents or the Supplementary Conditions.

5. GREEN BUILDINGS MINIMUM ENERGY STANDARDS: In accordance with West Virginia Code § 22-29-4, all new building construction projects of public agencies that have not entered the schematic design phase prior to July 1, 2012, or any building construction project receiving state grant funds and appropriations, including public schools, that have not entered the schematic design phase prior to July 1, 2012, shall be designed and constructed complying with the ICC International Energy Conservation Code, adopted by the State Fire Commission, and the ANSI/ASHRAE/IESNA Standard 90.1-2007: Provided, That if any construction project has a commitment of federal funds to pay for a portion of such project, this provision shall only apply to the extent such standards are consistent with the federal standards.

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Printed Name and Title) _____

(Address) _____

(Phone Number) / (Fax Number) _____

(email address) _____

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, 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 this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; 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.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

(Company)

(Signature of Authorized Representative)

(Printed Name and Title of Authorized Representative) (Date)

(Phone Number) (Fax Number)

(Email Address)

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.:

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

- ☐ Addendum No. 1
- ☐ Addendum No. 2
- ☐ Addendum No. 3
- ☐ Addendum No. 4
- ☐ Addendum No. 5

- ☐ Addendum No. 6
- ☐ Addendum No. 7
- ☐ Addendum No. 8
- ☐ Addendum No. 9
- ☐ Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Carahsoft Technology Corp.

Company

Natalie LeMay

Authorized Signature

03/06/2025

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

REQUEST FOR QUOTATION
e-Discovery Software as a Service

SPECIFICATIONS

1. **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of West Virginia Office of Technology to establish a contract for an e-Discovery software as a service. This software will be used for discovery in legal proceedings to process emails and other files. The software will facilitate keyword searching, document review, privilege report creation, data tagging and redaction prior to final report being released.

WVOT provides highly reliable, protected, and cost-effective technology services to approximately 25,000 computers and 20,000 network users. Services are delivered by approximately 200 full-time and temporary employees and supplemented by specialized contract services and staff on an as-needed basis. There are approximately 210 entities total within the executive branch where services are provided. Funding for the Office of Technology is derived from a fee for services model.

2. **DEFINITIONS:** The terms listed below shall have the meanings assigned to them below. Additional definitions can be found in section 2 of the General Terms and Conditions.

2.1 **“Business Hours”** means Monday - Friday 8:00 AM to 5:00 PM EST excluding weekends and Federal and State holidays, which are as follows:

- 2.1.1 New Year’s Day (January 1)
- 2.1.2 Martin Luther King Day (Third Monday in January)
- 2.1.3 President’s Day (Third Monday in February)
- 2.1.4 Memorial Day (Last Monday in May)
- 2.1.5 West Virginia Day (June 20)
- 2.1.6 Independence Day (July 4)
- 2.1.7 Labor Day (First Monday in September)
- 2.1.8 Columbus Day (Second Monday in October)
- 2.1.9 Veterans Day (November 11)
- 2.1.10 Thanksgiving (Fourth Thursday in November)
- 2.1.11 Day After Thanksgiving (Fourth Friday in November)
- 2.1.12 Christmas Day (December 25)

2.2 **“Contract Services”** means an e-Discovery system as more fully described in these specifications.

2.3 **“Pricing Page”** means the pages, contained wvOASIS or attached hereto as Exhibit A, upon which Vendor should list its proposed price for the Contract Services.

2.4 **“Solicitation”** means the official notice of an opportunity to supply the State with goods or services that is published by the Purchasing Division.

3. **QUALIFICATIONS:** Vendor, or Vendor’s staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications:

REQUEST FOR QUOTATION
e-Discovery Software as a Service

3.1. The Vendor must be compliant with Internal Revenue Service (IRS) 1075, Section AC-17 Remote Access, and Section 3.3.1. Cloud Computing.

4. MANDATORY REQUIREMENTS:

4.1 Mandatory Contract Services Requirements and Deliverables: Contract Services must meet or exceed the mandatory requirements listed below.

4.1.1 General Requirements– e-Discovery System

4.1.1.1 The Vendor must provide an e-Discovery System that is cloud-based (Software as a Service Model). as well as support Automated Cloud Data Collections and Connectors

4.1.1.2 The system must contain the following capabilities within a single platform that does not require integration with other software: self-service data loading, self-service data processing, client administration, self-service, productions, review, and analytics capabilities.

4.1.1.3 The Vendor must provide an e-Discovery System with unlimited user seats for a minimum of 12 months from date of award.

4.1.1.4 The system must allow client administrators to have the ability to set-up new users or workspaces and assign roles and permissions to new users.

4.1.1.5 The system must allow a user to have multiple roles and toggle between roles. For example, a client administrator can toggle between user roles to validate user permissions and provide user support.

4.1.1.6 The system must not require additional licenses and/or software from third parties.

4.1.1.7 The system must allow the customer/client administrators the ability to remove/delete documents and create archives from the platform.

REQUEST FOR QUOTATION
e-Discovery Software as a Service

4.1.1.8 The system must be accessible to an unlimited number of users and allow access to at least 50 concurrent cases each having at least one million documents without degradation to speed.

4.1.1.9 The system must be a configurable Platform that allows the administrators to configure applications like request tracking and FOIA requests.

4.1.1.10 The system must be built on scalable architecture with a storage capacity of at least two petabytes of data.

4.1.1.11 The Vendor must provide an e-Discovery System that features the following:

4.1.1.11.1 A system that has two-factor authentication access.

4.1.1.11.2 A system that allows the Agency to have 100% data input automation. The Vendor must not have access to Agency-owned data.

4.1.1.11.3 A system that provides 256-bit encryption to the data when at rest and in transit.

4.1.1.11.4 A system that scans files for viruses.

4.1.1.11.5 A system that allows for load file import and export.

4.1.2 Data Loading & Processing- e-Discovery System

4.1.2.1 The system must allow the Agency to have 100% data input automation.

4.1.2.2 The system must allow the user to load raw data such as PSTs, zip files, and other ESI for processing.

REQUEST FOR QUOTATION
e-Discovery Software as a Service

- 4.1.2.3 The system must allow the client administrator to move data between data stores and conduct early case assessment, including running search terms, and listing and counting file types reports, prior to making the data available to reviewers.
- 4.1.2.4 The system must allow the customer to create, save, and upload templates for data processing.
- 4.1.2.5 The system must have pre-built utilities to support processing for various files including imaging, loading, and text files.
- 4.1.2.6 The system must support uploading up to 10 GB of data directly from web-browser via “drag and drop”.
- 4.1.2.7 The system must allow loading and processing of a data set that has at least 1 terabyte of documents, data, or ESI, into the review tool.
- 4.1.2.8 The system must support data reduction and culling (De-NIST; custodial and global Deduplication; filtering by Custodian, file type, date; keyword searching) during processing.
- 4.1.2.9 The system must include built-in ESI processing capabilities (extraction of text and metadata, imaging, numbering, OCR, load file creation).
- 4.1.2.10 The system must keep emails and families together and locate orphaned documents during processing.
- 4.1.2.11 The system must support extraction and processing of files within container files such as zip and rar, and support the processing of files in nested containers or folders.
- 4.1.2.12 The system must have the ability to ingest, process, and view multiple file types.
- 4.1.2.13 The system must allow for load file import and export.
- 4.1.2.14 The system must allow the user the ability to create templates for processing, production, import, export.

REQUEST FOR QUOTATION
e-Discovery Software as a Service

4.1.2.15 The system must be able to securely transfer ESI to the review tool.

4.1.3 Review – e-Discovery System

4.1.3.1 The system must allow users to review and analyze ESI productions.

4.1.3.2 The system must allow users to identify and remove duplicate documents and data.

4.1.3.3 The system must allow users to redact and highlight portions of the document.

4.1.3.4 The system must allow users to search, tag, index, and code information and provide advance search features including but not limited to keyword, Boolean, stemming, wildcard, fuzzy, proximity and other search types.

4.1.3.5 The system must process searches, display documents, and allow users to perform document review with minimal loading times.

4.1.3.6 The system must include a file viewer that easily and quickly opens files without needing to install additional applications. Supported files must include: .docx, .xlsx, .pdf, .jpg, .jpeg, .mov, avi, .rtf, .txt., pub, .pptx.

4.1.3.7 The system must support searching on tags/codes and metadata.

4.1.3.8 The system must allow the user the option to assign and self-assign batches for review.

4.1.3.9 The system must provide search engines that support both Elasticsearch and dtSearch indexing and searching options within a single matter.

4.1.3.10 The system must allow the user to create workspaces, folders, etc., for customizable document organization.

REQUEST FOR QUOTATION
e-Discovery Software as a Service

4.1.3.11 The system must provide full administrator rights to the customer, including the ability to assign roles/permissions, create review assignments and/ or review batches for reviewers.

4.1.3.12 The system must allow for the customization of coding panels.

4.1.4 Advanced Analytics – eDiscovery System

4.1.4.1 The system must include the following content & context analysis capabilities: topic clustering, email threading, near-duplicate analysis, entities recognition.

4.1.4.2 The system must provide predictive coding, advanced artificial intelligence (AI) and Technology Assisted Review (TAR) technologies including TAR 1.0 and TAR 3.0.

4.1.4.3 The system must provide Active Learning (story builder with continuous active learning analytics).

4.1.5 Security – eDiscovery System

4.1.5.1 The system must provide secure authorized access and have multi-factor authentication for each user to prevent unauthorized access.

4.1.5.2 The systems must provide automatic session termination if no activity with a prescribed period of time.

4.1.5.3 The system must allow a client administrator to restrict security rights at the individual, group or role level.

4.1.5.4 The system must provide a security level that allows system administrators to add new users to the system and edit existing user permissions.

4.1.5.5 The vendor must provide regular maintenance including new releases and updates.

REQUEST FOR QUOTATION
e-Discovery Software as a Service

4.1.5.6 The system must provide at least 256-bit encryption to the data when at rest and in transit.

4.1.6 Production – eDiscovery System

4.1.6.1 The system must provide production of the ESI in a variety of formats including as searchable PDF, native or images and text with a load file.

4.1.6.2 The system must have a wizard-driven production process.

4.1.6.3 The system must have self-service production capabilities to allow the user to prepare and export from start to finish/download.

4.1.6.4 The system must allow the user to view all productions for a single file in the review platform.

4.1.7 Professional Services and Training – eDiscovery

4.1.7.1 The vendor must provide live training (which may be virtual).

4.1.7.2 The vendor must provide reviewer training and client administrator/organization administrator training.

4.1.7.3 The vendor must record live training and provide recorded training to the client at no additional cost.

4.1.7.4 The system must provide access to a knowledge base or help center, technical documentation, and online support resources.

4.1.7.5 The vendor must provide support services for the initial setup.

4.1.7.6 The vendor must provide support services for the duration of the contract for ongoing maintenance.

REQUEST FOR QUOTATION
e-Discovery Software as a Service

4.1.7.7 The vendor must offer client services support including project management and technical support services.

4.1.8 Support - eDiscovery

4.1.8.1 Support by telephone, online, in-app, and email 24 hours-a-day, 7 days-a-week, 365 days-a-year for troubleshooting technical issues

4.1.8.2 A response time of a minimum of 1 day to request for technical support.

4.1.8.3 Access to knowledgebase, technical documentation, and online support resources.

4.1.9 Billing - eDiscovery

4.1.9.1 Vendor will round up to the nearest next whole gigabyte (GB) for billing and auditing purposes. (Example 1.2GB will be billed at 2.0 GB)

4.1.9.2 Vendor will invoice monthly and bill at the maximum gigabyte (GB) capacity used by the state.

4.1.9.3 Vendor's proposed solution must provide billing capabilities designed to simplify the procedures of a chargeback model, as well as provide a holistic view of service. The state desires the billing detail to include but not be limited to billing by agency, consumption usage by each agency.

4.1.10 Software as a Service Addendum

4.1.10.1 Vendor must sign the attached Software as a Service Addendum prior to award.

4.1.11 Optional Renewals

4.1.11.1 Vendor will include in their bid the cost of optional Annual renewals for years 2, 3, and 4. These optional Annual renewals will be initiated on Agency request authorized under the authority of the Purchasing Division.

5 CONTRACT AWARD:

5.1 Contract Award: The Contract is intended to provide Agency with a purchase price for the Contract Services. The Contract shall be awarded to the

REQUEST FOR QUOTATION
e-Discovery Software as a Service

Vendor that provides the Contract Services meeting the required specifications for the lowest overall total cost as shown on the Pricing Pages.

5.2 Contract will be evaluated on all lines but only awarded for the first year with the option for renewal at the end of the first-year term. Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

5.3 Pricing Page: Vendor should complete the attached Exhibit A - Pricing Page by providing the unit cost per Gigabyte (GB) per month. The unit price will be multiplied with the quantity to provide the extended cost. The calculated Overall Total Cost must be entered into wvOASIS pricing section for commodity line 1. The Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified.

5.3.1 The Pricing Page contains a list of the Contract Items and estimated purchase volume. The estimated purchase volume for each item represents the approximate volume of anticipated purchases only. No future use of the Contract or any individual item is guaranteed or implied.

5.3.2 Vendor should provide with their bid a copy of any and all Software Terms and Conditions or licenses that the State of West Virginia or the Agency will have to agree to or accept as a part of this solicitation. This information will be required before contract is issued.

5.3.3 Vendor should include a copy of any Maintenance Terms and Conditions or Licenses that the State of West Virginia or the Agency will be required to agree to and accept as a part of this solicitation. This information will be required before contract is issued.

5.3.4 Vendor should type or electronically enter the information into the Pricing Pages through wvOASIS, if available, or as an electronic document.

6 PERFORMANCE: Vendor and Agency shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already

REQUEST FOR QUOTATION
e-Discovery Software as a Service

included herein by Agency. In the event that this Contract is designated as an open-end contract, Vendor shall perform in accordance with the release orders that may be issued against this Contract.

- 7 PAYMENT:** Agency shall pay a flat fee, as shown on the Pricing Pages, for all Contract Services performed and accepted under this Contract. Vendor shall accept payment in accordance with the payment procedures of the State of West Virginia.
- 8 TRAVEL:** Vendor shall be responsible for all mileage and travel costs, including travel time, associated with performance of this Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on Vendor's bid, but such costs will not be paid by the Agency separately.
- 9 FACILITIES ACCESS:** Performance of Contract Services may require access cards and/or keys to gain entrance to Agency's facilities. In the event that access cards and/or keys are required:
 - 9.1** Vendor must identify principal service personnel which will be issued access cards and/or keys to perform service.
 - 9.2** Vendor will be responsible for controlling cards and keys and will pay replacement fee, if the cards or keys become lost or stolen.
 - 9.3** Vendor shall notify Agency immediately of any lost, stolen, or missing card or key.
 - 9.4** Anyone performing under this Contract will be subject to Agency's security protocol and procedures.
 - 9.5** Vendor shall inform all staff of Agency's security protocol and procedures.

REQUEST FOR QUOTATION
e-Discovery Software as a Service

10 VENDOR DEFAULT: The following shall be considered a vendor default under this Contract.

10.1 Failure to perform Contract Services in accordance with the requirements contained herein.

10.2 Failure to comply with other specifications and requirements contained herein.

10.3 Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

10.4 Failure to remedy deficient performance upon request.

10.5 The following remedies shall be available to Agency upon default:

10.5.1 Immediate cancellation of the Contract.

10.5.2 Immediate cancellation of one or more release orders issued under this Contract.

10.5.3 Any other remedies available in law or equity.

11 MISCELLANEOUS:

Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager:	
Telephone Number:	
Fax Number:	
Email Address:	

APPENDIX A:

SOFTWARE AS A SERVICE ADDENDUM

Begins on next page.

Software as a Service Addendum

1. Definitions:

Acceptable alternative data center location means a country that is identified as providing equivalent or stronger data protection than the United States, in terms of both regulation and enforcement. DLA Piper's Privacy Heatmap shall be utilized for this analysis and may be found at <https://www.dlapiperdataprotection.com/index.html?t=world-map&c=US&c2=IN>.

Authorized Persons means the service provider's employees, contractors, subcontractors or other agents who have responsibility in protecting or have access to the public jurisdiction's personal data and non-public data to enable the service provider to perform the services required.

Data Breach means the unauthorized access and acquisition of unencrypted and unredacted personal data that compromises the security or confidentiality of a public jurisdiction's personal information and that causes the service provider or public jurisdiction to reasonably believe that the data breach has caused or will cause identity theft or other fraud.

Individually Identifiable Health Information means 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.

Non-Public Data means data, other than personal data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the public jurisdiction because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.

Personal Data means data that includes information relating to a person that identifies the person by first name or first initial, and last name, and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, state identification card); financial account information, including account number, credit or debit card numbers; or protected health information (PHI).

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.

Public Jurisdiction means any government or government agency that uses these terms and conditions. The term is a placeholder for the government or government agency.

Public Jurisdiction Data means all data created or in any way originating with the public jurisdiction, and all data that is the output of computer processing or other electronic manipulation of any data that was created by or in any way originated with the public jurisdiction, whether such data or output is stored on the public jurisdiction's hardware, the service provider's hardware or exists in any system owned, maintained or otherwise controlled by the public jurisdiction or by the service provider.

Public Jurisdiction Identified Contact means the person or persons designated in writing by the public jurisdiction to receive security incident or breach notification.

Restricted data means personal data and non-public data.

Security Incident means the actual unauthorized access to personal data or non-public data the service provider believes could reasonably result in the use, disclosure or theft of a public jurisdiction's unencrypted personal data or non-public data within the possession or control of the service provider. A security incident may or may not turn into a data breach.

Service Provider means the contractor and its employees, subcontractors, agents and affiliates who are providing the services agreed to under the contract.

Software-as-a-Service (SaaS) means the capability provided to the consumer to use the provider's applications running on a 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.

2. Data Ownership: The public jurisdiction will own all right, title and interest in its data that is related to the services provided by this contract. The service provider shall not access public jurisdiction user accounts or public jurisdiction 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 contract or (4) at the public jurisdiction's written request.

3. Data Protection and Privacy: Protection of personal privacy and data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of public jurisdiction information at any time. To this end, the service provider shall safeguard the confidentiality, integrity and availability of public jurisdiction information and comply with the following conditions:

- a) The service provider shall implement and maintain appropriate administrative, technical and physical security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. In Appendix A,

- the public jurisdiction shall indicate whether restricted information will be processed by the service provider. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the service provider applies to its own personal data and non-public data of similar kind. The service provider shall ensure that all such measures, including the manner in which personal data and non-public data are collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws, as well as the terms and conditions of this Addendum and shall survive termination of the underlying contract.
- b) The service provider represents and warrants that its collection, access, use, storage, disposal and disclosure of personal data and non-public data do and will comply with all applicable federal and state privacy and data protection laws, as well as all other applicable regulations, policies and directives.
 - c) The service provider shall support third-party multi-factor authentication integration with the public jurisdiction third-party identity provider to safeguard personal data and non-public data.
 - d) If, in the course of its engagement by the public jurisdiction, the service provider has access to or will collect, access, use, store, process, dispose of or disclose credit, debit or other payment cardholder information, the service provider shall at all times remain in compliance with the Payment Card Industry Data Security Standard ("PCI DSS") requirements, including remaining aware at all times of changes to the PCI DSS and promptly implementing all procedures and practices as may be necessary to remain in compliance with the PCI DSS, in each case, at the service provider's sole cost and expense. All data obtained by the service provider in the performance of this contract shall become and remain the property of the public jurisdiction.
 - e) All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the service provider is responsible for encryption of the personal data.
 - f) Unless otherwise stipulated, the service provider shall encrypt all non-public data at rest and in transit, in accordance with recognized industry practice. The public jurisdiction shall identify data it deems as non-public data to the service provider.
 - g) At no time shall any data or process – that either belong to or are intended for the use of a public jurisdiction or its officers, agents or employees — be copied, disclosed or retained by the service provider or any party related to the service provider for subsequent use in any transaction that does not include the public jurisdiction.
 - h) The service provider shall not use or disclose any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.
 - i) Data Location. For non-public data and personal data, the service provider shall provide its data center services to the public jurisdiction and its end users solely from data centers in the U.S. Storage of public jurisdiction data at rest shall be located solely in data centers in the U.S. The service provider shall not allow its personnel or contractors to store public jurisdiction data on portable devices, including personal computers, except for devices that are used and kept only at its

U.S. data centers. With agreement from the public jurisdiction, this term may be met by the service provider providing its services from an acceptable alternative data center location, which agreement shall be stated in Appendix A. The Service Provider may also request permission to utilize an acceptable alternative data center location during a procurement's question and answer period by submitting a question to that effect. The service provider shall permit its personnel and contractors to access public jurisdiction data remotely only as required to provide technical support.

4. Security Incident or Data Breach Notification: The service provider shall inform the public jurisdiction of any confirmed security incident or data breach.

- a) **Incident Response:** The service provider 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 defined by law or contained in the contract. Discussing security incidents with the public jurisdiction shall be handled on an urgent as-needed basis, as part of service provider communication and mitigation processes defined by law or contained in the contract.
- b) **Security Incident Reporting Requirements:** The service provider shall report a confirmed Security Incident as soon as practicable, but no later than twenty-four (24) hours after the service provider becomes aware of it, to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and (3) the public jurisdiction point of contact for general contract oversight/administration. The following information shall be shared with the public jurisdiction: (1) incident phase (detection and analysis; containment, eradication and recovery; or post-incident activity), (2) projected business impact, and, (3) attack source information.
- c) **Breach Reporting Requirements:** Upon the discovery of a data breach or unauthorized access to non-public data, the service provider shall immediately report to: (1) the department privacy officer, by email, with a read receipt, identified in Appendix A; and, (2) unless otherwise directed by the public jurisdiction in the underlying contract, the WVOT Online Computer Security and Privacy Incident Reporting System at <https://apps.wv.gov/ot/ir/Default.aspx>, and the public jurisdiction point of contact for general contract oversight/administration.

5. Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of the service provider.

- a) Immediately after being awarded a contract, the service provider shall provide the public jurisdiction with the name and contact information for an employee of service provider who shall serve as the public jurisdiction's primary security contact and shall be available to assist the public jurisdiction twenty-four (24) hours per day, seven (7) days per week as a contact in resolving obligations associated with a data breach. The service provider may provide this information in Appendix A.

- b) Immediately following the service provider's notification to the public jurisdiction of a data breach, the parties shall coordinate cooperate with each other to investigate the data breach. The service provider agrees to fully cooperate with the public jurisdiction in the public jurisdiction's handling of the matter, including, without limitation, at the public jurisdiction's request, making available all relevant records, logs, files, data reporting and other materials required to comply with applicable law and regulation.
- c) Within 72 hours of the discovery, the service provider shall notify the parties listed in 4(c) above, to the extent known: (1) date of discovery; (2) list of data elements and the number of individual records; (3) description of the unauthorized persons known or reasonably believed to have improperly used or disclosed the personal data; (4) description of where the personal data is believed to have been improperly transmitted, sent, or utilized; and, (5) description of the probable causes of the improper use or disclosure.
- d) The service provider shall (1) cooperate with the public jurisdiction as reasonably requested by the public jurisdiction to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and prevent any further data breach at the service provider's expense in accordance with applicable privacy rights, laws and regulations 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.
- e) If a data breach is a direct result of the service provider's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the service provider shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state or federal law; (3) a credit monitoring service (4) a website or a toll-free number and call center for affected individuals required by state law — all not to exceed the average per record per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach (or other similar publication if the named publication has not issued an updated average per record per cost in the last 5 years at the time of the data breach); and (5) complete all corrective actions as reasonably determined by service provider based on root cause. The service provider agrees that it shall not inform any third party of any data breach without first obtaining the public jurisdiction's prior written consent, other than to inform a complainant that the matter has been forwarded to the public jurisdiction's legal counsel and/or engage a third party with appropriate expertise and confidentiality protections for any reason connected to the data breach. Except with respect to where the service provider has an independent legal obligation to report a data breach, the service provider agrees that the public jurisdiction shall have the sole right to determine: (1) whether notice of the data breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies or others, as required by law or regulation, or otherwise in the public jurisdiction's discretion; and (2) the contents of such notice, whether any

type of remediation may be offered to affected persons, and the nature and extent of any such remediation. The service provider retains the right to report activity to law enforcement.

6. Notification of Legal Requests: The service provider shall contact the public jurisdiction upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the public jurisdiction's data under this contract, or which in any way might reasonably require access to the data of the public jurisdiction. The service provider shall not respond to subpoenas, service of process and other legal requests related to the public jurisdiction without first notifying the public jurisdiction, unless prohibited by law from providing such notice.

7. Termination and Suspension of Service:

- a) In the event of a termination of the contract, the service provider shall implement an orderly return of public jurisdiction data within the time period and format specified in the contract (or in the absence of a specified time and format, a mutually agreeable time and format) and after the data has been successfully returned, securely and permanently dispose of public jurisdiction data.
- b) During any period of service suspension, the service provider shall not take any action to intentionally erase any public jurisdiction data.
- c) In the event the contract does not specify a time or format for return of the public jurisdiction's data and an agreement has not been reached, in the event of termination of any services or agreement in entirety, the service provider shall not take any action to intentionally erase any public jurisdiction 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 service provider shall have no obligation to maintain or provide any public jurisdiction data and shall thereafter, unless legally prohibited, delete all public jurisdiction data in its systems or otherwise in its possession or under its control.

- d) The public jurisdiction 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 the Contract.
- e) The service provider shall securely dispose of all requested data in all of its forms, such as disk, CD/ DVD, backup tape and paper, when requested by the public jurisdiction. 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 public jurisdiction.

8. Background Checks: The service provider shall conduct criminal background checks in compliance with W.Va. Code §15-2D-3 and not utilize any staff to fulfill the obligations

of the contract, including subcontractors, 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 service provider shall promote and maintain an awareness of the importance of securing the public jurisdiction's information among the service provider's employees and agents.

9. Oversight of Authorized Persons: During the term of each authorized person's employment or engagement by service provider, service provider shall at all times cause such persons to abide strictly by service provider's obligations under this Agreement and service provider's standard policies and procedures. The service provider further agrees that it shall maintain a disciplinary process to address any unauthorized access, use or disclosure of personal data by any of service provider's officers, partners, principals, employees, agents or contractors.

10. Access to Security Logs and Reports: The service provider shall provide reports to the public jurisdiction in CSV format agreed to by both the service provider and the public jurisdiction. Reports shall include user access (successful and failed attempts), user access IP address, user access history and security logs for all public jurisdiction files and accounts related to this contract.

11. Data Protection Self-Assessment: The service provider shall perform a Cloud Security Alliance STAR Self-Assessment by completing and submitting the "Consensus Assessments Initiative Questionnaire" to the Public Jurisdiction Identified Contact. The service provider shall submit its self-assessment to the public jurisdiction prior to contract award and, upon request, annually thereafter, on the anniversary of the date of contract execution. Any deficiencies identified in the assessment will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

12. Data Center Audit: The service provider shall perform an audit of its data center(s) at least annually at its expense and provide a redacted version of the audit report upon request. The service provider may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit. Any deficiencies identified in the report or approved equivalent will entitle the public jurisdiction to disqualify the bid or terminate the contract for cause.

13. Change Control and Advance Notice: The service provider shall give 30 days, advance notice (to the public jurisdiction 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.

14. Security:

- a) At a minimum, the service provider's safeguards for the protection of data shall include: (1) securing business facilities, data centers, paper files, servers, back-up

systems and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implementing network, device application, database and platform security; 3) securing information transmission, storage and disposal; (4) implementing authentication and access controls within media, applications, operating systems and equipment; (5) implementing appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting background checks consistent with applicable law; and (6) providing appropriate privacy and information security training to service provider's employees.

- b) The service provider shall execute well-defined recurring action steps that identify and monitor vulnerabilities and provide remediation or corrective measures. Where the service provider's technology or the public jurisdiction's required dependence on a third-party application to interface with the technology creates a critical or high risk, the service provider shall remediate the vulnerability as soon as possible. The service provider must ensure that applications used to interface with the service provider's technology remain operationally compatible with software updates.
- c) Upon the public jurisdiction's written request, the service provider shall provide a high-level network diagram with respect to connectivity to the public jurisdiction's network that illustrates the service provider's information technology network infrastructure.

15. Non-disclosure and Separation of Duties: The service provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of public jurisdiction data to that which is absolutely necessary to perform job duties.

16. Import and Export of Data: The public jurisdiction shall have the ability to securely import, export or dispose of data in standard format in piecemeal or in entirety at its discretion without interference from the service provider. This includes the ability for the public jurisdiction to import or export data to/from other service providers identified in the contract (or in the absence of an identified format, a mutually agreeable format).

17. Responsibilities: The service provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the cloud services being provided. The technical and professional activities required for establishing, managing and maintaining the environments are the responsibilities of the service provider.

18. Subcontractor Compliance: The service provider shall ensure that any of its subcontractors to whom it provides any of the personal data or non-public data it receives hereunder, or to whom it provides any personal data or non-public data which the service provider creates or receives on behalf of the public jurisdiction, agree to the restrictions, terms and conditions which apply to the service provider hereunder.

19. Right to Remove Individuals: The public jurisdiction shall have the right at any time to require that the service provider remove from interaction with public jurisdiction any

service provider representative who the public jurisdiction believes is detrimental to its working relationship with the service provider. The public jurisdiction shall provide the service provider with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The service provider shall not assign the person to any aspect of the contract without the public jurisdiction's consent.

20. Business Continuity and Disaster Recovery: The service provider shall provide a business continuity and disaster recovery plan executive summary upon request. Lack of a plan will entitle the public jurisdiction to terminate this contract for cause.

21. Compliance with Accessibility Standards: The service provider shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.

22. Web Services: The service provider shall use web services exclusively to interface with the public jurisdiction's data in near real time when possible.

23. Encryption of Data at Rest: The service provider 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.

24. Subscription Terms: Service provider grants to a public jurisdiction a license to:

- a. Access and use the service for its business purposes;
- b. For SaaS, use underlying software as embodied or used in the service; and
- c. View, copy, upload, download (where applicable), and use service provider's documentation.

25. Equitable Relief: Service provider acknowledges that any breach of its covenants or obligations set forth in Addendum may cause the public jurisdiction irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, the public jurisdiction is entitled to seek equitable relief, including a restraining order, injunctive relief, specific performance and any other relief that may be available from any court, in addition to any other remedy to which the public jurisdiction may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity, subject to any express exclusions or limitations in this Addendum to the contrary.

AGREED:

Name of Agency:_____

Name of Vendor:_____

Signature:_____

Signature:_____

Title:_____

Title:_____

Date:_____

Date:_____

Appendix A

(To be completed by the Agency's Procurement Officer prior to the execution of the Addendum, and shall be made a part of the Addendum. Required information not identified prior to execution of the Addendum may only be added by amending Appendix A and the Addendum, via Change Order.)

Name of Service Provider/Vendor: _____

Name of Agency: _____

Agency/public jurisdiction's required information:

1. Will restricted information be processed by the service provider?
Yes ☐
No ☐
2. If yes to #1, does the restricted information include personal data?
Yes ☐
No ☐
3. If yes to #1, does the restricted information include non-public data?
Yes ☐
No ☐
4. If yes to #1, may the service provider store public jurisdiction data in a data center in an acceptable alternative data center location, which is a country that is not the U.S.?
Yes ☐
No ☐
5. Provide name and email address for the Department privacy officer:

Name: _____

Email address: _____

Vendor/Service Provider's required information:

6. Provide name and contact information for vendor's employee who shall serve as the public jurisdiction's primary security contact:

Name: _____

Email address: _____

Phone Number: _____

EXHIBIT A – Pricing Page
eDiscovery SaaS - (OT25112)

Section	Description	Unit of Measure	Estimated Quantity	Unit Cost	Extended Cost
4.1.1	Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00		\$ -
4.1.2	Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00		\$ -
4.1.7	Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00		\$ -
4.1.7.4	Contract Item #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00		\$ -
4.1.7.5	Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00		\$ -
4.1.7.7	Contract Item #6: e-Discovery SaaS Project Management	HR	100.00		\$ -
4.1.8	Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00		\$ -
4.1.7.6	Contract Item #8: Maintenance and Support Year 1	LS	1.00		\$ -
4.1.1	Optional Renewal Year 2: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00		\$ -
4.1.2	Optional Renewal Year 2: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00		\$ -
4.1.7	Optional Renewal Year 2:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00		\$ -
4.1.7.4	Optional Renewal Year 2: #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00		\$ -
4.1.7.5	Optional Renewal Year 2: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00		\$ -
4.1.7.7	Optional Renewal Year 2: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00		\$ -
4.1.8	Optional Renewal Year 2: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00		\$ -
4.1.7.6	Optional Renewal Year 2: Contract Item #8: Maintenance and Support Year 1	LS	1.00		\$ -
4.1.1	Optional Renewal Year 3: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00		\$ -
4.1.2	Optional Renewal Year 3: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00		\$ -
4.1.7	Optional Renewal Year 3:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00		\$ -
4.1.7.4	Optional Renewal Year 3: #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00		\$ -
4.1.7.5	Optional Renewal Year 3: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00		\$ -
4.1.7.7	Optional Renewal Year 3: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00		\$ -
4.1.8	Optional Renewal Year 3: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00		\$ -
4.1.7.6	Optional Renewal Year 3: Contract Item #8: Maintenance and Support Year 1	LS	1.00		\$ -
4.1.1	Optional Renewal Year 4: Contract Item #1: Unlimited Concurrent user license for e-discovery SaaS	LS	1.00		\$ -
4.1.2	Optional Renewal Year 4: Contract Item #2: One (1) Gigabyte Data e-Discovery SaaS usage Monthly Charge(data must rounded to the nearest whole gigabyte for billing/ auditing purposes see section 4.1.9)	EA	100.00		\$ -
4.1.7	Optional Renewal Year 4:Contract Item #3: Live individualized Agency virtual training session for up to 25 users per session (See specifications section 4.1.7 for further details)	EA	1.00		\$ -
4.1.7.4	Optional Renewal Year 4: #4: e-Discovery SaaS access to an online knowledge base or help center.	LS	1.00		\$ -
4.1.7.5	Optional Renewal Year 3: Contract Item #5: Initial Setup and configuration of eDiscovery SaaS	LS	1.00		\$ -
4.1.7.7	Optional Renewal Year 4: Contract Item #6: e-Discovery SaaS Project Management	HR	100.00		\$ -
4.1.8	Optional Renewal Year 4: Contract Item #7: e-Discovery SaaS Technical Support	HR	100.00		\$ -
4.1.7.6	Optional Renewal Year 4: Contract Item #8: Maintenance and Support Year 1	LS	1.00		\$ -
Total Cost				\$	-

See Exhibit A Pricing Page Attached as a separate Excel attachment.

Please refer to Specification 5.3 for more information.

Contract will be evaluated on all lines but only awarded on first year. Renewal options for years 2, 3, and 4 will be initiated by the Agency, agreed to by the Vendor and processed by the West Virginia Purchasing Division as Change Orders for subsequent years.

Vendor Signature:

Date: