verizon
4700 MacCorkle Ave. S.E.
Charleston, WV 25304
304-356-3395

January 22, 2015

Guy Nisbet
2019 Washington Street East
Charleston, WV 25305-0130

RE: CPR1500000001

Dear Mr. Nisbet:

Verizon is pleased to submit its proposal for a Network Security and Vulnerability Assessment.

Verizon is one of the world's leading providers of communications services. Verizon serves more than 139 million customer connections (wireless, wireline, broadband and TV) every day and is the leader in serving 205.2 million wireless customers. Verizon is a global leader in delivering innovation in communications, information and entertainment, with approximately $120.6 billion in 2013 annual revenue. Verizon's global presence extends to 75 countries in the Americas, Europe, Asia and the Pacific. Verizon ranks 16 in the Fortune 500.

As one of the world's leading managed security services providers, we offer:
•Flexible delivery options for your specific needs.
•Customizable solutions to meet your technical requirements.
•Vendor support, helping to limit conflicts that could affect your security.

Gartner has positioned Verizon as a Leader in its Magic Quadrant for Global Managed Security Services Providers for the fourth consecutive year.

Verizon will provide outstanding service quality, product flexibility, and a local dedicated Account Team. As a recognized leader in security, and the technologies that need to be protected, Verizon can help you meet your specific security challenges head-on.

Verizon commits to provide the services as described in this Proposal. I also give my personal commitment of service to the State of West Virginia. I look forward to continuing our business relationship and building an even stronger partnership with the State of West Virginia.

Sincerely,

Sandra Hawkins

Sandra Hawkins
Senior Account Manager
Authorized Contact
Verizon
304-356-3395
sandra.k.hawkins@verizon.com

NATURE OF PROPOSAL

This RFQ response is submitted to the WV Consolidated Public Retirement Board (referred to herein as "Customer") by Verizon Business Network Services Inc. on behalf of its affiliate, MCI Communications Services, Inc. d/b/a Verizon Business Services (individually and collectively referred to herein as "Verizon"). Verizon does not consider this RFQ response as legally binding to provide the professional services until an SOW is signed and a mutual understanding is reached. Verizon does not take exception to the RFQ terms and conditions. However, as permitted in the WV Purchasing Division's Procedures Handbook, Section 7.2.19, Verizon also submits additional industry-specific terms and conditions reflected in Verizon's Statement of Work (SOW), which is incorporated and included in Verizon's response. Verizon is also willing to sign a WV-96A and understands Verizon's SOW is in the last order of precedence and shall not supersede the WV-96A terms and conditions where a conflict arises.

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

State of West Virginia
Request for Quotation
10 — Consulting

Proc Folder: 15921
Doc Description: Addendum2 for CRFQ CPR15*1
Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2015-01-09	2015-01-22 13:30:00	CRFQ 0203 CPR1500000001	3

BID RECEIVING LOCATION

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

VENDOR

Vendor Name, Address and Telephone Number:
Verizon Business Network Svc Inc on behalf of MCI Communication Svc Inc
d/b/a Verizon Business Svcs
4700 MacCorkle Av SE
Charleston, WV 25304

FOR INFORMATION CONTACT THE BUYER
Guy Nisbet
(304) 558-2596
guy.l.nisbet@wv.gov

Signature X Marsha K. Harrell FEIN # 47-0751768 DATE 1/21/15

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

Marsha K Harrell
Senior Consultant
Pricing/Contract Management

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

SOLICITATION NUMBER: CRQS CPR1500000002
Addendum Number: 02

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[✓] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[ ] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Description of Modification to Solicitation:

Addendum issued to publish and distribute the following information to the vendor community.

1. Vendor submitted questions and Agency's responses.

2. Bid opening Changed from: 01/15/15 at 1:30 PM. EST
Bid Opening Now: 01/22/15 at 1:30 PM. EST.

No other Changes.

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

CRFQ CPR15*1
Vendor Submitted Questions
12/22/2014

Q.1. The first question is from page 22. The RFQ is looking for a 2 year contract with option for 4 one-year renewals. However, the next paragraph talks about a series of 5 assessments to be conducted over 4 years (in conjunction with the implementation of a new system by D&T).

A.1. Please reference the response to Question 12 for further information as to the timing of the work.

Q.2. Page 22-23 indicate: Approximately 85 Windows 7 workstations, Windows Servers, Cisco switches, Hosted site, Disaster recovery site, Need to know total live IPs in use.

A.2. While the number will change we currently have approximately 160 live IPs and an additional 90 IP telephones with their own range of IP addresses.

Q.3. 4.1.2.1 # of policies and procedures?

A.3. The policies and procedures for the WVOT can be found at:

http://www.technology.wv.gov/security/Pages/policies-issued-by-the-cto.aspx

Q.4. 4.1.2.4 # and types of servers, firewalls and IDS's and configurations for review?

A.4. The WVCPRB firewall is a Cisco ASA 5505. There are 250 lines of access list.

The server environment for the new system is in the procurement process. The new system will be a Windows operating system, running on HP blade servers. The new system will include development, test and production environments.

Q.5. 4.1.2.5 Remediation Services – expected scope?

A.5. The expectation is that WVCPRB data will be secure. The scope of the services will be dependent upon the nature of any vulnerabilities identified, and the ability of the prime contractor to address those vulnerabilities. Remediation is a responsibility of the prime contractor, although the NVA vendor awarded in this RFQ will be expected to assist in resolving any identified vulnerabilities.

Q.6. 4.1.4.1 # and type of firewall and # of rules for Firewall Architecture Review?

A.6. Please reference the response to Question 4.

Q.7. 4.1.5.1 IPT of 15 laptop & desktop systems?

A.7. A response cannot be provided for this question, because the term "IPT" is not clear in the stated question.

Q.8. Additionally, I would like to request a 30 day extension due to the timing of the RFQ. We will need answers to the questions above and there are very few working days between Dec 22nd and Jan 6th. Furthermore, it is extremely difficult to produce an RFQ response over the holidays due to the vacation schedules of the staff and executives.

A.8. The bid opening date has been extended to 1/22/2015.

Q.9. Will you consider out of state firms for this project?

A.9. Yes.

Q. 10. Are you able to share the name of the Pension Administration System? Or was it developed specifically for WVCPRB?

A.10. Deloitte Pension Administration Solution (DPAS). The base DPAS system will be specifically customized for WVCPRB.

Q.11. At each of the 5 Assessment phases, are you expecting all of the service be performed? Meaning, are you looking for an updated DLP gap analysis at each phase as well as internal and external system vulnerability assessments?

a. For example, I understand that the first assessment will focus on the data conversion server. Are you looking for a DLP gap analysis of the server during this phase? Or just an internal and external vulnerability assessment of the server?

A.11. Penetration testing should be performed at each assessment. Data Loss Prevention Gap Analysis should be performed for each rollout phase.

Q.12. I would like to verify the timing of each phase. My understanding is:

a. first assessment will be completed shortly after the contract award – approx. Q1 2015
b. second assessment shortly after the completion of the first – approx. Q2 2015
c. third assessment 18 months after the completion of the 2nd – approx. Q4 2016
d. fourth assessment one year after the completion of the 3rd – approx. Q4 2017
e. fifth assessment one year after the completion of the 4th – approx. Q1 2019

A.12. Based on the prime contractor's current implementation schedule, the following is an estimation of when the assessments may occur:

1st Assessment – Q1 2015
2nd Assessment – Q2 2015
3rd Assessment – Beginning Q4 2015
4th Assessment – End of Q3 2016
5th Assessment – End of Q3 2017

The dates are based on the current project schedule, and are subject to change.

Q.13. I understand that Deloitte is working to implement the new pension administration system. Will this project involve working alongside, or in conjunction with, Deloitte staff?

A.13. The NVA vendor will report to CPRB leadership, not to Deloitte. The project will require working in conjunction with Deloitte staff.

Q.14. Are you expecting onsite staff or are you open to working with the vendor on a mostly remote basis – with some onsite work throughout the project?
a. Is there an expectation of a certain number of hours/days per week of onsite work?

A.14. The successful performance of the work will require some on site work. However bidders are encouraged to describe the nature of the on-site vs. off-site hours in a detailed manner.

Q.15. If we are submitting our bid via hardcopy – how many copies of the documents do you require? Do you also require an electronic copy via CD or other?

A.15. The vendor should submit six hardcopies and six CDs.

Q.16. In addition to the five assessment phases, it appears there is an additional phase to include a roadmap for WVCPRB to ensure their DLP meets Best Practices. Is the expectation for this phase a report listing steps and procedures to complete for DLP and a meeting with stakeholders to explain? Or are you expecting more involvement in the implementation of the recommendations?

A.16. The expectation is for a report listing the steps and procedures to complete for DLP and a meeting with stakeholders to explain the Roadmap and any recommendations.

Q.17. Must the vendor be registered with the state of WV prior to being considered for any bid? Or, will the vendor be given time to register after being notified of the award?

A.17. The vendor does not need to be registered prior to submitting a bid. The vendor must be registered prior to the issuance of a purchase order for the contract.

Q.18. The Certified Information Systems Security Professional (CISSP) is recognized by the Department of Defense in Manual DoD 8570.01 as an approved Information Assurance certification and carries with it an ANSI Approved Continuing Education program which is audited and mandatory for individuals to continue to maintain the certification. The RFP states "Either the Expert level or Senior Level consultant should have an OSCP (Offensive Security Certified Professional) or equivalent level of certification for Penetration Testing." Does the buyer consider CISSP as an acceptable/equivalent level of certification?

A.18. The alternate certification is acceptable.

Q.19. Section 4.1.9 Please clarify the inclusion of subcontractors; subcontractors are mentioned i.e. section 4.1.9.1, however, section 4.1.9.3 states full-time employees.

A.19. Section 4.1.9.1 refers to a confirmation that the vendor nor any of the vendor's representatives have been convicted of, pled guilty to, pled nolo contendere or were named as an unindicted co-conspirator to any felony.

Section 4.1.9.3 requests confirmation of the vendor's key staff and affirmation that those individuals are full-time employees of the vendor.

Q.20. What additional information can you tell us about your systems that are in scope? Can you clarify if the web portals are in scope? What technologies are they build on and how many SQL databases are in scope?

A.20. The scope of the vulnerability assessment will include at a minimum, a scan of external entry points into the network, a review of all devices on the network with static IP addresses and a random 10% sample of the DHCP devices and, to the extent they apply, a review of server, firewall, and IDS configurations. The definition of the full scope of the assessment will be the responsibility of the third party organization performing the assessment and approved by WVCPRB.

Q.21. 4.1.6 DLP Gap Analysis We need to know how many sites would be involved in the audit (in scope). Also, if it would help to know what they are currently doing in terms of DLP.

A.21. Three sites will be involved in the assessment.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CPR1500000001

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. 6
[✓] Addendum No. 2	[ ] Addendum No. 7
[ ] Addendum No. 3	[ ] Addendum No. 8
[ ] Addendum No. 4	[ ] Addendum No. 9
[ ] Addendum No. 5	[ ] 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.

Verizon Business Network Svc Inc., on behalf of MCI Communications Svc Inc.
d/b/a Verizon Business Svcs
Company

Marsha K. Harrell
Authorized Signature

Marsha K Harrell
Senior Consultant
Pricing/Contract Management

1/21/15
Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.
Revised 6/8/2012

Purchasing Divison
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Request for Quotation
10 — Consulting

Proc Folder: 15921
Doc Description: Addendum2 for CRFQ CPR15*1
Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2015-01-09	2015-01-22 13:30:00	CRFQ 0203 CPR1500000001	3

BID RECEIVING LOCATION

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

VENDOR

Vendor Name, Address and Telephone Number:
Verizon Business Network Svc Inc., on behalf of MCI Communications Svc Inc.,
d/b/a Verizon Business Svcs
4700 MacCorkle Ave SE
Charleston, WV 25304

FOR INFORMATION CONTACT THE BUYER
Cindy L Adkins
(304) 558-3570
cindy.l.adkins@wv.gov

Signature X Marsha K. Harrell **FEIN #** 47-0751768 **DATE** 1/21/15

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

Marsha K Harrell
Senior Consultant
Pricing/Contract Management

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

State of West Virginia
Request for Quotation
10 — Consulting

Proc Folder: 15921
Doc Description: Addendum1for CRFQ CPR15*1
Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2014-12-29	2015-01-15 13:30:00	CRFQ 0203 CPR1500000001	2

BID RECEIVING LOCATION

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

VENDOR

Vendor Name, Address and Telephone Number:
Verizon Business Network Svc. Inc., on behalf of MCI Communications Svc. Inc., d/b/a Verizon Business Svcs
4700 MacCorkle Av SE
Charleston, WV 25304

FOR INFORMATION CONTACT THE BUYER
Guy Nisbet
(304) 558-2596
guy.l.nisbet@wv.gov

Signature X Marshak. Harrell **FEIN #** 47-0751768 **DATE** 1/21/15

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

Marsha K Harrell
Senior Consultant
Pricing/Contract Management

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

SOLICITATION NUMBER: CRQS CPR1500000002
Addendum Number: 01

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

[✓] Modify bid opening date and time

[ ] Modify specifications of product or service being sought

[ ] Attachment of vendor questions and responses

[ ] Attachment of pre-bid sign-in sheet

[ ] Correction of error

[ ] Other

Description of Modification to Solicitation:

Addendum issued to publish and distribute the following information to the vendor community. Bid opening is being moved to allow Agency time to address the Vendor questions that were presented. An Addendum will be published at a latter date to address these questions and the Agency responses.

Bid Opening was: 01/06/15 at 1:30 PM. EST
Bid Opening Now: 1/15/15 at 1:30 PM. EST.

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.

2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CPR150000001

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)

[X] Addendum No. 1	[ ] Addendum No. 6
[X] Addendum No. 2	[ ] Addendum No. 7
[ ] Addendum No. 3	[ ] Addendum No. 8
[ ] Addendum No. 4	[ ] Addendum No. 9
[ ] Addendum No. 5	[ ] 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.

Verizon Business Network Svc Inc, on behalf of MCI Communications Svc Inc
d/b/a Verizon Business Svcs
Company

Marsha K Harrell
Authorized Signature

Marsha K Harrell
Senior Consultant
Pricing/Contract Management

1/21/15
Date

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

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

State of West Virginia
Request for Quotation
10 — Consulting

Proc Folder: 15921
Doc Description: Information Security and Network Vulnerability Assessment
Proc Type: Central Contract - Fixed Amt

Date Issued	Solicitation Closes	Solicitation No	Version
2014-12-05	2015-01-06 13:30:00	CRFQ 0203 CPR1500000001	1

BID RECEIVING LOCATION

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

VENDOR

Vendor Name, Address and Telephone Number:
Verizon Business Network Svc Inc, on behalf of MCI Communications Svc Inc
d/b/a Verizon Business Svcs
4700 MacCorkle Av SE
Charleston WV 25304

FOR INFORMATION CONTACT THE BUYER
Guy Nisbet
(304) 558-2596
guy.l.nisbet@wv.gov

Signature X Marsha K. Harrell FEIN # 47-0751768 DATE 1/21/15

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

Marsha K Harrell
Senior Consultant
Pricing/Contract Management

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

INVOICE TO	SHIP TO
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

[illegible]	[illegible]
CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV24304 US	CONSOLIDATED PUBLIC RETIREMENT 4101 MACCORKLE AVE SE CHARLESTON WV 25304 US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
5	network security and vulnerability assessment	0.00000	LS		

Comm Code	Manufacturer	Specification	Model #
81111801			

Extended Description :

Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation

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. **PREBID MEETING:** The item identified below shall apply to this Solicitation.

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

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

   ☐ 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 person attending the pre-bid meeting may represent more than one Vendor.

An attendance sheet provided at the pre-bid meeting shall serve as the official document verifying attendance. The State will not accept any other form of proof or documentation to verify 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. Additionally, the person attending the pre-bid meeting should include the Vendor's E-Mail address, phone number, and Fax number on the attendance sheet. 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.

All Vendors should arrive prior to the starting time for the pre-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.

Questions submitted at least five business days prior to a scheduled pre-bid will be discussed at the pre-bid meeting if possible. 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 in order 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 e-mails should have solicitation number in the subject line.

   Question Submission Deadline: December 22nd, 2014 at 11:00 AM. EST.

   Submit Questions to: Guy Nisbet, Senior Buyer
   2019 Washington Street, East
   Charleston, WV 25305
   Fax: (304) 558-4115 (Vendors should not use this fax number for bid submission)
   Email: Guy.L.Nisbet@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 electronically through wvOASIS or signed and delivered by the Vendor to the Purchasing Division at the address listed below on or before the date and time of the bid opening. 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. The Purchasing Division will not accept bids, modification of bids, or addendum acknowledgment forms via e-mail. Acceptable delivery methods include electronic submission via wvOASIS, hand delivery, delivery by courier, or facsimile. The bid delivery address is:

   Department of Administration, Purchasing Division
   2019 Washington Street East
   Charleston, WV 25305-0130

A bid that is not submitted electronically through wvOASIS should contain the information listed below on the face of the envelope or the bid may be rejected by the Purchasing Division.:

SEALED BID:
BUYER:
SOLICITATION NO.:
BID OPENING DATE:
BID OPENING TIME:
FAX NUMBER:

In the event that Vendor is responding to a request for proposal, and choses to respond in a manner other than by electronic submission through wvOASIS, the Vendor shall submit one original technical and one original cost proposal plus N/A convenience copies of each to the Purchasing Division at the address shown above. Additionally, if Vendor does not submit its bid through wvOASIS, the Vendor should identify the bid type as either a technical or cost proposal on the face of each bid envelope submitted in response to a request for proposal as follows:

BID TYPE: (This only applies to CRFP)

☐ Technical

☐ Cost

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).

Bid Opening Date and Time: January 6th, 2015 at 1:30 PM.EST.
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 Acknowledgment Form, a copy of which is included herewith. 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. **ALTERNATES:** 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 should 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.

11. **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.

12. **COMMUNICATION LIMITATIONS:** In accordance with West Virginia Code of State Rules §148-1-6.6, 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.

13. **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.

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

15. **PREFERENCE:** Vendor Preference may only be granted upon written request and only in accordance with the West Virginia Code § 5A-3-37 and the West Virginia Code of State Rules. A Vendor Preference Certificate form has been attached hereto to allow Vendor to apply for the preference. Vendor's failure to submit the Vendor Preference Certificate form with its bid will result in denial of Vendor Preference. Vendor Preference does not apply to construction projects.

16. **SMALL, WOMEN-OWNED, OR MINORITY-OWNED BUSINESSES:** For any solicitations publicly advertised for bid, in accordance with West Virginia Code §5A-3-37(a)(7) 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. Preference for a non-resident small, women-owned, or minority owned business shall be applied in accordance with W. Va. CSR § 148-22-9.

17. **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 § 148-1-4.6.

GENERAL TERMS AND CONDITIONS:

1. **CONTRACTUAL AGREEMENT:** Issuance of a Award Document signed by the Purchasing Division Director, or his designee, and approved as to form by the Attorney General's office constitutes acceptance of this Contract made by and between the State of West Virginia and the Vendor. Vendor's signature on its bid 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. **"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.

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

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

   2.5. **"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.

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

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

   2.8. **"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: This Contract becomes effective on award and extends for a period of two (2) year(s).

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 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. Renewal of this Contract is limited to four (4) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed 48 months in total. Automatic renewal of this Contract is prohibited. Notwithstanding the foregoing, Purchasing Division approval is not required on agency delegated or exempt purchases. Attorney General approval may be required for vendor terms and conditions.

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, the vendor agrees that maintenance, monitoring, or warranty services will be provided for one year thereafter with an additional _____ successive one year renewal periods or multiple renewal periods of less than one year provided that the multiple renewal periods do not exceed _____ months in total. Automatic renewal of this Contract is prohibited.

☐ **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.

☐ **Other:** See attached.

4. **NOTICE TO PROCEED:** Vendor shall begin performance of this Contract immediately upon receiving notice to proceed unless otherwise instructed by the Agency. Unless otherwise specified, the fully executed Award Document will be considered notice to proceed.

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 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.

6. **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.

7. **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.

8. **REQUIRED DOCUMENTS:** All of the items checked below must be provided to the Purchasing Division by the Vendor as specified below.

☐ **BID BOND:** All Vendors shall furnish a 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.

☐ **PERFORMANCE BOND:** The apparent successful Vendor shall provide a performance bond in the amount of _____. The performance bond must be received by the Purchasing Division prior to Contract award. On construction contracts, the performance bond must be 100% of the Contract value.

☐ **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.

In lieu of the Bid Bond, Performance Bond, and Labor/Material Payment 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 a bond must be of the same amount and delivered on the same schedule as the bond it replaces. A letter of credit submitted in lieu of a performance and labor/material payment bond will only be allowed for projects under $100,000. Personal or business checks are not acceptable.

☐ **MAINTENANCE BOND:** The apparent successful Vendor shall provide a two (2) year maintenance bond covering the roofing system. The maintenance bond must be issued and delivered to the Purchasing Division prior to Contract award.

☑ **INSURANCE:** The apparent successful Vendor shall furnish proof of the following insurance prior to Contract award and shall list the state as a certificate holder:

☑ **Commercial General Liability Insurance:** In the amount of $1,000,000.00 _____ or more.

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

☐

☐

☐

☐

☐

The apparent successful Vendor shall also furnish proof of any additional insurance requirements contained in the specifications prior to Contract award regardless of whether or not that insurance requirement is listed above.

☐ **LICENSE(S) / CERTIFICATIONS / PERMITS:** In addition to anything required under the Section entitled Licensing, of the General Terms and Conditions, the apparent successful Vendor shall furnish proof of the following licenses, certifications, and/or permits prior to Contract award, in a form acceptable to the Purchasing Division.

☐

☐

☐

☐

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

9. **WORKERS' COMPENSATION INSURANCE:** The apparent successful 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. **LITIGATION BOND:** The Director reserves the right to require any Vendor that files a protest of an award to submit a litigation bond in the amount equal to one percent of the lowest bid submitted or $5,000, whichever is greater. The entire amount of the bond shall be forfeited if the hearing officer determines that the protest was filed for frivolous or improper purpose, including but not limited to, the purpose of harassing, causing unnecessary delay, or needless expense for the Agency. All litigation bonds shall be made payable to the Purchasing Division. In lieu of a bond, the protester may submit a cashier's check or certified check payable to the Purchasing Division. Cashier's or certified checks will be deposited with and held by the State Treasurer's office. If it is determined that the protest has not been filed for frivolous or improper purpose, the bond or deposit shall be returned in its entirety.

11. **LIQUIDATED DAMAGES:** Vendor shall pay liquidated damages in the amount of _____ for _____.
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.

12. **ACCEPTANCE/REJECTION:** The State may accept or reject any bid in whole, or in part. Vendor's signature on its bid signifies acceptance of the terms and conditions contained in the Solicitation and Vendor agrees to be bound by the terms of the Contract, as reflected in the Award Document, upon receipt.

13. **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.

14. **PAYMENT:** Payment in advance is prohibited under this Contract. Payment may only be made after the delivery and acceptance of goods or services. The Vendor shall submit invoices, in arrears.

15. **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.

16. **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 § 148-1-7.16.2.

17. **TIME:** Time is of the essence with regard to all matters of time and performance in this Contract.

18. **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.

19. **COMPLIANCE:** 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 law.

20. **PREVAILING WAGE:** On any contract for the construction of a public improvement, Vendor and any subcontractors utilized by Vendor shall pay a rate or rates of wages which shall not be less than the fair minimum rate or rates of wages (prevailing wage), as established by the West Virginia Division of Labor under West Virginia Code §§ 21-5A-1 et seq. and available at http://www.sos.wv.gov/administrative-law/wagerates/Pages/default.aspx. Vendor shall be responsible for ensuring compliance with

prevailing wage requirements and determining when prevailing wage requirements are applicable. The required contract provisions contained in West Virginia Code of State Rules § 42-7-3 are specifically incorporated herein by reference.

21. **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.

22. **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). No Change shall be implemented by the Vendor until such time as the Vendor receives an approved written change order from the Purchasing Division.

23. **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.

24. **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.

25. **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. Notwithstanding the foregoing, Purchasing Division approval may or may not be required on certain agency delegated or exempt purchases.

26. **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.

27. **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.

28. **BANKRUPTCY:** In the event the Vendor files for bankruptcy protection, the State of West Virginia may deem this Contract null and void, and terminate this Contract without notice.

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

30. **DISCLOSURE:** Vendor's response to the Solicitation and the resulting Contract are considered public documents and will be disclosed to the public in accordance with the laws, rules, and policies governing the West Virginia Purchasing Division. Those laws include, but are not limited to, the Freedom of Information Act found in West Virginia Code §§ 29B-1-1 et seq. and the competitive bidding laws found West Virginia Code §§ 5A-3-1 et seq., 5-22-1 et seq., and 5G-1-1 et seq.

If a Vendor considers any part of its bid to be exempt from public disclosure, Vendor must so indicate by specifically identifying the exempt information, identifying the exemption that applies, providing a detailed justification for the exemption, segregating the exempt information from the general bid information, and submitting the exempt information as part of its bid but in a segregated and clearly identifiable format. Failure to comply with the foregoing requirements will result in public disclosure of the Vendor's bid without further notice. A Vendor's act of marking all or nearly all of its bid as exempt is not sufficient to avoid disclosure and WILL NOT BE HONORED. Vendor's act of marking a bid or any part thereof as "confidential" or "proprietary" is not sufficient to avoid disclosure and WILL NOT BE HONORED. A legend or other statement indicating that all or substantially all of the bid is exempt from disclosure is not sufficient to avoid disclosure and WILL NOT BE HONORED. Additionally, pricing or cost information will not be considered exempt from disclosure and requests to withhold publication of pricing or cost information WILL NOT BE HONORED.

Vendor will be required to defend any claimed exemption for nondisclosure in the event of an administrative or judicial challenge to the State's nondisclosure. Vendor must indemnify the State for any costs incurred related to any exemptions claimed by Vendor. Any questions regarding the applicability of the various public records laws should be addressed to your own legal counsel prior to bid submission.

31. **LICENSING:** In accordance with West Virginia Code of State Rules §148-1-6.1.7, 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. 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.

32. **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.

33. **VENDOR CERTIFICATIONS:** By signing its bid or entering into this Contract, Vendor certifies (1) that its bid or offer was made without prior understanding, agreement, or connection with any corporation, firm, limited liability company, partnership, person or entity submitting a bid or offer for the same material, supplies, equipment or services; (2) that its bid or offer is in all respects fair and without collusion or fraud; (3) 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; and (4) that it has reviewed this Solicitation in its entirety; understands the requirements, terms and conditions, and other information contained herein. Vendor's signature on its bid or offer also affirms that neither it nor its representatives have any interest, nor shall 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. The individual signing this bid or offer on behalf of Vendor certifies that he or she is authorized by the Vendor to execute this bid or offer or any documents related thereto on Vendor's behalf; that he or she is authorized to bind the Vendor in a contractual relationship; and that, to the best of his or her knowledge, the Vendor has properly registered with any State agency that may require registration.

34. **PURCHASING CARD ACCEPTANCE:** The State of West Virginia currently utilizes a Purchasing Card program, administered under contract by a banking institution, to process payment for goods and services. The Vendor must accept the State of West Virginia's Purchasing Card for payment of all orders under this Contract unless the box below is checked.

    ☐ Vendor is not required to accept the State of West Virginia's Purchasing Card as payment for all goods and services.

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 an y 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. **PURCHASING AFFIDAVIT:** In accordance with West Virginia Code § 5A-3-10a, all Vendors are required to sign, notarize, and submit the Purchasing Affidavit stating that neither the Vendor nor a related party owe a debt to the State in excess of $1,000. The affidavit must be submitted prior to award, but should be submitted with the Vendor's bid. A copy of the Purchasing Affidavit is included herewith.

38. **ADDITIONAL AGENCY AND LOCAL GOVERNMENT USE:** This Contract may be utilized by and extends to other agencies, spending units, and political subdivisions of the State of West Virginia; county, municipal, and other local government bodies; and school districts ("Other Government Entities"). This Contract shall be extended to the aforementioned Other Government Entities on the same prices, terms, and conditions as those offered and agreed to in this Contract. If the Vendor does not wish to extend the prices, terms, and conditions of its bid and subsequent contract to the Other Government Entities, the Vendor must clearly indicate such refusal in its bid. A refusal to extend this Contract to the Other Government Entities shall not impact or influence the award of this Contract in any manner.

39. **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.

40. **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.requisitions@wv.gov.

41. **BACKGROUND CHECK:** In accordance with W. Va. Code § 15-2D-3, the Director of the Division of Protective Services shall require any service provider whose employees are regularly employed on the grounds or in the buildings of the Capitol complex or who have access to sensitive or critical information to submit to a fingerprint-based state and federal background inquiry through the state repository. The service provider is responsible for any costs associated with the fingerprint-based state and federal background inquiry.

    After the contract for such services has been approved, but before any such employees are permitted to be on the grounds or in the buildings of the Capitol complex or have access to sensitive or critical information, the service provider shall submit a list of all persons who will be physically present and working at the Capitol complex to the Director of the Division of Protective Services for purposes of verifying compliance with this provision.

    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.

42. **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 heath, basic oxygen, electric furnace, Bessemer or other steel making process. The Purchasing Division Director may, in writing, authorize the use of foreign steel products if:

    c. 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

d. 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.

43. **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.

SPECIFICATIONS

1 **PURPOSE AND SCOPE:** The West Virginia Purchasing Division is soliciting bids on behalf of West Virginia Consolidated Public Retirement Board to establish a contract for information security and network vulnerability assessment.

The contract will be for a two (2) year period, with the possibility of four (4) one-year renewals.

The West Virginia Consolidated Public Retirement Board (WVCPRB) is requesting quotations from information security consulting vendor for an Information Security and Network Vulnerability Assessment (Assessment). The Assessment will need to be performed at five distinct milestone points over the next four (4) years in conjunction with the new pension administration system being implemented Deloitte Consulting LLP.

The First Assessment: will be focused on the data conversion server(s). **The Second Assessment:** will be focused on the remaining installation of the development and test environments. **The Third Assessment:** will be approximately eighteen months later, and just prior to the migration to the new production environment. **The Fourth Assessment:** will be approximately one year later and just prior to the final phase deployment of member self-service features. **The Fifth and Final Assessment:** will be approximately one year after the release of the final phase, occurring during the system warranty period and prior to final handoff of the solution to WVCPRB.

The Consolidated Public Retirement Board is responsible for the administration of all State retirement plans for educational employees, public employees, deputy sheriffs, judges, and public safety personnel, with the exclusion of some higher educational plans. The plans administered include defined benefit and defined contribution retirement systems. Benefits include service retirement, disability and survivor benefits, and access to health care coverage for benefit recipients and their dependents. General administration and management of the plans by the Retirement Board is established under West Virginia law.

Current Operating Environment: CPRB employs approximately 80 people. The current computing environment includes:

- The main facility located at MacCorkle Avenue, Charleston, WV, and the current systems site located at the Capitol Complex in Charleston, West Virginia.
- Approximately 85 PC workstations Windows 7
- Windows servers
- Office 365 environment

- Cisco Ethernet switches and fiber runs for LAN
- 10Mb connection to state backbone and rely on state's primary firewall services

Expectations: In addition, at the time of the initial assessment, the new development environment will include:

- The main facility located at MacCorkle Avenue, Charleston, WV, the production hosting site located in downtown Charleston, West Virginia, and the remote Disaster Recovery facility (hot site) located in rural West Virginia.
- VMware Server software, version 5.5

Also, at the time of the last assessment, the technical environment will also include a full production and disaster recovery site:

- The main facility located at MacCorkle Avenue, Charleston, WV. the production hosting site located at the State Capitol Complex in Charleston, West Virginia, and the remote business continuity facility (hot site) located in rural West Virginia
- Browser based Windows .Net framework, Visual Studio, version 2012
- SQL Server, version2012, VM Ware, version 5.5, SharePoint, version2013, MS Dynamics, version2013
- 4 separate technical environments including Development, Test, Production, and Training/Ad Hoc environments
- Web portals for employers, staff, and participant members

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 **"Contract Services"** means information security and network vulnerability assessment.

2.2 **"Pricing Page"** means the pages contained in wvOASIS or attached as ***Exhibit "A,"*** upon which the Vendor should list its proposed price for the Contract Services.

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

2.4 **"Common Vulnerability Scoring System"** (CVSS) is a free and open industry standard for assessing the severity of computer system security vulnerabilities.

2.5 **Security Content Automation Protocol** (SCAP) is a method for using commonly accepted standards to enable automated vulnerability management and security policy compliance metrics.

2.6 **"Expert"** – Vendor staff having fifteen or greater years of experience in the required services described in this RFQ. The Expert level consultant will use current information security technology disciplines and practices to ensure the confidentiality, integrity and availability of agency information assets in accordance with established standards and procedures. Provides knowledge and counsel on changing regulatory, threat, and technology landscapes to develop or maintain security policies and standards, and ensure the systems are secure. Either the Expert level or Senior Level consultant should have an OSCP (Offensive Security Certified Professional) or equivalent level of certification for Penetration Testing.

2.7 **"Senior"** – Vendor staff having ten or more years of experience in the required services. The Senior level staff performs all procedures necessary to ensure the safety of information systems assets and to protect systems from intentional or inadvertent access or destruction. This role will interact with CPRB to understand the overall security needs and may require familiarity with domain structures, user authentication, and digital signatures. The Senior level vendor conducts accurate evaluation of the level of security required and must be able to weigh business needs against security concerns and articulate issues to management. Either the Expert level or Senior Level consultant should have an OSCP (Offensive Security Certified Professional) or equivalent level of certification for Penetration Testing.

2.8 **"Specialist"** – Vendor staff having five or more years of service, with a greater depth of knowledge and experience than a technician. The Specialist level will assist the more senior level consultants in developing the deliverables in this RFQ, and will be knowledgeable on the changing regulatory, threat, and technology landscapes.

2.9 **"Technician"** – Vendor staff having five or more years of service, possessing the basic knowledge and abilities to perform the required work. Works under the general direction of the Specialist, Senior, or Expert level consultant and performs activities that support the deliverables in this RFQ.

3 QUALIFICATIONS

3.1 Subsequent to contract award, but prior to the start of work, all firm personnel assigned to the engagement must sign and accept a non-disclosure and confidentiality agreement. An example of the WVCPRB Confidentiality Agreement is included as ***Attachment 4***.

3.2 Vendor should provide documentation of similar work performed in the successful performance of information security and network vulnerability assessments in compliance with the ***National Institute of Standards and Technology Special Publication 800-37***[1] please document such references on Attachment 1.

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 Primary persons responsible for the engagement must have a minimum of 5 years of experience in security design and testing of Microsoft .Net, Microsoft SQL Server, and Cisco Systems Networking. As part of the solicitation response, please provide copies of professional certifications which support this requirement and provide the pertinent reference information on ***Attachment 2***. Perform the Information Security and Network Vulnerability Assessment in accordance with the National Institute of Standards and Technology Standards referenced in Section 3.3.

4.1.2 Prioritize and rank the discovered vulnerabilities using the **Common Vulnerability Scoring System (CVSS)**. This will include at a minimum:

4.1.2.1 Evaluation of the security policy and procedures

4.1.2.2 A scan of external entry points into the network

4.1.2.3 A review of all of the devices on the network with static IP addresses

4.1.2.4 A review of the server, firewall, and IDS configurations

4.1.2.5 Provide Post-Assessment Remediation Services if prime contractor cannot address the identified vulnerabilities.

4.1.3 For each assessment, provide a written report, including at a minimum, the following:

[1] Reference included as Exhibit B.

4.1.3.1 Executive Summary

4.1.3.2 Summary of Target Environment

4.1.3.3 Scope (including systems assessed and method used)

4.1.3.4 Findings (in social engineering, data loss prevention, firewall architecture and policy, and endpoint assessment)

4.1.3.5 Recommendations (including "quick wins" and strategic recommendations)

4.1.3.6 Support or cross-reference all observed deficiencies and associated recommendations to one or more of the following standards or guidelines: ***National Institute of Standards and Technology Special Publication 800-53*** [2], or ***SANS Consensus Audit Guidelines***[3].

4.1.3.7 Appendix (including evidence and screenshots).

4.1.4 Firewall Architecture and Policy Review

4.1.4.1 Perform external automated vulnerability scanning using a vulnerability scanning solution approved by the Security Content Automation Protocol (SCAP) to identify Internet-exposed weaknesses at the network and host level. [4]

4.1.4.2 Use Expert interview, paper analysis, and direct observation to identify deficiencies in firewall policy, architecture, and administration.

4.1.4.3 Quantify the Internet attack surface and provide specific recommendations to reduce and manage risks from the Internet vector.

4.1.5 Endpoint Assessment

4.1.5.1 Perform automated host-based scanning against a sample of 15 desktop and laptop systems to identify weaknesses that facilitate remote desktop compromise.

[2] Reference provided as Exhibit C.
[3] Reference provided as Exhibit D.
[4] Reference provided as Exhibit E.

4.1.5.2 Identify ways to optimize currently deployed technologies which monitor, detect, and respond to endpoint exploit and compromise.

4.1.5.3 Provide a vendor-agnostic roadmap for closing discovered endpoint gaps and aligning CPRB with endpoint security best practices within 18 months of the assessment.

4.1.6 Data Loss Prevention Gap Analysis

4.1.6.1 Use Expert interview, paper analysis, and direct observation to audit how CPRB exchanges confidential data with external parties, and identify weaknesses.

4.1.6.2 Identify ways to optimize currently deployed technologies to monitor, detect, and respond to data loss caused by stolen or lost mobile and portable storage devices.

4.1.6.3 Provide a vendor-agnostic roadmap for closing discovered gaps and aligning CPRB with data loss prevention best practices within 18 months of the assessment.

4.1.7 Collaborate with the CPRB Guidance Team to develop and deliver executive presentations of the assessment and its results.

4.1.8 Provide documented evidence of the performance of a vulnerability assessment and/or penetration test on a government entity or corporation that has the minimum of 5,000 employees. Evidence of this should be in the form of a list of the Vendor's clients meeting this requirement with the total number of employees for each client identified with the client name. The employee count should be the total number of employees in the entire organization (federal agency, state government, county government, corporation, etc.), including all divisions, agencies, sections, etc. and may be rounded to the nearest hundred. (For example, the State of West Virginia has approximately 30,000 employees.)

4.1.9 As part of the Solicitation, provide a signed attestation and confirmation of the following on ***Attachment 3***:

4.1.9.1 Confirm that neither the vendor nor any of the vendor's employees, agents, independent contractors, or subcontractors have been convicted of, pled guilty to, pled nolo contendere or were named as an unindicted co-conspirator to any felony.

4.1.9.2 Confirm that there is no concluded or pending litigation against the vendor or vendor employees related to a contracted engagement.

4.1.9.3 Identify key staffs which would be assigned to the project and affirm that those individuals are full-time employees of the vendor.

4.1.9.4 Verify that neither the vendor nor any officer or employee have given any remuneration or anything of value directly or indirectly to CPRB or any of its Retirement Board members, officers, employees, or contracted consultants.

4.1.9.5 Verify that neither the vendor, nor any officer, principal or employee have given any remuneration or anything of value as a finder's fee, cash solicitation fee, or fee for consulting, lobbying or otherwise, in connection with this Solicitation.

4.1.9.6 Verify that within the past five years neither the vendor, nor any officer or employee of the vendor have been a defending party in a legal proceeding before a court related to the provision of the services.

4.1.9.7 Verify that within the past five years neither the vendor, nor any officer or employee been the subject of a governmental regulatory agency inquiry, investigation, or charge.

4.1.9.8 Verify that neither the vendor, any officer of the vendor, nor any owner of a twenty percent (20%) interest or greater in the vendor has filed for bankruptcy, reorganization, a debt arrangement, moratorium, or any proceeding under any bankruptcy or insolvency law, or any dissolution or liquidation proceeding.

4.1.9.9 Verify that neither the vendor, nor any officer, principal or employee who shall perform work under the contract has a possible conflict of interest (e.g. employment with the State of West Virginia).

4.1.9.10 Verify that the vendor does not have any active managed security service provider contract(s) with any State of West Virginia agency.

4.1.9.11 Provide a statement of whether there are any pending Securities Exchange Commission investigations involving the Vendor, and if

such are pending or in progress, an explanation providing relevant details and an attached opinion of counsel as to whether the pending investigation(s) will impair the Vendor's performance in a contract under this Solicitation.

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

Vendor's who wish to respond to a Centralized Request for Quotation (CRFQ) online may submit information through the State's wvOASIS Vendor Self Service (VSS). Vendors should download the Exhibit "A": Proposal Form/Pricing Page as well as any other required documents that are attached separately to the CRFQ and published to the VSS. Vendors must complete these forms with their prices information and other required information per the specifications and include it as attachments to their online response with an Attachment Type of "Pricing". The Pricing Page attachments (Pricing) are then downloaded buy the Buyer during the scheduled bid opening for bid evaluation.

If unable to respond online please submit the Exhibit "A" Proposal Form/Pricing Pages and all other required documentation with your bid prior to the scheduled bid opening date.

5.1.1 Evaluation will be based on Total Cost; Items one (1) through five (5), award will be for the Total Cost of the five (5) Assessments Items one through five.

5.1.2 Total for the Assessments Items 1 through 5 are Firm Fixed Price.

5.2 Pricing Page: Vendor should complete the Pricing Page Exhibit "A" by entering the Unit Coast for each of the 5 Assessments .Vendor should complete the Pricing Page/Pricing Section in full as failure to complete the Pricing Page/Section in full in its entirety may result in Vendor's bid being disqualified.

Vendor should type or electronically enter the information into the Pricing Page to prevent errors in the evaluation.

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 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:** Payments will be based upon the Agency acceptance at the completion of the deliverables described in the Mandatory Requirements Section 4 of this Request for Quotation. Each of the five periodic assessments will have an independent payment point 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.

10 **VENDOR DEFAULT:**

10.1 The following shall be considered a vendor default under this Contract.

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

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

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

10.1.4 Failure to remedy deficient performance upon request.

10.2 The following remedies shall be available to Agency upon default.

10.2.1 Cancellation of the Contract.

10.2.2 Cancellation of one or more release orders issued under this Contract.

10.2.3 Any other remedies available in law or equity.

11 MISCELLANEOUS:

11.1 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: Sandra Hawkins

Telephone Number: 304 356-3395

Fax Number: 304 356-3590

Email Address: sandra.k.hawkins@verizon.com

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 1 – Vendor References

Reference No. 1	
Name:	Scott Davis
Position:	VP of Information Technology
Address:	1 Credit Union Place, Harrisburg, PA
Telephone Number:	Will be provided upon written request
Project Name:	Pennsylvania State Employees Credit Union Penetration Testing & Vulnerability Assessments
Project Description:	Application assessments and penetration testing performed to identify gaps in the security profile. These assessments seek to identify vulnerabilities in systems such as web browsers, servers, static contentment and applications logic scripts. The penetration testing allows us to identify gaps internal and external to the network and applications.

Reference No. 2	
Name:	Due to privacy concerns, contact information will be provided upon written request from State of West Virginia
Position:	
Address:	
Telephone Number:	
Project Name:	Massachusetts Port Aurthority PCI-DSS Gap Analysis
Project Description:	Services performed were to review the MassPort information technology security policies. With input from the customer personnel we reviewed their then current security controls and verification through documentation to determine the level of performance as it relates to PCI Data Security Standards. We provided a gap analysis report that identifies areas of non-compliance and offer recommendations for corrective actions.

Reference No. 3	
Name:	Due to privacy concerns, contact information will be provided upon written request from State of West Virginia
Position:	
Address:	
Telephone Number:	
Project Name:	U.S. Department of Labor System Re-Authorization
Project Description:	Verizon conducted a comprehensive risk assessment and security authorization testing of the DOLNet System, a government owed general support system hosted and operated by Verizon. The assessment was conducted in accordance with NIST SP 800-37 to identify vulnerabilities and risks to the DOLNet Systems and evaluate

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 1 – Vendor References

	existing security controls in-place in order to ensure that they are correctly implemented and functioning as intended.

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 2 – Vendor Primary Staff References

Due to the dynamic nature of the information security industry, Verizon is unable to assign specific security consultants to this project until contract award. Verizon will, upon final award, schedule a kick-off meeting which will include all team members, state project manager and key state personnel. The project plan will be reviewed and accepted by all participants.

We have included on the following pages a representative sampling of actual resumes of the security consultants who will work on this project for the State.

All Verizon security personnel, permanent or otherwise, are subject to an appropriate screening process to establish their identity, bona fides and qualification for the intended role. They pass a thorough background check and drug screening before they are hired.

Reference No. 1	
Name:	See following pages
Position:	
Address:	
Telephone Number:	
Project Name:	
Project Description:	
Duties Performed:	

Reference No. 2	
Name:	See following pages
Position:	
Address:	
Telephone Number:	
Project Name:	
Project Description:	
Duties Performed:	

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 2 – Vendor Primary Staff References

Reference No. 3	
Name:	See following pages
Position:	
Address:	
Telephone Number:	
Project Name:	
Project Description:	
Duties Performed:	

Professional Profile

Mr. Verizon Consultant is currently an Executive Security Consultant in the Professional Security Services organization within Verizon Business. This organization is responsible for providing project management, integration services, and e-business solutions covering all aspects of security and privacy.

Mr. Consultant has more than 12 years of information security experience, primarily as an IT consulting professional specializing in web application, network, wireless, and source code vulnerability assessments. Further, he has multiple additional skills to help organizations with various information security scenarios. He has worked for a multitude of companies, including governments, financial institutions, utility companies, entertainment companies, and health care organizations in North America, South America, Europe, Asia, Australia, and Africa.

Mr. Consultant developed Verizon Business' Penetration Testing Methodology and Secure Application Development training classes, and he is currently a lead instructor for both. He has taught these classes to customers on a worldwide basis in North America, Central America, Europe, and Asia, and Australia.

Mr. Consultant is the inventor for US patent 7,551,073 for a "method, system and program product for alerting an information technology support organization of a security event".

Mr. Consultant has developed the first freely available, open source, centrally-managed, massively distributable, agent-based data loss prevention solution, OpenDLP, to help organizations identify sensitive data at rest on hundreds or thousands of systems simultaneously. Given Perl-compatible regular expressions and administrative authentication credentials on a Windows system or domain, a Linux-based web application distributes, installs, and starts Windows agents that run as a low priority service. These agents periodically relay findings to the Linux-based web application over a trusted SSL connection. When finished scanning, OpenDLP automatically removes itself from the Windows systems. There are also options to perform agentless scans of Windows systems, UNIX systems, and databases. He has presented this tool at several high profile security conferences, including Shmoocon in Washington DC in 2011, HackInTheBox in Amsterdam Netherlands in 2011, and Defcon in Las Vegas NV in 2011 and 2012. In addition to OpenDLP, Mr. Consultant has contributed to other security and open source projects, including Nessus and Gentoo Linux.

Mr. Consultant continues to write software for penetration testing, including a wireless network scanner for Linux-based PDAs, a web application input validation fuzzer, a web-based front-end to Rainbow Cracking, a web-based mapping software for wireless security assessments, and a statistical trending application that compares a customer's results to its industry or to its own previous tests.

Experience and Accomplishments

Mr. Consultant specializes in penetration testing services for multiple clients, including web application security assessments, wired, and wireless engagements. Mr. Consultant is highly proficient in using open source, commercial, and self-developed tools to help automate certain tasks, but he is also highly skilled in manual exploitation and in finding previously undocumented vulnerabilities in various products. When Mr. Consultant finds vulnerabilities, he provides detailed recommendations to clients to help them alleviate the issues.

Mr. Consultant's security projects have included scenarios where he has discovered ways to bypass security controls on systems to obtain sensitive customer, employee, and medical information. He has also been involved in projects that have allowed him to access a corporate network through an insecure wireless client from outside the customers' buildings. Furthermore, he has been involved in numerous web application security assessments where he was able to gain access to highly sensitive data and to companies' internal corporate networks over the Internet through web application vulnerabilities. Mr. Consultant has also been involved in reviewing source code for many closed-source applications and devices used by financial institutions and international government agencies. In all of these

scenarios, Mr. Consultant worked with the customers to resolve the identified vulnerabilities and helped them create or modify policies and procedures to mitigate future risk.

Security Tools and Platforms

Operating Systems

AIX, FreeBSD, Linux (Gentoo, Debian-based, Redhat-based), OpenBSD, Solaris, Windows NT/2000/XP/2003/Vista/7.

Vulnerability Assessment and Penetration Testing Tools

Public Domain: Aircrack-ng, AirSnort, Kismet, Nikto, nmap
Commercial: AirMagnet, Appscan, ISS, nCircle, Nessus, NeXpose, WebInspect, Burp Proxy, Ounce
Self-Developed: OpenDLP, web application scanner, wireless network scanner, various other tools

Programming Languages

ASP, C, C++, C#, HTML/JavaScript, Java, Perl, PHP, Python, SQL (MySQL, Microsoft SQL, PostgreSQL), Visual Basic

Education, Conferences, and Patents

- Graduate with a Bachelors of Science degree in Computer Science from Grand Valley State University in 2000
- Speaker at ShmooCon 2011 with a talk titled "Gone in 60 Minutes: Stealing Sensitive Data from Thousands of Systems Simultaneously with OpenDLP"
- Speaker at HackInTheBox Amsterdam 2011 with a talk titled "Gone in 60 Minutes: Stealing Sensitive Data from Thousands of Systems Simultaneously with OpenDLP"
- Speaker at Defcon 2011 with a talk titled "Gone in 60 Minutes: Stealing Sensitive Data from Thousands of Systems Simultaneously with OpenDLP"
- Speaker at Defcon 2012 with a talk titled "Post-Exploitation Nirvana: Launching OpenDLP Agents over Meterpreter Sessions"
- Inventor of US patent 7,551,073 for a "method, system and program product for alerting an information technology support organization of a security event"

verizon business
Security Solutions powered by Cybertrust

Mr. Verizon Consultant

Professional Profile

Mr. Verizon Consultant is a Senior Security Consultant in the Professional Security Services organization within Verizon Business. This organization is responsible for providing project management, integration services, and e-business solutions covering all aspects of security and privacy.

Mr. Consultant has over twenty-seven years of experience in securing telecommunications circuits using cryptography and over seventeen years of experience in securing client-server based networks and web-based business. He currently specializes in Verizon Businesses' penetration testing offerings. Mr. Consultant applies the Verizon Business security methodology with today's technologies to ensure a secure network environment.

Experience and Accomplishments

Mr. Consultant, as a senior security consultant, specializes in intrusion testing "ethical hacking" services for multiple clients, including financial institutions, medical organizations' as well as many of the Fortune 500 organizations. During the testing Mr. Consultant utilizes the tool sets of today's hacker community along with in-depth manual analysis to find more detailed vulnerabilities. Once vulnerabilities are identified Mr. Consultant provides detailed reports to alleviate the vulnerabilities to assist in keeping the client's network environment secure. Mr. Consultant identifies weaknesses at both the operating system and application layers.

Mr. Consultant assisted in the development of a Fortune 100 Ethical Hacker Certification written test.

Mr. Consultant, as the Evaluation of Shared Applications (ESA) Team Lead, provided team scheduling, coordination, and performance of vulnerability assessments for shared applications. ESA applications were applications placed in a shared network environment amongst a large customer base. The testing included examining the applications for cross-customer access, as well as authenticated and non-authenticated vulnerabilities.

As an independent consultant, Mr. Consultant designed, engineered, and installed networks of various sizes for clients ranging from law offices to a casino. In addition he developed and implemented a network security plan for a casino.

Mr. Consultant participated as a Technical Contributor for the IIS 3.0 and 4.0 exams, SMS 1.2 exam, Proxy Server 1.0 and 2.0 exams, Exchange Server 5.0 and 5.5 exams, IEAK exam and the revised Windows 95 exam.

As Network Security Officer and Computer Systems Security Officer, Mr. Consultant revamped the security of the Headquarters Second Air Force (HQ 2AF) network. High-level officials at the Pentagon recognized the security procedures at Keesler AFB as an example for the Air Force to follow. In addition he provided HQ Second Air Force input to Air Education and Training Command CIO with regard to the Air Force Virtual Private Network (VPN) Rollout Strategy and the Air Force Public Key Infrastructure Implementation Plan.

As an instructor in the Air Force he developed and taught system administration and maintenance instructional material for the Sun SPARCstation 10 Model 51, DEC MicroVAX II, and Cromemco CS-250 systems.

Security Tools and Platforms

Operating Systems

Linux, AIX, FreeBSD, OpenBSD, Solaris, Windows NT/2000/XP/2003/7, OS/2, VMS, Cromix+

Vulnerability Assessment and Penetration Testing Tools

Aircrack-ng, AirSnort, Kismet, Nessus, Nikto, nmap, AirMagnet, Appscan, ISS, WebInspect, , L0phtCrack, John the Ripper, Wireshark, netcat, CORE Impact, Metasploit, Paros, WebScarab, BurpSuite, Cain and Abel, ettercap, and many, many more tools as the assessments require.

Education and Certifications

- Bachelor of Science degree from Faulkner University in Management of Human Resources - 4.0 GPA - Selected for Who's Who among Students in American Universities and Colleges
- Associate of Applied Science degree from the Community College of the Air Force in Electronic Systems Technology
- Associate of Applied Science degree from the Community College of the Air Force in Instructor of Technology and Military Science

Professional Certificates:

- Certified Master Internet Security Specialist
- Cisco Certified Network Associate (CCNA)
- Microsoft Certified Systems Engineer (MCSE)
- IBM Certified LAN Server Engineer (CLSE)
- IBM Certified OS/2 Engineer (COS/2E)
- IBM Certified LAN Server Instructor (CLSI)
- IBM Certified OS/2 Instructor (COS/2I)
- IBM Certified LAN Server Administrator (CLSA)
- Microsoft Certified Product Specialist (MCPS)
- CompTIA A+ Certification Program

Various technical training courses while in the United States Air Force and while assigned to NATO

Mr. Consultant has written for a number of books for various publishers including Osborne/McGraw Hill, Microsoft Press, and Syngress media. The Osborne/McGraw-Hill titles about Microsoft Windows NT and Windows 2000 products were approved by Microsoft as Approved Study Guides for their certification tests. The books were used worldwide by Global Knowledge in their training classes and have been translated into six languages. Over 1,000,000 copies of the books Mr. Consultant has participated in have been sold. The publications Mr. Consultant has participated in include:

Book – Publisher – Status

- Hack Proofing your Network: Internet Tradecraft – Syngress Media – Co-author/Technical Editor
- Windows NT Security Step by Step – The SANS Institute – Contributor
- Configuring Windows 2000 Server Security – Syngress Media – Co-author/Technical Editor
- Designing Security for a Windows 2000 Network – Osborne/McGraw-Hill – Technical Editor
- Mission Critical Internet Security – Syngress Media – Technical Editor
- Configuring Cisco Network Security – Osborne/McGraw-Hill – Technical Editor
- Cisco LAN Switch Configuration – Osborne/McGraw-Hill – Co-author
- Building a Cisco Network for Windows 2000 – Syngress Media – Co-author/Technical Editor
- Windows 2000 Server System Administration Handbook – Syngress Media – Co-author
- Managing Active Directory for Windows 2000 Server – Syngress Media - Technical Editor
- Windows 2000 Deployment Strategies – Syngress Media – Technical Editor

- Windows 2000 Configuration Wizards – Syngress Media – Co-author
- Designing Windows 2000 Directory Services – Osborne/McGraw-Hill – Technical Editor
- Year 2000 Technical Reference for Windows NT Server – Syngress Media – Co-author
- Exchange Server 5.5 – Osborne/McGraw-Hill – Co-author
- Exchange Server 5.5 Administrator's Companion – Microsoft Press – Co-author
- SQL Server 7.0 Administration– Osborne/McGraw-Hill – Co-author
- SQL Server 7.0: Database Implementation Training Kit – Microsoft Press – Technical Reviewer
- Windows NT Server 4.0 in the Enterprise – Osborne/McGraw-Hill – Co-author
- TCP/IP on Windows NT 4.0 – Osborne/McGraw-Hill – Co-author
- Windows NT Server 4.0 – Osborne/McGraw-Hill – Co-author
- Windows NT Workstation 4.0 – Osborne/McGraw-Hill – Co-author
- Test Yourself MCSE Certification Practice Exams – Osborne/McGraw-Hill – Co-author
- Networking Essentials – Osborne/McGraw-Hill – Co-author
- Windows 98 – Osborne/McGraw-Hill – Co-author
- Network + Test Yourself – Osborne/McGraw-Hill – Co-author
- Network + - Osborne/McGraw-Hill – Co-author
- MCSE Windows 2000 Professional Test Yourself – Osborne/McGraw Hill – Technical Editor
- MCSE Windows 2000 Server Test Yourself – Osborne/McGraw-Hill – Technical Editor
- MCSE Designing Security for Windows 2000 Test Yourself – Osbourne/McGraw-Hill – Technical Editor
- Email Virus Handbook – Osborne/McGraw-Hill – Technical Editor

verizonbusiness
Security Solutions powered by Cybertrust

Mr. Verizon Consultant

Professional Profile

Mr. Verizon Consultant is currently a Senior Security Consultant in the Professional Security Services organization within Verizon Business. This organization is responsible for providing project management, integration services, and e-business solutions covering all aspects of security and privacy.

Mr. Consultant has more than 12 years of information security experience, primarily as an IT consulting professional specializing in web and mobile application, network, wireless, and source code vulnerability assessments. Furthermore, Mr. Consultant has significant experience in reverse engineering, crash analysis, and exploit development.

Experience and Accomplishments

Mr. Consultant has performed security assessments of nearly every type for a multitude of companies, including governments, financial institutions, utility companies, health care and retail organizations in North America, Europe, and Africa.

Mr. Consultant is currently a lead instructor for the Verizon Business' Penetration Testing Methodology and Secure Application Development training classes.

Mr. Consultant is the author of numerous papers regarding application fuzzing, binary instrumentation, crash analysis, and exploit development [1]. Furthermore, he is a member of the Corelan [2] research group which frequently releases papers, tutorials, and software in the attempt to demystify the process in which flaws are discovered and to decrease the time required when determining the exploitability of application flaws.

Mr. Consultant continues to write software for penetration testing and reverse engineering. He has recently ported the popular Freeradius-WPE patches to OpenWRT which allows Verizon Business security consultants to perform assessments against WPA Enterprise networks on a self-contained, mobile platform. He has contributed to various open source projects including the Metasploit [3] and Peach Fuzzing Frameworks [4], [5]. Mr. Consultant has also identified and publically disclosed numerous security flaws in commercial and open source applications [6], [7], [8].

Mr. Consultant is currently developing an application based on Intel's Pin, a binary instrumentation tool, in order to perform taint analysis and identify security flaws such as heap overflows and use after free conditions when analyzing application crashes. He is also currently developing an application which aims to reverse MSCHAPv2 hashes into single round DES blocks; significantly reducing the amount of time and efforts required to decrypt into plaintext.

Security Tools and Platforms

Operating Systems

AIX, FreeBSD, Linux (Redhat-based, Debian-based), Solaris, Windows NT/2000/XP/2003/2008/Vista/7/8.

Vulnerability Assessment and Penetration Testing Tools

Public Domain: Metasploit, Aircrack-ng, Kismet, nmap, SQLmap
Commercial: Appscan, nCircle, Nessus, NeXpose, WebInspect, Burp Proxy, Ounce, IDA Pro

Programming Languages

Assembly, ASP, C, C++, C#, HTML/JavaScript, Java, Perl, PHP, Python, Ruby, SQL (MySQL, Microsoft SQL, PostgreSQL), Visual Basic

Education and Certifications

- Associates Degree in Computer Security and Forensics from Pittsburgh Technical Institute (2006)
- Offensive Security OSCE
- CompTIA Security+

[1] http://www.flinkd.org/
[2] https://www.corelan.be/
[3] http://www.metasploit.com/modules/auxiliary/admin/cisco/cisco_secure_acs_bypass
[4] http://peachfuzzer.com/PublicPits.html
[5] http://www.flinkd.org/projects/peach-pits/
[6] http://www.securityfocus.com/bid/36842
[7] http://packetstormsecurity.com/files/author/6090/
[8] ***Due to security concerns, numerous vulnerabilities have been privately coordinated directly with the application vendors.*

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 3 – Attestation and Confirmations

Provide confirmation to the following statements, sign and submit this Attachment as part of the RFQ submission:

Statement	Confirmed (Yes/No)
Confirm that neither the vendor nor any of the vendor's employees, agents, independent contractors, or subcontractors have been convicted of, pled guilty to, pled nolo contendere or were named as an unindicted co-conspirator to any felony.	No
Confirm that there is no concluded or pending litigation against the vendor or vendor employees related to a contracted engagement.	No
Identify key staffs which would be assigned to the project and affirm that those individuals are full-time employees of the vendor.	Yes
Verify that neither the vendor nor any officer or employee have given any remuneration or anything of value directly or indirectly to CPRB or any of its Retirement Board members, officers, employees, or contracted consultants.	No
Verify that neither the vendor, nor any officer, principal or employee have given any remuneration or anything of value as a finder's fee, cash solicitation fee, or fee for consulting, lobbying or otherwise, in connection with this RFQ.	No
Verify that within the past five years neither the vendor, nor any officer or employee of the vendor have been a defending party in a legal proceeding before a court related to the provision of the services.	No
Verify that within the past five years neither the vendor, nor any officer or employee been the subject of a governmental regulatory agency inquiry, investigation, or charge.	No
Verify that neither the vendor, any officer of the vendor, nor any owner of a twenty percent (20%) interest or greater in the vendor has filed for bankruptcy, reorganization, a debt arrangement, moratorium, or any proceeding under any bankruptcy or insolvency law, or any dissolution or liquidation proceeding.	No
Verify that neither the vendor, nor any officer, principal or employee who shall perform work under the contract has a possible conflict of interest (e.g. employment with the State of West Virginia).	No
Verify that the vendor does not have any active managed	No

REQUEST FOR QUOTATION

Information Security and Network Vulnerability Assessment

Attachment 3 – Attestation and Confirmations

Statement	Confirmed (Yes/No)
security service provider contract(s) with any State of West Virginia agency.	
Confirm there are no pending Securities Exchange Commission investigations involving the Vendor, and if such are pending or in progress, an explanation providing relevant details and an attached opinion of counsel as to whether the pending investigation(s) will impair the Vendor's performance in a contract under this Solicitation.	No

Company: Verizon Business Network Svc Inc., on behalf of MCI Communications Svc Inc, d/b/a Verizon Business Svcs

Printed Name: Marsha K. Harrell

Signature: Marsha K. Harrell

Title:

Marsha K Harrell
Senior Consultant
Pricing/Contract Management

Date: 1/21/15

Attachment 4

Consolidated Public Retirement Board
Confidentiality and Non-disclosure Statement

Protecting confidentiality and understanding the sensitive nature of information recorded at the Consolidated Public Retirement Board (CPRB) becomes the responsibility of every person. We must strictly adhere to a policy of non-disclosure of any information relating to our clients, and every state employee or contract worker working inside of or with our office must sign and abide by this confidentiality statement.

At no time, shall any state employee or contract worker who is working inside or with the CPRB discuss or distribute personal information regarding any client of this agency. This personal information includes, but is not limited to, client or employee salaries, medical history, pension specific information, social security numbers, or any other identifying numbers, addresses, banking information, telephone numbers, or any other data or information excluded from protection by the WV Freedom of Information Act.

"I, _____ the (title) _____ of

(company)_____understand the sensitive nature and the confidentiality of the client/employee information stored at the West Virginia Consolidated Public Retirement Board. All employees of this company therefore acknowledge and agree that personal client/employee information and any other related data is to be treated as confidential information which is not a matter of public record. All employees of the above named company therefore agree not to permit distribution or engage in discussion of this information to any person. I understand that, if at any time I am approached by an outside individual, agency or media representative, I shall direct their queries to the Executive Director of the West Virginia Consolidated Public Retirement Board."

Print Name: _____

Company: _____

Signature: _____ Date:

Revised 7/05/07 Vendors

Exhibit A
Pricing Page
Information Security and Network Vulnerability Assessment service for CPRB

Item	Item Description	Description	Unit of Measure	Unit Cost	Quantity Needed	Extended Cost
1	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 1	per Complete Assesment		1	125450.00
2	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 2	per Complete Assesment		1	56950.00
3	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 3	per Complete Assesment		1	72780.00
4	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 4	per Complete Assesment		1	72780.00
5	Perform the following items as specified in the RFQ: Review Prioritize and rank the discovered vulnerabilities, Written Report, Firewall Architecture and Policy review, Endpoint Assessment, Data Loss Prevention Gap Analysis and Executive Presentation.	Assessment 5	per Complete Assesment		1	72780.00
					TOTAL of Assessments	400740.00

Assessment Cost are <u>firm fixed</u> for each complete Assessments

*** Contrat Award will be for Total of Assessments ***

Exhibit "B"

NIST Special Publication 800-37
Revision 1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Guide for Applying the Risk Management Framework to Federal Information Systems

A Security Life Cycle Approach

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Special Publication 800-37, Revision 1, 93 pages

(February 2010)

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Electronic mail: sec-cert@nist.gov

Compliance with NIST Standards and Guidelines

In accordance with the provisions of FISMA,[1] the Secretary of Commerce shall, on the basis of standards and guidelines developed by NIST, prescribe standards and guidelines pertaining to federal information systems. The Secretary shall make standards compulsory and binding to the extent determined necessary by the Secretary to improve the efficiency of operation or security of federal information systems. Standards prescribed shall include information security standards that provide minimum information security requirements and are otherwise necessary to improve the security of federal information and information systems.

- Federal Information Processing Standards (FIPS) are approved by the Secretary of Commerce and issued by NIST in accordance with FISMA. FIPS are compulsory and binding for federal agencies.[2] FISMA requires that federal agencies comply with these standards, and therefore, agencies may not waive their use.
- Special Publications (SPs) are developed and issued by NIST as recommendations and guidance documents. For other than national security programs and systems, federal agencies must follow those NIST Special Publications mandated in a Federal Information Processing Standard. FIPS 200 mandates the use of Special Publication 800-53, as amended. In addition, OMB policies (including OMB Reporting Instructions for FISMA and Agency Privacy Management) state that for other than national security programs and systems, federal agencies must follow certain specific NIST Special Publications.[3]
- Other security-related publications, including interagency reports (NISTIRs) and ITL Bulletins, provide technical and other information about NIST's activities. These publications are mandatory only when specified by OMB.
- Compliance schedules for NIST security standards and guidelines are established by OMB in policies, directives, or memoranda (e.g., annual FISMA Reporting Guidance).

[1] The E-Government Act (P.L. 107-347) recognizes the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for organizations to develop, document, and implement an organization-wide program to provide security for the information systems that support its operations and assets.

[2] The term *agency* is used in this publication in lieu of the more general term *organization* only in those circumstances where its usage is directly related to other source documents such as federal legislation or policy.

[3] While federal agencies are required to follow certain specific NIST Special Publications in accordance with OMB policy, there is flexibility in how agencies apply the guidance. Federal agencies apply the security concepts and principles articulated in the NIST Special Publications in accordance with and in the context of the agency's missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of *adequate security* for federal information systems. Given the high priority of information sharing and transparency within the federal government, agencies also consider reciprocity in developing their information security solutions. When assessing federal agency compliance with NIST Special Publications, Inspectors General, evaluators, auditors, and assessors consider the intent of the security concepts and principles articulated within the specific guidance document and how the agency applied the guidance in the context of its mission/business responsibilities, operational environment, and unique organizational conditions.

Acknowledgements

This publication was developed by the *Joint Task Force Transformation Initiative* Interagency Working Group with representatives from the Civil, Defense, and Intelligence Communities in an ongoing effort to produce a unified information security framework for the federal government. The Project Leader, Ron Ross, from the National Institute of Standards and Technology, wishes to acknowledge and thank the senior leadership team from the U.S. Departments of Commerce and Defense, the Office of the Director of National Intelligence, the Committee on National Security Systems, and the members of the interagency working group whose dedicated efforts contributed significantly to the publication. The senior leadership team, working group members, and their organizational affiliations include:

U.S. Department of Defense

Cheryl J. Roby
Acting Assistant Secretary of Defense for Networks and Information Integration/ DoD Chief Information Officer

Gus Guissanie
Acting Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance

Dominic Cussatt
Senior Policy Advisor

Office of the Director of National Intelligence

Honorable Priscilla Guthrie
Intelligence Community Chief Information Officer

Sherrill Nicely
Deputy Intelligence Community Chief Information Officer

Mark J. Morrison
Deputy Associate Director of National Intelligence for IC Information Assurance

Roger Caslow
Lead, C&A Transformation

National Institute of Standards and Technology

Cita M. Furlani
Director, Information Technology Laboratory

William C. Barker
Chief, Computer Security Division

Ron Ross
FISMA Implementation Project Leader

Committee on National Security Systems

Cheryl J. Roby
Acting Chair, Committee on National Security Systems

Eustace D. King
CNSS Subcommittee Co-Chair (DoD)

William Hunteman
CNSS Subcommittee Co-Chair (DoE)

Joint Task Force Transformation Initiative Interagency Working Group

Ron Ross *NIST, JTF Leader*	Gary Stoneburner *Johns Hopkins APL*	Dominic Cussatt *Department of Defense*	Kelley Dempsey *NIST*
Marianne Swanson *NIST*	Jennifer Fabius Greene *MITRE Corporation*	Dorian Pappas *National Security Agency*	Arnold Johnson *NIST*
Stuart Katzke *Booz Allen Hamilton*	Peter Williams *Booz Allen Hamilton*	Peter Gouldmann *Department of State*	Christian Enloe *NIST*

In addition to the above acknowledgments, a special note of thanks goes to Peggy Himes and Elizabeth Lennon for their superb technical editing and administrative support. The authors also wish to recognize Beckie Bolton, Marshall Abrams, John Gilligan, Richard Graubart, Esten Porter, Karen Quigg, George Rogers, John Streufert, and Glenda Turner for their exceptional contributions in helping to improve the content of the publication. And finally, the authors gratefully acknowledge and appreciate the significant contributions from individuals and organizations in the public and private sectors, nationally and internationally, whose thoughtful and constructive comments improved the overall quality and usefulness of this publication.

DEVELOPING COMMON INFORMATION SECURITY FOUNDATIONS

COLLABORATION AMONG PUBLIC AND PRIVATE SECTOR ENTITIES

In developing standards and guidelines required by FISMA, NIST consults with other federal agencies and offices as well as the private sector to improve information security, avoid unnecessary and costly duplication of effort, and ensure that NIST publications are complementary with the standards and guidelines employed for the protection of national security systems. In addition to its comprehensive public review and vetting process, NIST is collaborating with the Office of the Director of National Intelligence (ODNI), the Department of Defense (DOD), and the Committee on National Security Systems (CNSS) to establish a common foundation for information security across the federal government. A common foundation for information security will provide the Intelligence, Defense, and Civil sectors of the federal government and their contractors, more uniform and consistent ways to manage the risk to organizational operations and assets, individuals, other organizations, and the Nation that results from the operation and use of information systems. A common foundation for information security will also provide a strong basis for reciprocal acceptance of security authorization decisions and facilitate information sharing. NIST is also working with public and private sector entities to establish specific mappings and relationships between the security standards and guidelines developed by NIST and the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27001, Information Security Management System (ISMS).

Table of Contents

Prologue

"...Through the process of risk management, leaders must consider risk to U.S. interests from adversaries using cyberspace to their advantage and from our own efforts to employ the global nature of cyberspace to achieve objectives in military, intelligence, and business operations..."

"...For operational plans development, the combination of threats, vulnerabilities, and impacts must be evaluated in order to identify important trends and decide where effort should be applied to eliminate or reduce threat capabilities; eliminate or reduce vulnerabilities; and assess, coordinate, and deconflict all cyberspace operations..."

"...Leaders at all levels are accountable for ensuring readiness and security to the same degree as in any other domain..."

-- THE NATIONAL STRATEGY FOR CYBERSPACE OPERATIONS
OFFICE OF THE CHAIRMAN, JOINT CHIEFS OF STAFF, U.S. DEPARTMENT OF DEFENSE

CHAPTER ONE

INTRODUCTION

THE NEED FOR INFORMATION SECURITY AND MANAGING RISK

Organizations[4] depend on information technology and the information systems[5] that are developed from that technology to successfully carry out their missions and business functions. Information systems can include as constituent components, a range of diverse computing platforms from high-end supercomputers to personal digital assistants and cellular telephones. Information systems can also include very specialized systems and devices (e.g., telecommunications systems, industrial/process control systems, testing and calibration devices, weapons systems, command and control systems, and environmental control systems). Federal information and information systems[6] are subject to serious threats that can have adverse impacts on organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation[7] by compromising the confidentiality, integrity, or availability of information being processed, stored, or transmitted by those systems. Threats to information and information systems include environmental disruptions, human or machine errors, and purposeful attacks. Cyber attacks on information systems today are often aggressive, disciplined, well-organized, well-funded, and in a growing number of documented cases, very sophisticated. Successful attacks on public and private sector information systems can result in serious or grave damage to the national and economic security interests of the United States. Given the significant and growing danger of these threats, it is imperative that leaders at all levels of an organization understand their responsibilities for achieving adequate information security and for managing information system-related security risks.[8]

1.1 BACKGROUND

NIST in partnership with the Department of Defense (DoD), the Office of the Director of National Intelligence (ODNI), and the Committee on National Security Systems (CNSS), has developed a common information security framework for the federal government and its contractors. The intent of this common framework is to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies. This publication, developed by the Joint Task Force Transformation Initiative Working Group, transforms the traditional Certification and Accreditation (C&A) process into the six-step Risk Management Framework (RMF). The revised process emphasizes: (i) building information security capabilities into federal information systems through the application of state-of-the-practice management, operational, and technical security controls; (ii) maintaining awareness of the

[4] The term *organization* is used in this publication to describe an entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).

[5] An *information system* is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[6] A *federal information system* is an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.

[7] Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.

[8] Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

security state of information systems on an ongoing basis though enhanced monitoring processes; and (iii) providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems.

The RMF has the following characteristics:

- Promotes the concept of near real-time risk management and ongoing information system authorization through the implementation of robust continuous monitoring processes;
- Encourages the use of automation to provide senior leaders the necessary information to make cost-effective, risk-based decisions with regard to the organizational information systems supporting their core missions and business functions;
- Integrates information security into the enterprise architecture and system development life cycle;
- Provides emphasis on the selection, implementation, assessment, and monitoring of security controls, and the authorization of information systems;
- Links risk management processes at the information system level to risk management processes at the organization level through a risk executive (function); and
- Establishes responsibility and accountability for security controls deployed within organizational information systems and inherited by those systems (i.e., common controls).

The risk management process described in this publication changes the traditional focus of C&A as a static, procedural activity to a more dynamic approach that provides the capability to more effectively manage information system-related security risks in highly diverse environments of complex and sophisticated cyber threats, ever-increasing system vulnerabilities, and rapidly changing missions.

1.2 PURPOSE AND APPLICABILITY

The purpose of this publication is to provide guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization,[9] security control selection and implementation, security control assessment, information system authorization,[10] and security control monitoring. The guidelines have been developed:

- To ensure that managing information system-related security risks is consistent with the organization's mission/business objectives and overall risk strategy established by the senior leadership through the risk executive (function);
- To ensure that information security requirements, including necessary security controls, are integrated into the organization's enterprise architecture and system development life cycle processes;

[9] FIPS 199 provides security categorization guidance for nonnational security systems. CNSS Instruction 1253 provides similar guidance for national security systems.

[10] Security *authorization* is the official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.

- To support consistent, well-informed, and ongoing security authorization decisions (through continuous monitoring), transparency of security and risk management-related information, and reciprocity;[11] and
- To achieve more secure information and information systems within the federal government through the implementation of appropriate risk mitigation strategies.

This publication satisfies the requirements of the Federal Information Security Management Act (FISMA) and meets or exceeds the information security requirements established for executive agencies[12] by the Office of Management and Budget (OMB) in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*. The guidelines in this publication are applicable to all federal information systems other than those systems designated as national security systems as defined in 44 U.S.C., Section 3542. The guidelines have been broadly developed from a technical perspective to complement similar guidelines for national security systems and may be used for such systems with the approval of appropriate federal officials exercising policy authority over such systems. State, local, and tribal governments, as well as private sector organizations are encouraged to consider using these guidelines, as appropriate.[13]

1.3 TARGET AUDIENCE

This publication serves individuals associated with the design, development, implementation, operation, maintenance, and disposition of federal information systems including:

- Individuals with mission/business ownership responsibilities or fiduciary responsibilities (e.g., heads of federal agencies, chief executive officers, chief financial officers);
- Individuals with information system development and integration responsibilities (e.g., program managers, information technology product developers, information system developers, information systems integrators, enterprise architects, information security architects);
- Individuals with information system and/or security management/oversight responsibilities (e.g., senior leaders, risk executives, authorizing officials, chief information officers, senior information security officers[14]);

---

[11] *Reciprocity* is the mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information. Reciprocity is best achieved by promoting the concept of transparency (i.e., making sufficient evidence regarding the security state of an information system available, so that an authorizing official from another organization can use that evidence to make credible, risk-based decisions regarding the operation and use of that system or the information it processes, stores, or transmits).

[12] An *executive agency* is: (i) an executive department specified in 5 U.S.C., Section 101; (ii) a military department specified in 5 U.S.C., Section 102; (iii) an independent establishment as defined in 5 U.S.C., Section 104(1); and (iv) a wholly owned government corporation fully subject to the provisions of 31 U.S.C., Chapter 91. In this publication, the term executive agency is synonymous with the term *federal agency*.

[13] In accordance with the provisions of FISMA and OMB policy, whenever the interconnection of federal information systems to information systems operated by state/local/tribal governments, contractors, or grantees involves the processing, storage, or transmission of federal information, the information security standards and guidelines described in this publication apply. Specific information security requirements and the terms and conditions of the system interconnections, are expressed in the Memorandums of Understanding and Interconnection Security Agreements established by participating organizations.

[14] At the *agency* level, this position is known as the Senior Agency Information Security Officer. Organizations also refer to this position as the *Chief Information Security Officer*.

- Individuals with information system and security control assessment and monitoring responsibilities (e.g., system evaluators, assessors/assessment teams, independent verification and validation assessors, auditors, or information system owners); and
- Individuals with information security implementation and operational responsibilities (e.g., information system owners, common control providers, information owners/stewards, mission/business owners, information security architects, information system security engineers/officers).

1.4 ORGANIZATION OF THIS SPECIAL PUBLICATION

The remainder of this special publication is organized as follows:

- **Chapter Two** describes the fundamental concepts associated with managing information system-related security risks including: (i) an organization-wide view of risk management and the application of the Risk Management Framework; (ii) the integration of information security requirements into the system development life cycle; (iii) the establishment of information system boundaries; and (iv) the allocation of security controls to organizational information systems as system-specific, hybrid, or common controls.
- **Chapter Three** describes the tasks required to apply the Risk Management Framework to information systems including: (i) the categorization of information and information systems; (ii) the selection of security controls; (iii) the implementation of security controls; (iv) the assessment of security control effectiveness; (v) the authorization of the information system; and (vi) the ongoing monitoring of security controls and the security state of the information system.
- **Supporting appendices** provide additional information regarding the application of the Risk Management Framework to information systems including: (i) references; (ii) glossary; (iii) acronyms; (iv) roles and responsibilities; (v) summary of Risk Management Framework tasks; (vi) security authorization of information systems; (vii) monitoring the security state of information systems; (viii) operational scenarios; and (ix) security controls in external environments.

CHAPTER TWO

THE FUNDAMENTALS

MANAGING INFORMATION SYSTEM-RELATED SECURITY RISKS

This chapter describes the basic concepts associated with managing information system-related security risks. These concepts include: (i) incorporating risk management principles and best practices into organization-wide strategic planning considerations, core missions and business processes, and supporting organizational information systems; (ii) integrating information security requirements into system development life cycle processes; (iii) establishing practical and meaningful boundaries for organizational information systems; and (iv) allocating security controls to organizational information systems as system-specific, hybrid, or common controls.

2.1 INTEGRATED ORGANIZATION-WIDE RISK MANAGEMENT

Managing information system-related security risks is a complex, multifaceted undertaking that requires the involvement of the entire organization—from senior leaders providing the strategic vision and top-level goals and objectives for the organization, to mid-level leaders planning and managing projects, to individuals on the front lines developing, implementing, and operating the systems supporting the organization's core missions and business processes. Risk management can be viewed as a holistic activity that is fully integrated into every aspect of the organization. Figure 2-1 illustrates a three-tiered approach to risk management that addresses risk-related concerns at: (i) the *organization* level; (ii) the *mission and business process* level; and (iii) the *information system* level.[15]

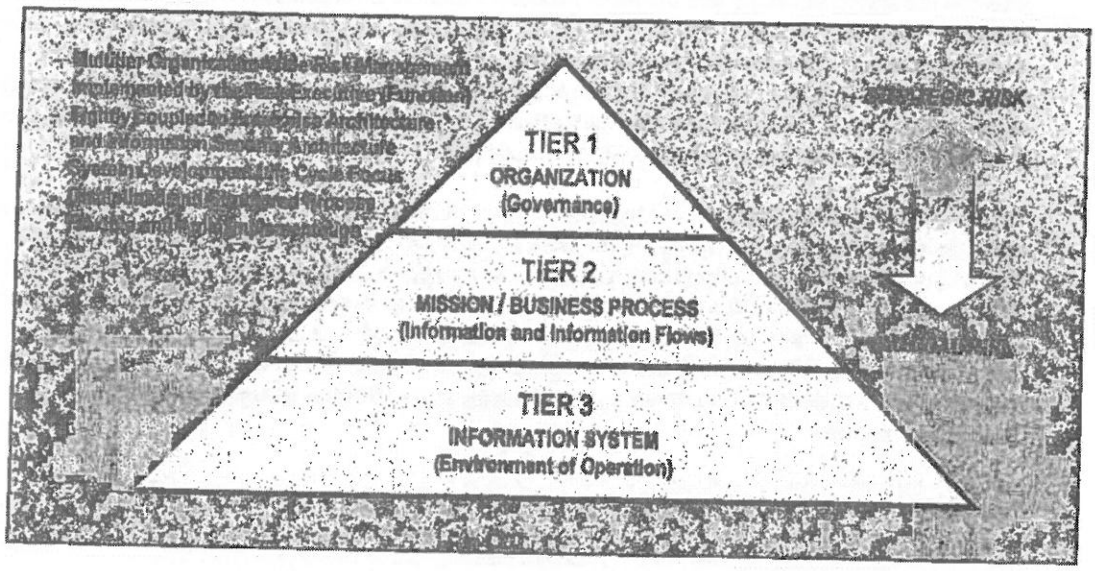


FIGURE 2-1: TIERED RISK MANAGEMENT APPROACH

[15] NIST Special Publication 800-39, *Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View* (projected for publication in 2010), will provide guidance on the holistic approach to risk management.

Tier 1 addresses risk from an organizational perspective with the development of a comprehensive governance structure and organization-wide risk management strategy that includes: (i) the techniques and methodologies the organization plans to employ to assess information system-related security risks and other types of risk of concern to the organization;[16] (ii) the methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment; (iii) the types and extent of risk mitigation measures the organization plans to employ to address identified risks; (iv) the level of risk the organization plans to accept (i.e., risk tolerance); (v) how the organization plans to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation; and (vi) the degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out. As part of the overall governance structure established by the organization, the risk management strategy is propagated to organizational officials and contractors with programmatic, planning, developmental, acquisition, operational, and oversight responsibilities, including for example: (i) authorizing officials; (ii) chief information officers; (iii) senior information security officers; (iv) enterprise/information security architects; (v) information system owners/program managers; (vi) information owners/stewards; (vii) information system security officers; (viii) information system security engineers; (ix) information system developers and integrators; (x) system administrators; (xi) contracting officers; and (xii) users.

Tier 2 addresses risk from a *mission* and *business process* perspective and is guided by the risk decisions at **Tier 1**. **Tier 2** activities are closely associated with enterprise architecture[17] and include: (i) defining the core missions and business processes for the organization (including any derivative or related missions and business processes carried out by subordinate organizations); (ii) prioritizing missions and business processes with respect to the goals and objectives of the organization; (iii) defining the types of information that the organization needs to successfully execute the stated missions and business processes and the information flows both internal and external to the organization; (iv) developing an organization-wide information protection strategy and incorporating high-level information security requirements[18] into the core missions and business processes; and (v) specifying the degree of autonomy for subordinate organizations (i.e., organizations within the parent organization) that the parent organization permits for assessing, evaluating, mitigating, accepting, and monitoring risk.

Because subordinate organizations responsible for carrying out derivative or related missions and business processes may have already invested in their own methods of assessing, evaluating, mitigating, accepting and monitoring risk, parent organizations may allow a greater degree of autonomy within parts of the organization or across the entire organization in order to minimize costs. When a diversity of risk assessment methods is allowed, organizations may choose to employ when feasible, some means of translation and/or synthesis of the risk-related information to ensure that the output of the different risk assessment activities can be correlated in a meaningful manner.

---

[16] Types of *risk* include, for example: (i) program/acquisition risk (cost, schedule, performance); (ii) compliance and regulatory risk; (iii) financial risk; (iv) legal risk; (v) operational (mission/business) risk; (vi) political risk; (vii) project risk; (viii) reputational risk; (ix) safety risk; (x) strategic planning risk; and (xi) supply chain risk.

[17] Federal Enterprise Architecture Reference Models and Segment and Solution Architectures are defined in the OMB Federal Enterprise Architecture (FEA) Program, *FEA Consolidated Reference Model Document*, Version 2.3, October 2003 and OMB *Federal Segment Architecture Methodology (FSAM)*, January 2009, respectively.

[18] Information security requirements can be obtained from a variety of sources (e.g., legislation, policies, directives, regulations, standards, and organizational mission/business/operational requirements). Organization-level security requirements are documented in the information security program plan or equivalent document.

Tier 3 addresses risk from an *information system* perspective and is guided by the risk decisions at Tiers 1 and 2. Risk decisions at Tiers 1 and 2 impact the ultimate selection and deployment of needed safeguards and countermeasures (i.e., security controls) at the information system level. Information security requirements are satisfied by the selection of appropriate management, operational, and technical security controls from NIST Special Publication 800-53.[19] The security controls are subsequently allocated to the various components of the information system as system-specific, hybrid, or common controls in accordance with the information security architecture developed by the organization.[20] Security controls are typically *traceable* to the security requirements established by the organization to ensure that the requirements are fully addressed during design, development, and implementation of the information system. Security controls can be provided by the organization or by an external provider. Relationships with external providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain arrangements.[21]

Risk management tasks begin early in the system development life cycle and are important in shaping the security capabilities of the information system. If these tasks are not adequately performed during the initiation, development, and acquisition phases of the system development life cycle, the tasks will, by necessity, be undertaken later in the life cycle and be more costly to implement. In either situation, all tasks are completed prior to placing the information system into operation or continuing its operation to ensure that: (i) information system-related security risks are being adequately addressed on an ongoing basis; and (ii) the authorizing official explicitly understands and accepts the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of a defined set of security controls and the current security state of the information system.

The Risk Management Framework (RMF), illustrated in Figure 2-2, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. The RMF operates primarily at Tier 3 in the risk management hierarchy but can also have interactions at Tiers 1 and 2 (e.g., providing feedback from ongoing authorization decisions to the risk executive [function], dissemination of updated threat and risk information to authorizing officials and information system owners). The RMF steps include:

- *Categorize* the information system and the information processed, stored, and transmitted by that system based on an impact analysis.[22]
- *Select* an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.[23]

---

[19] The RMF categorization step, including consideration of legislation, policies, directives, regulations, standards, and organizational mission/business/operational requirements, facilitates the identification of security requirements.

[20] The allocation of security controls can take place at all three tiers in the risk management hierarchy. For example, security controls that are identified as common controls may be allocated at the organization, mission/business process, or information system level. See Section 2.4 for additional information on security control allocation.

[21] Appendix I provides additional guidance regarding external service providers and the provision of security controls in external environments.

[22] FIPS 199 provides security categorization guidance for nonnational security systems. CNSS Instruction 1253 provides similar guidance for national security systems.

[23] NIST Special Publication 800-53 provides security control selection guidance for nonnational security systems. CNSS Instruction 1253 provides similar guidance for national security systems.

- ***Implement*** the security controls and describe how the controls are employed within the information system and its environment of operation.
- ***Assess*** the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- ***Authorize*** information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable.
- ***Monitor*** the security controls in the information system on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials.

Chapter Three provides a detailed description of each of the specific tasks necessary to carry out the six steps in the RMF.

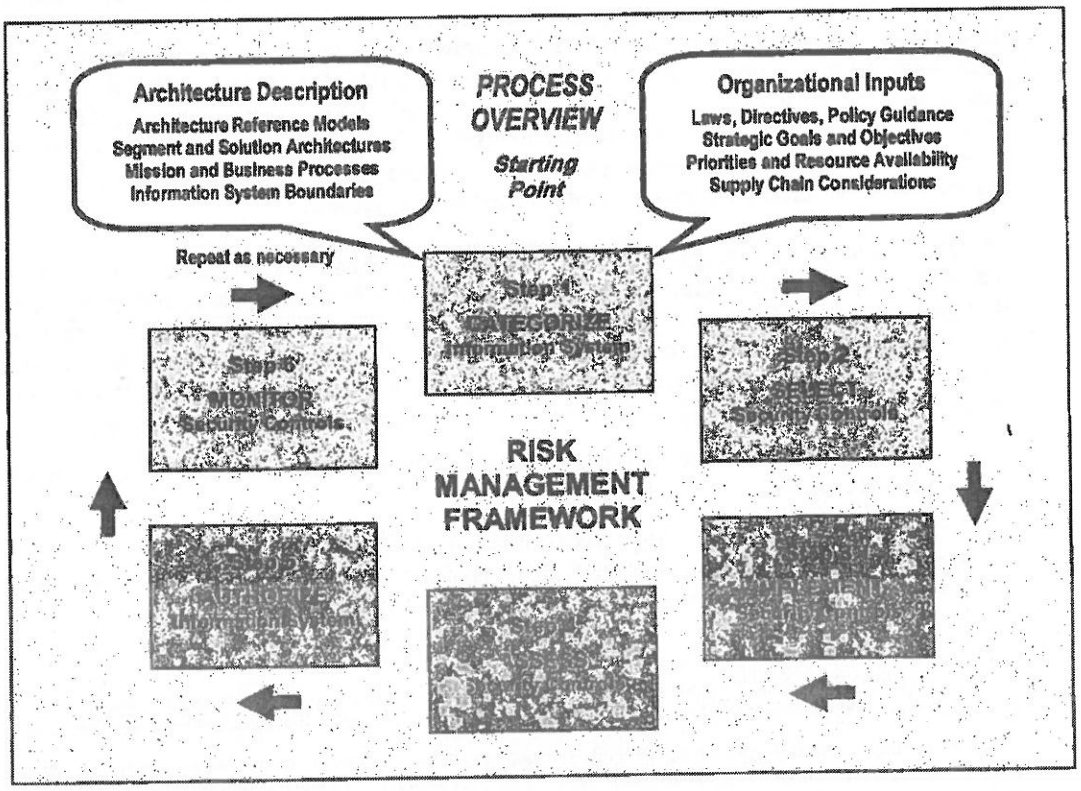


FIGURE 2-2: RISK MANAGEMENT FRAMEWORK

In summary, there is a significant degree of flexibility in how organizations employ the risk management processes described above. While it is convenient to portray the risk management approach in Figure 2-1 as hierarchical, the reality of project and organization dynamics can be much more complex. The organizational management style may be at one or more points on the

continuum from top-down command to consensus among peers. For risk management to succeed at all levels of the organization, the organization must have a consistent and effective approach to risk management that is applied to all risk management processes and procedures. Organizational officials identify the resources necessary to complete the risk management tasks described in this publication and ensure that those resources are made available to appropriate personnel. Resource allocation includes both funding to carry out the risk management tasks and assigning qualified personnel needed to accomplish the tasks.[24]

2.2 SYSTEM DEVELOPMENT LIFE CYCLE

All federal information systems, including operational systems, systems under development, and systems undergoing modification or upgrade, are in some phase of a system development life cycle.[25] Requirements definition is a critical part of any system development process and begins very early in the life cycle, typically in the *initiation* phase.[26] Security requirements are a subset of the overall functional and nonfunctional (e.g., quality, assurance) requirements levied on an information system and are incorporated into the system development life cycle simultaneously with the functional and nonfunctional requirements. Without the early integration of security requirements, significant expense may be incurred by the organization later in the life cycle to address security considerations that could have been included in the initial design. When security requirements are considered as an integral subset of other information system requirements, the resulting system has fewer weaknesses and deficiencies, and therefore, fewer vulnerabilities that can be exploited in the future.

Early integration of information security requirements into the system development life cycle is the most cost-effective and efficient method for an organization to ensure that its protection strategy is implemented. It also ensures that information security processes are not isolated from the other routine management processes employed by the organization to develop, implement, operate, and maintain information systems supporting ongoing missions and business functions. In addition to incorporating information security requirements into the system development life cycle, security requirements are also integrated into the program, planning, and budgeting activities within the organization to ensure that resources are available when needed and program/project milestones are completed. The enterprise architecture provides a central record of this integration within an organization.

Ensuring that information security requirements are integrated into the organization's system development life cycle processes regardless of the type of life cycle processes employed, helps facilitate development and implementation of more resilient information systems to reduce risk to organizational operations and assets, individuals, other organizations, and the Nation. This can be accomplished using the well-established concept of *integrated project teams*.[27] A responsible organizational official (e.g., agency head, mission or business owner, integrated project team leader, program manager, information system owner, authorizing official) ensures that security professionals are an integral part of any information system development activities from the

[24] Resource requirements include funding for training organizational personnel to ensure that they can effectively carry out their assigned responsibilities.

[25] There are typically five phases in a generic system development life cycle including: (i) *initiation*; (ii) *development/acquisition*; (iii) *implementation*; (iv) *operation/maintenance*; and (v) *disposal*.

[26] Organizations may employ a variety of system development life cycle processes including, for example, waterfall, spiral, or agile development.

[27] Integrated project teams are multidisciplinary entities consisting of a number of individuals with a range of skills and roles to help facilitate the development of information systems that meet the requirements of the organization.

initial definition of information security requirements at Tier 1 and Tier 2 to the selection of security controls at Tier 3. Such consideration is used to foster close cooperation among personnel responsible for the design, development, implementation, operation, maintenance, and disposition of information systems and the information security professionals advising the senior leadership on appropriate security controls needed to adequately mitigate risk and protect critical missions and business functions.

Finally, organizations maximize the use of security-relevant information (e.g., assessment results, information system documentation, and other artifacts) generated during the system development life cycle to satisfy requirements for similar information needed for information security-related purposes. Similar security-relevant information concerning common controls, including security controls provided by external providers, is factored into the organization's risk management process. The judicious reuse of security-relevant information by organizations is an effective method to help eliminate duplication of effort, reduce documentation, promote reciprocity, and avoid unnecessary costs that may result when security activities are conducted independently of system development life cycle processes. In addition, reuse promotes greater consistency of information used in the design, development, implementation, operation, maintenance, and disposition of an information system including security-related considerations.

2.3 INFORMATION SYSTEM BOUNDARIES

One of the most challenging problems for information system owners, authorizing officials, chief information officers, senior information security officers, and information security architects is identifying appropriate boundaries for organizational information systems.[28] Well-defined boundaries establish the scope of protection for organizational information systems (i.e., what the organization agrees to protect under its direct management control or within the scope of its responsibilities) and include the people, processes, and information technologies that are part of the systems supporting the organization's missions and business processes. Information system boundaries are established in coordination with the security categorization process and before the development of security plans. Information system boundaries that are too expansive (i.e., too many system components and/or unnecessary architectural complexity) make the risk management process extremely unwieldy and complex. Boundaries that are too limited increase the number of information systems that must be separately managed and as a consequence, unnecessarily inflate the total information security costs for the organization. The following sections provide general guidelines to assist organizations in establishing appropriate system boundaries to achieve cost-effective solutions for managing information security-related risks from the operation and use of information systems.

2.3.1 Establishing Information System Boundaries

The set of information resources[29] allocated to an information system defines the boundary for that system. Organizations have significant flexibility in determining what constitutes an information system and its associated boundary. If a set of information resources is identified as an information system, the resources are generally under the same direct management control.[30]

---

[28] With regard to the risk management process and information security, the term *information system boundary* is synonymous with *authorization boundary*.

[29] Information resources consist of information and related resources including personnel, equipment, funds, and information technology.

[30] For information systems, direct management control involves budgetary, programmatic, or operational authority and associated *responsibility* and *accountability*.

Direct management control does not necessarily imply that there is no intervening management. It is also possible for multiple information systems to be considered as independent *subsystems*[31] of a more complex information system. This situation may arise in many organizations when smaller information systems are coalesced for purposes of risk management into a larger, more comprehensive system. On a larger scale, an organization may develop a *system of systems* involving multiple independent information systems (possibly distributed across a widespread geographic area) supporting a set of common missions and/or business functions.[32]

In addition to consideration of direct management control, it may also be helpful for organizations to determine if the information resources being identified as an information system:

- Support the same mission/business objectives or functions and essentially the same operating characteristics and information security requirements; and
- Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments).[33]

Since commonality can change over time, this determination is revisited periodically as part of a continuous monitoring process carried out by the organization (see Section 3.6). While the above considerations may be useful to organizations in determining information system boundaries for purposes of risk management, they are not viewed as limiting the organization's flexibility in establishing commonsense boundaries that promote effective information security within the available resources of the organization. Information system owners consult with authorizing officials, chief information officers, senior information security officers, information security architects, and the risk executive (function)[34] when establishing or changing system boundaries. The process of establishing information system boundaries and the associated risk management implications is an organization-wide activity that includes careful negotiation among all key participants—taking into account mission and business requirements, technical considerations with respect to information security, and programmatic costs to the organization.

Software *applications* (e.g., database applications, Web applications) hosted by an information system are included in the risk management process since application security is critical to the overall security of the system.[35] Software *applications* depend on the resources provided by the hosting information system and as such, can take advantage of (i.e., leverage) the security controls provided by the system to help provide a foundational level of protection for the hosted applications, when this type of inheritance is applicable. Additional application-level security controls are provided by the respective software applications, as needed. Organizations ensure that all security controls, including application-level controls employed in separate software applications, are managed and tracked on an ongoing basis. Application owners coordinate with information system owners to ensure that information security and risk management activities are carried out as seamlessly as possible among applications and hosting systems. This coordination includes, for example, consideration for: (i) the selection, implementation, assessment, and monitoring of security controls for hosted applications; (ii) the effects of changes to hosted

[31] A *subsystem* is a major subdivision of an information system consisting of information, information technology, and personnel that perform one or more specific functions.

[32] The National Airspace System (NAS) operated by the Federal Aviation Administration (FAA) is an example of a system of systems.

[33] Similarity of operating environments includes, for example, consideration of threat, policy, and management.

[34] The roles and responsibilities of the risk executive (function) are described in Appendix D.

[35] Software applications and information systems hosting the applications may be owned by different organizations.

applications on the overall security state of the information system and the missions and business processes supported by that system; and (iii) the effects of changes to the information system on hosted applications. Employing strong configuration management and control processes within software applications and the hosting information system, and reusing security control assessment results helps to provide the necessary protection for applications.

Security controls provided by the hosted software application are documented in the security plan for the hosting information system and assessed for effectiveness during the risk management process (i.e., during the initial authorization of the information system and subsequently, during the continuous monitoring process). Application-level security controls are also assessed for effectiveness if the applications are added after the hosting information system is authorized to operate. Information system owners take appropriate measures to ensure that hosted applications do not affect the security state of the hosting system and obtain the necessary information from application owners to conduct security impact analyses, when needed.

2.3.2 Boundaries for Complex Information Systems

The application of security controls within a complex information system can present significant challenges to an organization. From a centralized development, implementation, and operations perspective, the information system owner, in collaboration with the authorizing official, senior information security officer, information security architect, and information system security engineer, examines the purpose of the information system and considers the feasibility of decomposing the complex system into more manageable *subsystems*. From a distributed development, implementation, and operations perspective, the organization recognizes that multiple entities, possibly operating under different policies, may be contributing to the development, implementation, and/or operations of the subsystems that compose the complex information system. In such a scenario, the organization is responsible for ensuring that these separate subsystems can work together in both a secure and functional manner. Treating an information system as multiple subsystems, each with its own subsystem boundary, facilitates a more targeted application of security controls to achieve adequate security and a more cost-effective risk management process. Knowledge of the security properties of individual subsystems does not necessarily provide the complete knowledge of the security properties of the complex information system. The organization applies best practices in systems and security engineering and documents the decomposition of the information system in the security plan.

Information security architecture plays a key part in the security control selection and allocation process for a complex information system. This includes monitoring and controlling communications at key internal boundaries among subsystems and providing system-wide *common controls* (see Section 2.4) that meet or exceed the requirements of the constituent subsystems inheriting those system-wide common controls. One approach to security control selection and allocation is to categorize each identified subsystem (including dynamic subsystems as described in Section 2.3.3). Separately categorizing each subsystem does not change the overall categorization of the information system. Rather, it allows the subsystems to receive a separate and more targeted allocation of security controls from NIST Special Publication 800-53 instead of deploying higher-impact controls across every subsystem. Another approach is to bundle smaller subsystems into larger subsystems within the overall complex information system, categorize each of the aggregated subsystems, and allocate security controls to the subsystems, as needed. While subsystems within complex information systems may exist as complete systems, the subsystems are, in most cases, not treated as independent entities because they are typically interdependent and interconnected.

When the results of security categorizations for the identified subsystems are different, the organization carefully examines the interfaces, information flows, and security-relevant dependencies[36] among subsystems and selects security controls for the interconnection of the subsystems to eliminate or reduce potential vulnerabilities in this area. This helps to ensure that the information system is adequately protected.[37] Security controls for the interconnection of subsystems are also employed when the subsystems implement different security policies or are administered by different authorities. The extent to which the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the complex information system, can be determined by combining security control assessments at the subsystem level and adding system-level considerations addressing interface issues among subsystems. This approach facilitates a more targeted and cost-effective risk management process by scaling the level of effort of the assessment in accordance with the subsystem security categorization and allowing for reuse of assessment results at the information system level. Figure 2-3 illustrates the concept of decomposition for a complex information system.

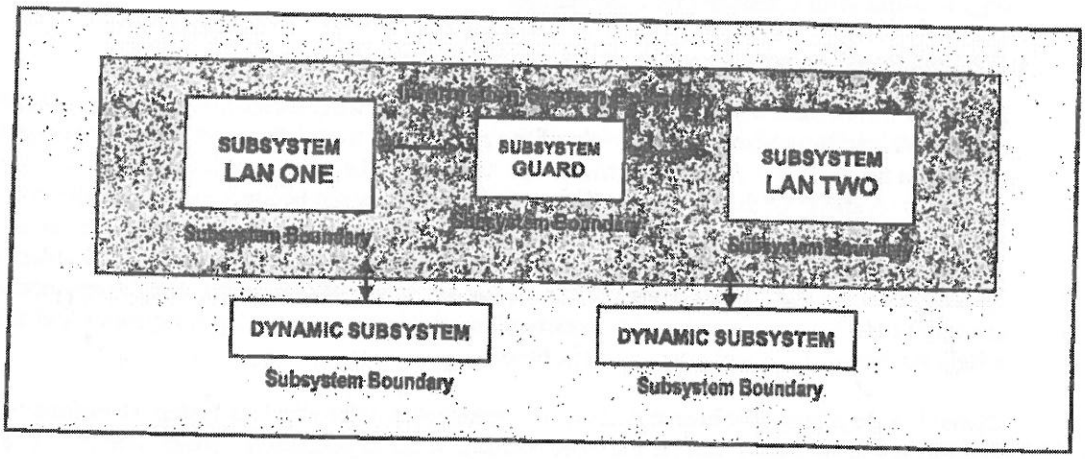


FIGURE 2-3: DECOMPOSITION OF COMPLEX INFORMATION SYSTEM

In the above example, an information system contains a system guard that monitors the flow of information between two local area networks. The information system can be partitioned into multiple subsystems: (i) local area network one; (ii) local area network two; (iii) the system guard separating the two networks; and (iv) several dynamic subsystems that become part of the system at various points in time (see Section 2.3.3). Each subsystem within the information system may

[36] Subsystem interfaces include ports and protocols. Information flows address information transmitted between subsystems. Security-relevant dependencies refer to security functions/services (e.g., encryption, auditing), performed by one subsystem that are required by one or more of the other subsystems.

[37] The types of interfaces and couplings among subsystems may introduce inadvertent weaknesses and vulnerabilities in a complex information system. For example, if a large organizational intranet is decomposed by enterprise services into smaller subsystems (e.g., severable subsystems such as local area network segments) and subsequently categorized individually, the specific protections at the subsystem level may allow a vector of attack against the intranet by erroneously selecting and implementing security controls that are not sufficiently strong with respect to the rest of the system. To avoid this situation, organizations carefully examine the interfaces among subsystems and take appropriate actions to eliminate potential vulnerabilities in this area, thus helping to ensure that the information system is adequately protected.

be categorized individually. The security categorization of the information system as a whole is not changed by taking into consideration all of the individual subsystem categorizations. When all subsystems within the complex information system have completed an initial security control assessment, the organization takes additional measures to ensure that: (i) security controls not included in the subsystem assessments are assessed for effectiveness; and (ii) the subsystems work together in a manner that meets the security requirements of the information system.[38]

2.3.3 Changing Technologies and the Effect on Information System Boundaries

Changes to current information technologies and computing paradigms add complications to the traditional tasks of establishing information system boundaries and protecting the missions and business processes supported by organizational information systems. In particular, net-centric architectures[39] (e.g., service-oriented architectures [SOAs], cloud computing) introduce two important concepts: (i) *dynamic subsystems*; and (ii) *external subsystems*. While the concepts of dynamic subsystems and external subsystems (described in the following sections) are not new, the pervasiveness and frequency of their invocation in net-centric architectures can present organizations with significant new challenges.

Dynamic Subsystems

For many information systems, the determination of subsystems is established at system initiation and maintained throughout the life cycle of the system. However, there are some instances, most notably in net-centric architectures, where the subsystems that compose the system may not be present at all stages of the life cycle. Some subsystems may not become part of an information system until sometime after system initiation, while other subsystems may leave the system sometime prior to system termination. Generally, this will not impact the external boundary of the information system if the dynamic subsystems are in the system design and the appropriate security controls are reflected in the security plan. But it does impact the subsystems that exist within the boundary at any given point in time.

Dynamic subsystems that become part of an organizational information system at various points in time may or may not be under the direct control of the organization. These subsystems may be provided by external providers (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements). Regardless of whether the subsystem is or is not controlled by the organization, the expectations of its capabilities have to be considered. The dynamic inclusion or exclusion of the subsystems may or may not require reassessment of the information system as a whole. This is determined based on constraints and assumptions (e.g., functions the subsystems perform, connections to other subsystems and other information systems) imposed upon the subsystems at system design and incorporated in the security plan. So long as the subsystems conform to the identified constraints and assumptions, they can be dynamically added or removed from the information system without requiring reassessments of the entire system.

---

[38] The organization can: (i) issue a single authorization for the entire complex information system (to include bundling assessment results from individual subsystem assessments and any additional assessment results at the system level); or (ii) implement a strategy for managing the risk associated with connecting separately authorized information systems when viewed as a system of systems.

[39] A net-centric architecture is a complex system of systems comprised of subsystems and services that are part of a continuously evolving, complex community of people, devices, information, and services interconnected by a network that enhances information sharing and collaboration. A service-oriented architecture (SOA) is an example of a net-centric architecture.

As noted above, the assumptions and constraints on the dynamic subsystems are reflected in the information system design and the security plan. The determination as to whether the subsystems conform to the assumptions and constraints is addressed during the continuous monitoring phase of the risk management process. Depending upon the nature of the subsystems (including the functions, connections, and relative trust relationships established with the subsystem providers), the determination of conformance may be performed in a manual or automated manner, and may occur prior to, or during the subsystem connecting/disconnecting to the information system.

External Subsystems

Another characteristic often apparent in net-centric architectures is that some of the subsystems (or components of subsystems)[40] are outside of the direct control of the organization that owns the information system and authorizes its operation. The nature of such external subsystems can vary from organizations employing external cloud computing services to process, store, and transmit information to organizations allowing platforms under their control to host applications/services developed by some external entity.

As noted in Appendix I (Security Controls in External Environments), FISMA and OMB policy require external providers handling federal information or operating information systems on behalf of the federal government to meet the same security requirements as federal agencies. These security requirements also apply to external subsystems storing, processing, or transmitting federal information and any services provided by or associated with the subsystem. Appendix I further notes that the assurance or confidence that the risk from using external services is at an acceptable level depends on the trust that the organization places in the external service provider. In some cases, the level of trust is based on the amount of direct control the organization is able to exert on the external service provider with regard to employment of security controls necessary for the protection of the service and the evidence brought forth as to the effectiveness of those controls. In other instances, trust may be based on other factors, such as the experience the organization has with the external service provider, and the confidence (trust) the organization has in the provider taking the correct actions. There are a variety of factors that can complicate the level of trust issue in the case of net-centric architectures to include:

- The delineation between what is owned by the external entity and the organization may be somewhat blurred (e.g., organization-owned platform executing external entity-developed service/application software or firmware);
- The degree of control the organization has over the external entity providing/supporting the subsystems/services may be very limited;
- The nature and content of the subsystems may be subject to rapid change; and
- The subsystems/services may be of such critical nature that they need to be incorporated into organizational information systems very rapidly.

The consequence of the factors above is that some of the more traditional means of verifying the correct functioning of a subsystem and the effectiveness of security controls (e.g., clearly defined requirements, design analysis, testing and evaluation before deployment) may not be feasible for a net-centric subsystem/service. As a result, organizations may be left to depend upon the nature of the trust relationships with the suppliers of the net-centric subsystems/services as the basis for determining whether or not to allow/include the subsystems/services (e.g., use of GSA list of

[40] In this context, the term subsystem includes the *services* provided by or associated with that subsystem.

approved providers). Alternatively, organizations may allow such subsystems/services to be used only in those instances where they have constrained the nature of information or process flow such that the organization believes that any potential adverse impact is manageable. Ultimately, when the level of trust in the external provider of subsystems/services is below expectations, the organization: (i) employs compensating controls; (ii) accepts a greater degree of risk; or (iii) does not obtain the service (i.e., performs its core missions and business operations with reduced levels of functionality or possibly no functionality at all).

2.4 SECURITY CONTROL ALLOCATION

There are three types of security controls for information systems that can be employed by an organization: (i) *system-specific controls* (i.e., controls that provide a security capability for a particular information system only); (ii) *common controls* (i.e., controls that provide a security capability for multiple information systems); or (iii) *hybrid controls* (i.e., controls that have both system-specific and common characteristics).[41] The organization *allocates* security controls to an information system consistent with the organization's enterprise architecture and information security architecture.[42] This activity is carried out as an organization-wide activity involving authorizing officials, information system owners, chief information security officer, senior information security officer, enterprise architect, information security architect, information system security officers, common control providers, and risk executive (function).

As part of the information security architecture, organizations are encouraged to identify and implement security controls that can support multiple information systems efficiently and effectively as a common capability (i.e., common controls). When these controls are used to support a specific information system, they are referenced by that specific system as *inherited controls*. Common controls promote more cost-effective and consistent information security across the organization and can also simplify risk management activities. By allocating security controls to an information system as system-specific controls, hybrid controls, or common controls, the organization assigns responsibility and accountability to specific organizational entities for the overall development, implementation, assessment, authorization, and monitoring of those controls.

The organization has significant flexibility in deciding which families of security controls or specific controls from selected families in NIST Special Publication 800-53 are appropriate for the different types of allocations. Since the security control allocation process involves the assignment and provision of security capabilities derived from security controls, the organization ensures that there is effective communication among all entities either receiving or providing such capabilities. This communication includes, for example, ensuring that common control authorization results and continuous monitoring information are readily available to those organizational entities inheriting common controls, and that any changes to common controls are effectively communicated to those affected by such changes.[43] Figure 2-4 illustrates security

[41] NIST Special Publication 800-53 provides additional guidance on security controls for information systems.

[42] *Allocation* is a term used to describe the process an organization employs: (i) to determine whether security controls are defined as system-specific, hybrid, or common; and (ii) to assign security controls to specific information system components responsible for providing a particular security capability (e.g., router, server, remote sensor).

[43] Communication regarding the security status of common (inherited) controls is essential irrespective of whether the common control provider is internal or external to the organization. Appendix I provides guidance for organizations relying on security controls in external environments including the types of contractual agreements and arrangements that are necessary to ensure appropriate security-relevant information is conveyed to the organization from external providers.

control allocation within an organization and using the RMF to produce information for senior leaders (including authorizing officials) on the ongoing security state of organizational information systems and the missions and business processes supported by those systems.

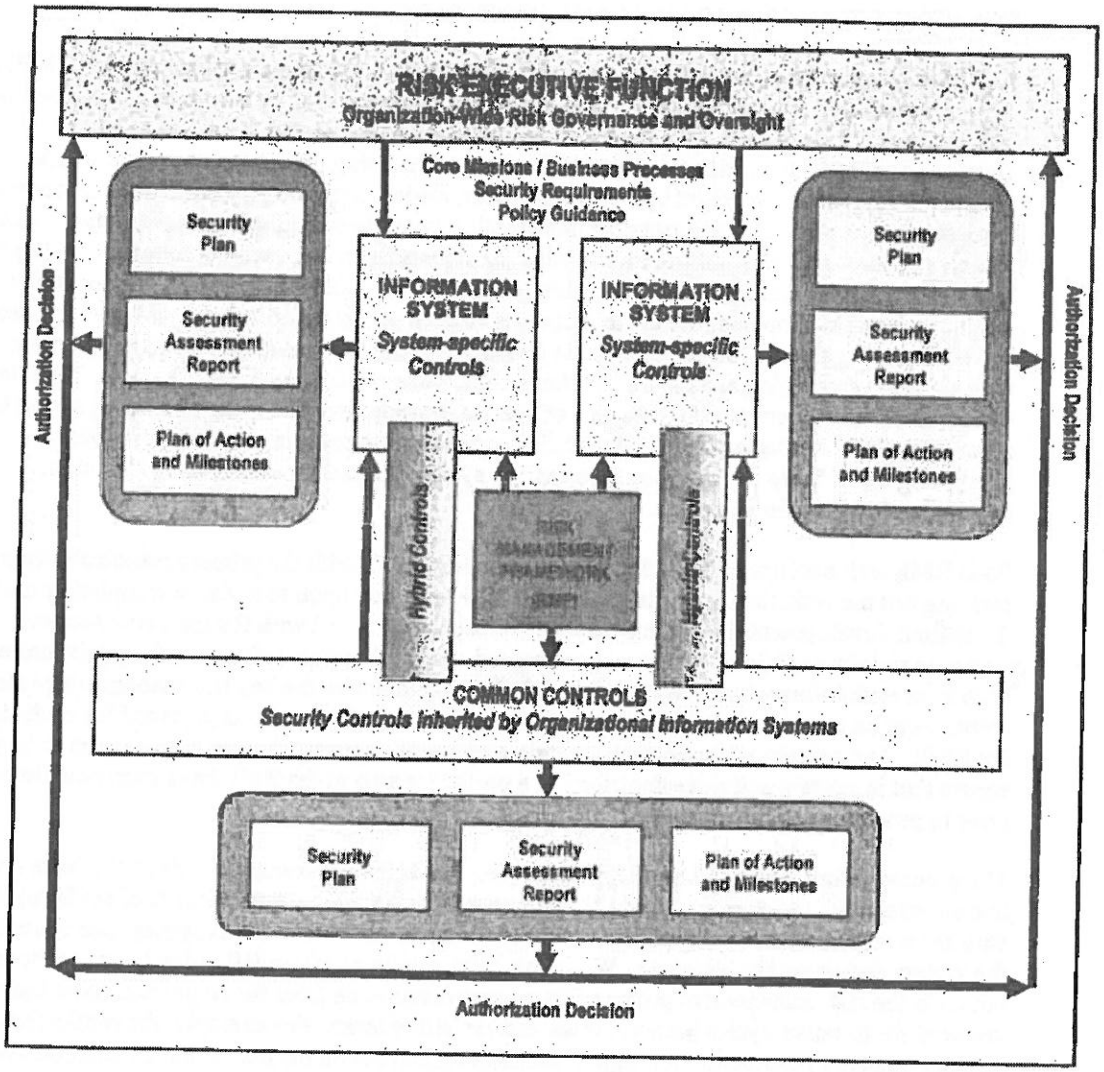


FIGURE 2-4: SECURITY CONTROL ALLOCATION

CHAPTER THREE

THE PROCESS

EXECUTING THE RISK MANAGEMENT FRAMEWORK TASKS

This chapter describes the process of applying the Risk Management Framework (RMF) to federal information systems.[44] The process includes a set of well-defined risk-related tasks that are to be carried out by selected individuals or groups within well-defined organizational roles (e.g., risk executive [function], authorizing official, authorizing official designated representative, chief information officer, senior information security officer, enterprise architect, information security architect, information owner/steward, information system owner, common control provider, information system security officer, and security control assessor).[45] Many risk management roles defined in this publication have counterpart roles defined in the routine system development life cycle processes carried out by organizations. Whenever possible and consistent with core missions/business processes, organizations align risk management roles with similar (or complementary) roles defined for the system development life cycle. RMF tasks are executed concurrently with or as part of system development life cycle processes, taking into account appropriate dependencies. This helps to ensure that organizations are effectively integrating the process of managing information system-related security risks with system development life cycle processes.

Each RMF task description includes the individual or group with the primary responsibility for carrying out the task, the supporting roles that may be called upon to assist in completing the task, the system development life cycle phase most closely associated with the task, supplemental guidance to help explain how the task is executed, and appropriate references for publications or Web sites with information related to the task.[46] To summarize the key risk management-related activities to be carried out by the organization, a milestone checkpoint is provided for each step in the RMF. The milestone checkpoints contain a series of questions for the organization to help ensure that important activities described in a particular step in the RMF have been completed prior to proceeding to the next step.

The process of implementing the RMF tasks (i.e., the order and manner in which the tasks occur and are executed, the names of primary/supporting roles, the names and format of artifacts) may vary from organization to organization. The RMF tasks can be applied at appropriate phases in the system development life cycle. While the tasks appear in sequential order, there can be many points in the risk management process that require divergence from the sequential order including the need for iterative cycles between tasks and revisiting tasks. For example, the results from security control assessments can trigger remediation actions on the part of an information system

[44] The process for managing risk described in this publication can be tailored to meet the needs of many communities of interest within the federal government including, for example, the Civil, Defense, and Intelligence Communities. Tailoring provides flexibility in applying the risk management concepts associated with the RMF in a manner that is most suitable for the organizations and the information systems involved.

[45] Appendix D describes the roles and responsibilities of key participants involved in an organization's risk management process.

[46] A reference is included in the RMF task list if: (i) the reference is generally applicable to both national security systems and nonnational security systems; (ii) the reference for nonnational security systems has an equivalent or supporting reference for national security systems; or (iii) the reference relates to specific national security community guidance regarding the implementation of certain NIST standards or guidelines.

owner, which can in turn require the reassessment of selected controls. Monitoring the security controls in an information system can also generate a potential cycle of tracking changes to the system and its environment of operation, conducting security impact analyses, taking remediation actions, reassessing security controls, and reporting the security status of the system. There may also be other opportunities to diverge from the sequential nature of the tasks when it is more efficient or cost-effective to do so. For example, while the security control assessment tasks are listed after the security control implementation tasks, some organizations may choose to begin the assessment of certain controls as soon as they are implemented but prior to the complete implementation of all controls described in the security plan. This may result in the organization assessing the physical and environmental protection controls within a facility prior to assessing the security controls employed in the hardware and software components of the information system (which may be implemented at a later time). Regardless of the task ordering, the last step before an information system is placed into operation is the explicit acceptance of risk by the authorizing official.

RMF steps and associated tasks can be applied to both new development and legacy information systems. For legacy systems, organizations can use RMF Steps 1 through 3 to confirm that the security categorization has been completed and is appropriate and that the requisite security controls have been selected and allocated. Applying the first three steps in the RMF to legacy systems can be viewed as a *gap analysis* to determine if the necessary and sufficient security controls (i.e., system-specific, hybrid, and common controls) have been appropriately selected and allocated. Security control weaknesses and deficiencies, if discovered, can be subsequently addressed in RMF Steps 3 through 6 similar to new development systems. If no weaknesses or deficiencies are discovered in the security controls during the gap analysis and there is a current security authorization in effect, the organization can move directly to the last step in the RMF, continuous monitoring. If a current security authorization is not in place, the organization continues with RMF Steps 4 through 6.

The security categorization process influences the level of effort expended when implementing the RMF tasks. Information systems supporting the most critical and/or sensitive operations and assets within the organization as indicated by the security categorization, demand the greatest level of attention and effort to ensure that appropriate information security and risk mitigation are achieved. Most RMF tasks can be carried out by external providers with appropriate contractual agreements or other arrangements in place (see Appendix I). A summary table of the RMF tasks is provided in Appendix E.

APPLICATION OF THE RISK MANAGEMENT FRAMEWORK

The Risk Management Framework and associated RMF tasks apply to both *information system owners* and *common control providers*. In addition to supporting the authorization of information systems, the RMF tasks support the selection, development, implementation, assessment, authorization, and ongoing monitoring of common controls inherited by organizational information systems. Execution of the RMF tasks by common control providers, both internal and external to the organization, helps to ensure that the security capabilities provided by the common controls can be inherited by information system owners with a degree of assurance appropriate for their information protection needs. This approach recognizes the importance of security control effectiveness within information systems and the infrastructure supporting those systems.

Since the tasks in the RMF are described in a *sequential* manner, organizations may choose to deviate from that sequential structure in order to be consistent with their established management and system development life cycle processes or to achieve more cost-effective and efficient solutions with regard to the execution of the tasks. Regardless of the task ordering, the last step before an information system is placed into operation is the explicit acceptance of risk by the authorizing official. Organizations may also execute certain RMF tasks in an iterative manner or in different phases of the system development life cycle. For example, security control assessments may be carried out during system development, system implementation, and system operation/maintenance (as part of continuous monitoring).

Organizations may also choose to expend a greater *level of effort* on certain RMF tasks and commit fewer resources to other tasks based on the level of maturity of selected processes and activities within the organization. Since the RMF is life cycle-based, there will be a need to revisit various tasks over time depending on how the organization manages changes to the information systems and the environments in which those systems operate. Managing information security-related risks for an information system is viewed as part of a larger organization-wide risk management activity carried out by senior leaders. The RMF must simultaneously provide a disciplined and structured approach to mitigating risks from the operation and use of organizational information systems and the flexibility and agility to support the core missions and business operations of the organization in highly dynamic environments of operation.

3.1 RMF STEP 1 – CATEGORIZE INFORMATION SYSTEM

SECURITY CATEGORIZATION

TASK 1-1: Categorize the information system and document the results of the security categorization in the security plan.

Primary Responsibility: Information System Owner; Information Owner/Steward.

Supporting Roles: Risk Executive (Function); Authorizing Official or Designated Representative; Chief Information Officer; Senior Information Security Officer; Information System Security Officer.

System Development Life Cycle Phase: Initiation (concept/requirements definition).

Supplemental Guidance: The security categorization process is carried out by the information system owner and information owner/steward in cooperation and collaboration with appropriate organizational officials (i.e., senior leaders with mission/business function and/or risk management responsibilities). The security categorization process is conducted as an organization-wide activity taking into consideration the enterprise architecture and the information security architecture. This helps to ensure that individual information systems are categorized based on the mission and business objectives of the organization. The results of the security categorization process influence the selection of appropriate security controls for the information system and also, where applicable, the minimum assurance requirements for that system. The organization may consider decomposing the information system into multiple subsystems to more efficiently and effectively allocate security controls to the system. One approach is to categorize each identified subsystem (including dynamic subsystems). Separately categorizing each subsystem does not change the overall categorization of the information system. Rather, it allows the constituent subsystems to receive a separate allocation of security controls from NIST Special Publication 800-53 instead of deploying higher-impact controls across every subsystem. Another approach is to bundle smaller subsystems into larger subsystems within the information system, categorize each of the aggregated subsystems, and allocate security controls to the subsystems, as appropriate. Security categorization information is documented in the system identification section of the security plan or included as an attachment to the plan. The risk executive (function) provides guidance and relevant information to authorizing officials concerning the *risk management strategy* for the organization (e.g., risk assessment methodologies employed by the organization, evaluation of risks determined, risk mitigation approaches, organizational risk tolerance, approaches for monitoring risk over time, known existing aggregated risks from current information systems, and other sources of risk). Security categorization determinations consider potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation.

References: FIPS Publication 199; NIST Special Publications 800-30, 800-39, 800-59, 800-60; CNSS Instruction 1253.

INFORMATION SYSTEM DESCRIPTION

TASK 1-2: Describe the information system (including system boundary) and document the description in the security plan.

Primary Responsibility: Information System Owner.

Supporting Roles: Authorizing Official or Designated Representative; Senior Information Security Officer; Information Owner/Steward; Information System Security Officer.

System Development Life Cycle Phase: Initiation (concept/requirements definition).

Supplemental Guidance: Descriptive information about the information system is documented in the *system identification* section of the security plan, included in attachments to the plan, or referenced in other standard sources for information generated as part of the system development life cycle. Duplication of information is avoided, whenever possible. The level of detail provided in the security plan is determined by the organization and is typically commensurate with the security categorization of the information system. Information may be added to the system description as it becomes available during the system development life cycle and execution of the RMF tasks. A system description may include, for example:

- Full descriptive name of the information system including associated acronym;
- Unique information system identifier (typically a number or code);
- Information system owner and authorizing official including contact information;
- Parent or governing organization that manages, owns, and/or controls the information system;
- Location of the information system and environment in which the system operates;
- Version or release number of the information system;

- Purpose, functions, and capabilities of the information system and missions/business processes supported;
- How the information system is integrated into the enterprise architecture and information security architecture;
- Status of the information system with respect to acquisition and/or system development life cycle;
- Results of the security categorization process for the information and information system;
- Types of information processed, stored, and transmitted by the information system;
- Boundary of the information system for risk management and security authorization purposes;
- Applicable laws, directives, policies, regulations, or standards affecting the security of the information system;
- Architectural description of the information system including network topology;
- Hardware and firmware devices included within the information system;
- System and applications software resident on the information system;
- Hardware, software, and system interfaces (internal and external);
- Subsystems (static and dynamic) associated with the information system;
- Information flows and paths (including inputs and outputs) within the information system;
- Cross domain devices/requirements;
- Network connection rules for communicating with external information systems;
- Interconnected information systems and identifiers for those systems;
- Encryption techniques used for information processing, transmission, and storage;
- Cryptographic key management information (public key infrastructures, certificate authorities, etc.);
- Information system users (including organizational affiliations, access rights, privileges, citizenship, if applicable);
- Ownership/operation of information system (e.g., government-owned, government-operated; government-owned, contractor-operated; contractor-owned, contractor-operated; nonfederal [state and local governments, grantees]);
- Security authorization date and authorization termination date;
- Incident response points of contact; and
- Other information as required by the organization.

References: None.

INFORMATION SYSTEM REGISTRATION

TASK 1-3: Register the information system with appropriate organizational program/management offices.

Primary Responsibility: Information System Owner.

Supporting Roles: Information System Security Officer.

System Development Life Cycle Phase: Initiation (concept/requirements definition).

Supplemental Guidance: The *registration* process begins by identifying the information system (and subsystems, if appropriate) in the system inventory and establishes a relationship between the information system and the parent or governing organization that owns, manages, and/or controls the system. Information system registration, in accordance with organizational policy, uses information in the system identification section of the security plan to inform the parent or governing organization of: (i) the existence of the information system; (ii) the key characteristics of the system; and (iii) any security implications for the organization due to the ongoing operation of the system. Information system registration provides organizations with an effective management/tracking tool that is necessary for security status reporting in accordance with applicable laws, Executive Orders, directives, policies, standards, guidance, or regulations. Those subsystems that are more dynamic in nature (e.g., subsystems in net-centric architectures) may not be present throughout all phases of the system development life cycle. Such subsystems are registered either as a subset of a well-defined information system or a method of registration for dynamic subsystems is implemented that includes as much information as feasible. Some information about dynamic subsystems is known prior to the subsystem manifesting itself in the information system (e.g., assumptions and constraints specified in the security plan). However, more detailed information may not be known until the subsystem manifests itself.

References: None.

Milestone Checkpoint #1

- Has the organization completed a *security categorization* of the information system including the information to be processed, stored, and transmitted by the system?
- Are the results of the security categorization process for the information system consistent with the organization's *enterprise architecture* and commitment to *protecting organizational missions/business processes*?
- Do the results of the security categorization process reflect the organization's *risk management strategy*?
- Has the organization adequately described the *characteristics* of the information system?
- Has the organization *registered* the information system for purposes of management, accountability, coordination, and oversight?

3.2 RMF STEP 2 – SELECT SECURITY CONTROLS

COMMON CONTROL IDENTIFICATION

TASK 2-1: Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).

Primary Responsibility: Chief Information Officer or Senior Information Security Officer; Information Security Architect; Common Control Provider.

Supporting Roles: Risk Executive (Function); Authorizing Official or Designated Representative; Information System Owner; Information System Security Engineer.

System Development Life Cycle Phase: Initiation (concept/requirements definition).

Supplemental Guidance: Common controls are security controls that are inherited by one or more organizational information systems. Common controls are identified by the chief information officer and/or senior information security officer in collaboration with the information security architect and assigned to specific organizational entities (designated as common control providers) for development, implementation, assessment, and monitoring. Common control providers may also be *information system owners* when the common controls are resident within an information system. The organization consults information system owners when identifying common controls to ensure that the security capability provided by the inherited controls is sufficient to deliver adequate protection. When the common controls provided by the organization are not sufficient for information systems inheriting the controls, the system owners supplement the common controls with system-specific or hybrid controls to achieve the required protection for the system and/or accept greater risk. Information system owners inheriting common controls can either document the implementation of the controls in their respective security plans or reference the controls contained in the security plans of the common control providers. Organizations may choose to defer common control identification and security control selection until a later phase in the system development life cycle. When common controls are not resident within an information system (e.g., physical and environmental protection controls, personnel security controls), the organization selects one or more senior organizational officials or executives to serve as authorizing officials for those controls. These authorizing officials are responsible for accepting the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the deployment of the security controls provided by common control providers and *inherited* by organizational information systems. Common control providers are responsible for: (i) documenting common controls in a *security plan* (or equivalent document prescribed by the organization); (ii) ensuring that common controls are developed, implemented, and assessed for effectiveness by qualified assessors with a level of independence required by the organization; (iii) documenting assessment findings in a *security assessment report*; (iv) producing a *plan of action and milestones* for all common controls deemed less than effective (i.e., having unacceptable weaknesses or deficiencies in the controls); (v) receiving authorization for the common controls from the designated authorizing official; and (vi) monitoring common control effectiveness on an ongoing basis.

Security plans, security assessment reports, and plans of action and milestones for common controls (or a summary of such information) are made available to information system owners (whose systems are *inheriting* the controls) after the information is reviewed and approved by the senior official or executive responsible and accountable for the controls. The organization ensures that common control providers keep this information current since the controls typically support multiple organizational information systems. Security plans, security assessment reports, and plans of action and milestones for common controls are used by authorizing officials within the organization to make risk-based decisions in the security authorization process for their information systems. The use of common controls is documented within the security plans for information systems inheriting those controls. Organizations ensure that common control providers have the capability to rapidly broadcast changes in the status of common controls that adversely affect the protections being provided by and expected of the common controls. Common control providers are able to quickly inform information system owners when problems arise in the inherited common controls (e.g., when an assessment or reassessment of a common control indicates the control is flawed in some manner, when a new threat or attack method arises that renders the common control less than effective in protecting against the new threat or attack method). Organizations are encouraged, when feasible, to employ automated management systems to maintain records of the specific common controls used in each organizational information system to enhance the ability of common control providers to rapidly communicate with information system owners. If common controls are provided to the organization (and its information systems) by entities *external* to the organization (e.g., shared and/or external service providers), arrangements are made with the external/shared service providers by the organization to obtain information on the effectiveness of the deployed controls. Information obtained from external organizations regarding the effectiveness of common controls is factored into authorization decisions.

References: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-53; CNSS Instruction 1253.

SECURITY CONTROL SELECTION

TASK 2-2: Select the security controls for the information system and document the controls in the security plan.

Primary Responsibility: Information Security Architect; Information System Owner.

Supporting Roles: Authorizing Official or Designated Representative; Information Owner/Steward; Information System Security Officer; Information System Security Engineer.

System Development Life Cycle Phase: Initiation (concept/requirements definition).

Supplemental Guidance: The security controls are selected based on the security categorization of the information system. The security control selection process includes, as appropriate: (i) choosing a set of baseline security controls; (ii) tailoring the baseline security controls by applying scoping, parameterization, and compensating control guidance; (iii) supplementing the tailored baseline security controls, if necessary, with additional controls and/or control enhancements to address unique organizational needs based on a risk assessment (either formal or informal) and local conditions including environment of operation, organization-specific security requirements, specific threat information, cost-benefit analyses, or special circumstances; and (iv) specifying minimum assurance requirements, as appropriate. Organizations document in the security plan, the decisions (e.g., tailoring, supplementation, etc.) taken during the security control selection process, providing a sound rationale for those decisions. The security plan contains an overview of the security requirements for the information system in sufficient detail to determine that the security controls selected would meet those requirements. The security plan, in addition to the list of security controls to be implemented, describes the intended application of each control in the context of the information system with sufficient detail to enable a compliant implementation of the control. During the security control selection process organizations may begin planning for the continuous monitoring process by developing a monitoring strategy. The strategy can include, for example, monitoring criteria such as the volatility of specific security controls and the appropriate frequency of monitoring specific controls. Organizations may choose to address security control volatility and frequency of monitoring during control selection as inputs to the continuous monitoring process. The monitoring strategy can be included in the security plan to support the concept of near real-time risk management and ongoing authorization (see Task 2-3). Information system owners *inheriting* common controls can either document the implementation of the controls in their respective security plans or reference the controls contained in the security plans of the common control providers (see Task 2-1). Information system owners can refer to the security authorization packages prepared by common control providers when making determinations regarding the adequacy of common controls inherited by their respective systems.

For net-centric architectures where subsystems may be added or removed from an information system dynamically, the organization includes in the security plan for the system: (i) descriptions of the functions of the dynamic subsystems; (ii) the security controls employed in the subsystems; (iii) constraints/assumptions regarding the functions of the dynamic subsystems and the associated security controls in the subsystems; (iv) dependencies of other subsystems on the proper functioning of the security controls of the dynamic subsystems; (v) procedures for determining that the dynamic subsystems conform to the security plan, assumptions, and constraints; and (vi) the impact of the dynamic subsystems and associated security controls on existing security controls in the information system. While inclusion of a dynamic subsystem may impact the information system or some of the currently identified subsystems, it does not necessarily mean the subsystem will impact the *security* of the system or other subsystems. That is, not all subsystems are security relevant. Changes in the net-centric architectures that exceed the anticipated limits of the security plan may not be allowed or may require reassessment prior to being approved. When security controls are designated as common controls, the organization ensures that sufficient information is available to information system owners and authorizing officials to support the risk management process. When security services are provided by external providers (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization: (i) defines the external services provided to the organization; (ii) describes how the external services are protected in accordance with the security requirements of the organization; and (iii) obtains the necessary assurances that the risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of the external services is acceptable. The organization also considers that replicated subsystems within a complex information system may exhibit common vulnerabilities that can be exploited by a common threat source, thereby negating the redundancy that might be relied upon as a risk mitigation measure. The impact due to a security incident against one constituent subsystem might cascade and impact many subsystems at the same time.

References: FIPS Publications 199, 200; NIST Special Publications 800-30, 800-53; CNSS Instruction 1253.

MONITORING STRATEGY

TASK 2-3: Develop a strategy for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation.

Primary Responsibility: Information System Owner or Common Control Provider.

Supporting Roles: Risk Executive (Function); Authorizing Official or Designated Representative; Chief Information Officer; Senior Information Security Officer; Information Owner/Steward; Information System Security Officer.

System Development Life Cycle Phase: Initiation (concept/requirements definition).

Supplemental Guidance: A critical aspect of risk management is the ongoing monitoring of security controls employed within or inherited by the information system. An effective monitoring strategy is developed early in the system development life cycle (i.e., during system design or COTS procurement decision) and can be included in the security plan. The implementation of a robust continuous monitoring program allows an organization to understand the security state of the information system over time and maintain the initial security authorization in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business functions. The ongoing monitoring of security controls using automated tools and supporting databases facilitates near real-time risk management for the information system. An effective monitoring program includes: (i) configuration management and control processes; (ii) security impact analyses on proposed or actual changes to the information system and its environment of operation; (iii) assessment of selected security controls employed within and inherited by the information system (including controls in dynamic subsystems); and (iv) security status reporting to appropriate organizational officials. The continuous monitoring strategy for the information system identifies the security controls to be monitored, the frequency of monitoring, and the control assessment approach. The strategy defines how changes to the information system will be monitored, how security impact analyses will be conducted, and the security status reporting requirements including recipients of the status reports.

The criteria for selecting security controls to be monitored post deployment and for determining the frequency of such monitoring is established by the information system owner or common control provider in collaboration with selected organizational officials including, for example, the authorizing official or designated representative, chief information officer, senior information security officer, and risk executive (function). The selection criteria reflect the priorities and importance of the information system to organizational operations and assets, individuals, other organizations, and the Nation. Security controls that are volatile (i.e., most likely to change over time), critical to certain aspects of the organization's protection strategy, or identified in current plans of action and milestones are assessed as frequently as necessary consistent with the criticality of the function and capability of the monitoring tools. The use of automation facilitates a greater frequency and volume of security control assessments.

Determining the frequency for assessing security controls inherited by the information system (i.e., common controls) includes the organization's determination of the trustworthiness of the common control provider. An organizational assessment of risk (either formal or informal) can also be used to guide the selection of specific security controls to be monitored and the frequency of such monitoring. The approach to security control assessments during continuous monitoring may include detection of the status of information system components and analysis of historical, operational data, as well as the reuse of assessment procedures and results that supported the initial authorization decision.

The authorizing official or designated representative approve the monitoring strategy including the set of security controls that are to be monitored on an ongoing basis as well as the frequency of the monitoring activities. The approval of the monitoring strategy can be obtained in conjunction with the security plan approval. The monitoring of security controls continues throughout the system development life cycle. For security controls employed in information systems with dynamic subsystems, the monitoring strategy accounts for subsystems that did not exist at the beginning of the system development life cycle. An effective monitoring strategy for dynamic subsystems achieves an appropriate balance with regard to risk by: (i) not placing unnecessary or unrealistic burdens on the organization by requiring reauthorization of the information system each time a new subsystem is added or removed; and (ii) not compromising the accepted security posture of the overall system.

References: NIST Special Publications 800-30, 800-39, 800-53; 800-53A; CNSS Instruction 1253.

SECURITY PLAN APPROVAL

TASK 2-4: Review and approve the security plan.

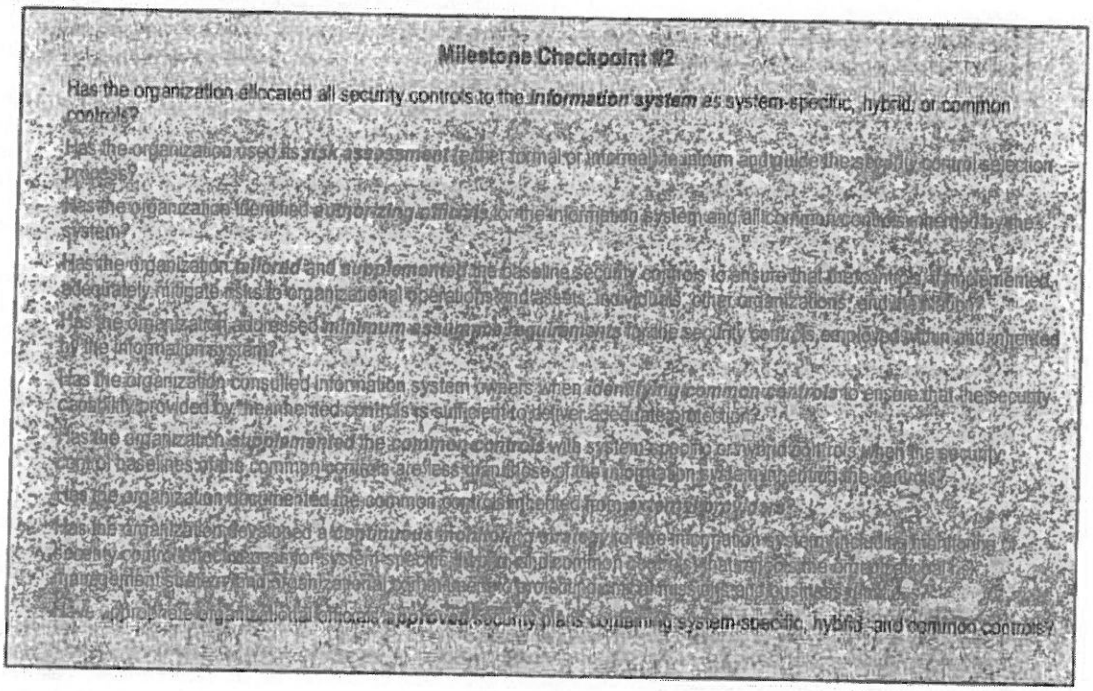
Primary Responsibility: Authorizing Official or Designated Representative.

Supporting Roles: Risk Executive (Function); Chief Information Officer; Senior Information Security Officer.

System Development Life Cycle Phase: Development/Acquisition.

Supplemental Guidance: The independent review of the security plan by the authorizing official or designated representative with support from the senior information security officer, chief information officer, and risk executive (function), helps determine if the plan is complete, consistent, and satisfies the stated security requirements for the information system. The security plan review also helps to determine, to the greatest extent possible with available planning or operational documents, if the security plan correctly and effectively identifies the potential risk to organizational operations and assets, individuals, other organizations, and the Nation, that would be incurred if the controls identified in the plan were implemented as intended. Based on the results of this independent review and analysis, the authorizing official or designated representative, chief information officer, senior information security officer, or risk executive (function) may recommend changes to the security plan. If the security plan is deemed unacceptable, the authorizing official or designated representative sends the plan back to the information system owner (or common control provider) for appropriate action. If the security plan is deemed acceptable, the authorizing official or designated representative approves the plan. The acceptance of the security plan represents an important milestone in both the risk management process and the system development life cycle. The authorizing official or designated representative, by approving the security plan, agrees to the set of security controls (system-specific, hybrid, and/or common controls) proposed to meet the security requirements for the information system. This approval allows the risk management process to advance to the next step in the RMF (i.e., the implementation of the security controls). The approval of the security plan also establishes the level of effort required to successfully complete the remainder of the steps in the RMF and provides the basis of the security specification for the acquisition of the information system, subsystems, or components.

References: NIST Special Publications 800-30, 800-53; CNSS Instruction 1253.



3.3 RMF STEP 3 – IMPLEMENT SECURITY CONTROLS

SECURITY CONTROL IMPLEMENTATION

TASK 3-1: Implement the security controls specified in the security plan.

Primary Responsibility: Information System Owner or Common Control Provider.

Supporting Roles: Information Owner/Steward; Information System Security Officer; Information System Security Engineer.

System Development Life Cycle Phase: Development/Acquisition; Implementation.

Supplemental Guidance: Security control implementation is consistent with the organization's enterprise architecture and information security architecture. The information security architecture serves as a resource to allocate security controls (including, for example, security mechanisms and services) to an information system and any organization-defined subsystems. Security controls targeted for deployment within the information system (including subsystems) are allocated to specific system components responsible for providing a particular security capability. Not all security controls need to be allocated to every subsystem. Categorization of subsystems, information security architecture, and allocation of security controls work together to help achieve a suitable balance. Allocating some security controls as common controls or hybrid controls is part of this architectural process. Organizations use best practices when implementing the security controls within the information system including system and software engineering methodologies, security engineering principles, and secure coding techniques. In addition, organizations ensure that mandatory configuration settings are established and implemented on information technology products in accordance with federal and organizational policies (e.g., Federal Desktop Core Configuration). Information system security engineers with support from information system security officers employ a sound security engineering process that captures and refines information security requirements and ensures the integration of those requirements into information technology products and systems through purposeful security design or configuration. When available, organizations consider the use of information technology products that have been tested, evaluated, or validated by approved, independent, third-party assessment facilities. In addition, organizations satisfy, where applicable, minimum assurance requirements when implementing security controls. Assurance requirements are directed at the activities and actions that security control developers and implementers define and apply to increase the level of confidence that the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Assurance requirements address the quality of the design, development, and implementation of the security functions in the information system. For higher-impact systems (i.e., potential high-value targets) in situations where specific and credible threat information indicates the likelihood of advanced cyber attacks, additional assurance measures are considered. Organizations consider any implementation-related issues associated with the integration and/or interfaces among common controls and system-specific controls.

For the identified common controls inherited by the information system, information system security engineers with support from information system security officers coordinate with the common control provider to determine the most appropriate way to apply the common controls to the organizational information systems. For certain management and operational controls, formal integration into information technology products, services, and systems may not be required. For certain types of operational and/or technical controls, implementation may require additional components, products, or services to enable the information system to utilize the previously selected common controls to the fullest extent. If selection of common controls previously had been deferred, identification of common controls inherited by the information system is revisited to determine if better determinations can be made at this point in the system development life cycle. Information system owners can refer to the authorization packages prepared by common control providers when making determinations regarding the adequacy of the implementations of common controls for their respective systems. For common controls that do not meet the protection needs of the information systems inheriting the controls or that have unacceptable weaknesses or deficiencies, the system owners identify compensating or supplementary controls to be implemented. To the maximum extent and consistent with the flexibility allowed in applying the tasks in the RMF, organizations and their contractors conduct initial security control assessments (also referred to as developmental testing and evaluation) during information system development and implementation. Conducting security control assessments in parallel with the development and implementation phases of the system development life cycle facilitates the early identification of weaknesses and deficiencies and provides the most cost-effective method for initiating corrective actions. Issues found during these assessments can be referred to authorizing officials for early resolution, as appropriate. The results of the initial security control assessments can also be used during the security authorization process to avoid delays or costly repetition of assessments. Assessment results that are subsequently reused in other phases of the system development life cycle meet the reuse requirements (including independence) established by the organization.

References: FIPS Publication 200; NIST Special Publications 800-30, 800-53, 800-53A; CNSS Instruction 1253; Web: SCAP.NIST.GOV.

SECURITY CONTROL DOCUMENTATION

TASK 3-2: Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).

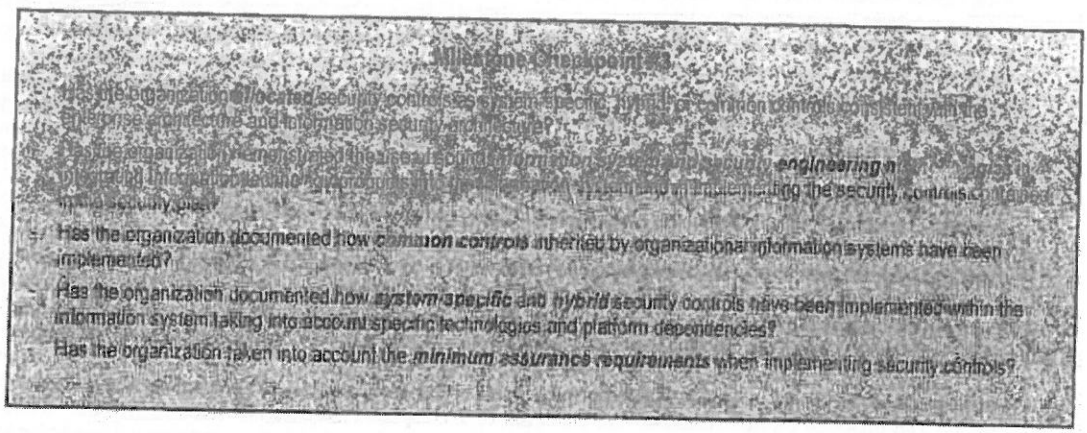
Primary Responsibility: Information System Owner or Common Control Provider.

Supporting Roles: Information Owner/Steward; Information System Security Officer; Information System Security Engineer.

System Development Life Cycle Phase: Development/Acquisition; Implementation.

Supplemental Guidance: Security control documentation describes how system-specific, hybrid, and common controls are implemented. The documentation formalizes plans and expectations regarding the overall functionality of the information system. The functional description of the security control implementation includes planned inputs, expected behavior, and expected outputs where appropriate, typically for those technical controls that are employed in the hardware, software, or firmware components of the information system. Documentation of security control implementation allows for traceability of decisions prior to and after deployment of the information system. The level of effort expended on documentation of the information system is commensurate with the purpose, scope, and impact of the system with respect to organizational missions, business functions, and operations. To the extent possible, organizations reference existing documentation (either by vendors or other organizations that have employed the same or similar information systems), use automated support tools, and maximize communications to increase the overall efficiency and cost effectiveness of security control implementation. The documentation also addresses platform dependencies and includes any additional information necessary to describe how the security capability required by the security control is achieved at the level of detail sufficient to support control assessment. Documentation for security control implementation follows best practices for hardware and software development as well as for system/security engineering disciplines and is consistent with established organizational policies and procedures for documenting system development life cycle activities. Whenever possible and practicable for technical security controls that are mechanism-based, organizations take maximum advantage of functional specifications provided by or obtainable from hardware and software vendors and/or systems integrators including security-relevant documentation that may assist the organization during the assessment and monitoring of the controls. Similarly, for management and operational controls, organizations obtain security control implementation information from appropriate organizational entities (e.g., facilities offices, human resource offices, physical security offices). Since the enterprise architecture and information security architecture established by the organization significantly influence the approach used to implement security controls, providing documentation of this process helps to ensure traceability with regard to meeting the organization's information security requirements.

References: NIST Special Publication 800-53; CNSS Instruction 1253.



3.4 RMF STEP 4 – ASSESS SECURITY CONTROLS

ASSESSMENT PREPARATION

TASK 4-1: Develop, review, and approve a plan to assess the security controls.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Authorizing Official or Designated Representative; Chief Information Officer; Senior Information Security Officer; Information System Owner or Common Control Provider; Information Owner/Steward; Information System Security Officer.

System Development Life Cycle Phase: Development/Acquisition; Implementation.

Supplemental Guidance: The *security assessment plan* provides the objectives for the security control assessment, a detailed roadmap of how to conduct such an assessment, and assessment procedures. The assessment plan reflects the type of assessment the organization is conducting (e.g., developmental testing and evaluation, independent verification and validation, assessments supporting security authorizations or reauthorizations, audits, continuous monitoring, assessments subsequent to remediation actions). Conducting security control assessments in parallel with the development/acquisition and implementation phases of the life cycle permits the identification of weaknesses and deficiencies early and provides the most cost-effective method for initiating corrective actions. Issues found during these assessments can be referred to authorizing officials for early resolution, as appropriate. The results of security control assessments carried out during system development and implementation can also be used (consistent with reuse criteria) during the security authorization process to avoid system fielding delays or costly repetition of assessments. The security assessment plan is reviewed and approved by appropriate organizational officials to ensure that the plan is consistent with the security objectives of the organization, employs state-of-the practice tools, techniques, procedures, and automation to support the concept of continuous monitoring and near real-time risk management, and is cost-effective with regard to the resources allocated for the assessment. The purpose of the security assessment plan approval is two-fold: (i) to establish the appropriate expectations for the security control assessment; and (ii) to bound the level of effort for the security control assessment. An approved security assessment plan helps to ensure that an appropriate level of resources is applied toward determining security control effectiveness. When security controls are provided to an organization by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization obtains a security assessment plan from the provider.

Organizations consider both the *technical expertise* and level of *independence* required in selecting security control assessors. Organizations also ensure that security control assessors possess the required skills and technical expertise to successfully carry out assessments of system-specific, hybrid, and common controls. This includes knowledge of and experience with the specific hardware, software, and firmware components employed by the organization. An independent assessor is any individual or group capable of conducting an impartial assessment of security controls employed within or inherited by an information system. Impartiality implies that assessors are free from any perceived or actual conflicts of interest with respect to the development, operation, and/or management of the information system or the determination of security control effectiveness. Independent security control assessment services can be obtained from other elements within the organization or can be contracted to a public or private sector entity outside of the organization. Contracted assessment services are considered independent if the information system owner is not directly involved in the contracting process or cannot unduly influence the independence of the assessor(s) conducting the assessment of the security controls. The authorizing official or designated representative determines the required level of independence for security control assessors based on the results of the security categorization process for the information system and the ultimate risk to organizational operations and assets, individuals, other organizations, and the Nation. The authorizing official determines if the level of assessor independence is sufficient to provide confidence that the assessment results produced are sound and can be used to make a risk-based decision on whether to place the information system into operation or continue its operation. In special situations, for example when the organization that owns the information system is small or the organizational structure requires that the security control assessment be accomplished by individuals that are in the developmental, operational, and/or management chain of the system owner, independence in the assessment process can be achieved by ensuring that the assessment results are carefully reviewed and analyzed by an independent team of experts to validate the completeness, consistency, and veracity of the results. The authorizing official consults with the Office of the Inspector General, the senior information security officer, and the chief information officer to discuss the implications of any decisions on assessor independence in the types of special circumstances described above. This discussion may occur prior to each security assessment or only once if an organization is establishing an organizational policy and approach for specific special circumstances that will be applied to all information systems meeting the specific special circumstance criteria. Security control assessments in support of initial and subsequent security authorizations are conducted by independent assessors.

References: NIST Special Publication 800-53A.

SECURITY CONTROL ASSESSMENT

TASK 4-2: Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Information System Owner or Common Control Provider; Information Owner/Steward; Information System Security Officer.

System Development Life Cycle Phase: Development/Acquisition; Implementation.

Supplemental Guidance: Security control assessments determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Security control assessments occur as early as practicable in the system development life cycle, preferably during the development phase of the information system. These types of assessments are referred to as *developmental testing and evaluation* and are intended to validate that the required security controls are implemented correctly and consistent with the established information security architecture. Developmental testing and evaluation activities include, for example, design and code reviews, application scanning, and regression testing. Security weaknesses and deficiencies identified early in the system development life cycle can be resolved more quickly and in a much more cost-effective manner before proceeding to subsequent phases in the life cycle. The objective is to identify the information security architecture and security controls up front and to ensure that the system design and testing validate the implementation of these controls.

The information system owner relies on the technical expertise and judgment of assessors to: (i) assess the security controls employed within or inherited by the information system using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and reduce or eliminate identified vulnerabilities. The assessor findings are an unbiased, factual reporting of the weaknesses and deficiencies discovered during the security control assessment. Organizations are encouraged to maximize the use of automation to conduct security control assessments to help: (i) increase the speed and overall effectiveness and efficiency of the assessments; and (ii) support the concept of ongoing monitoring of the security state of organizational information systems. When iterative development processes such as agile development are employed, this typically results in an iterative assessment as each cycle is conducted. A similar process is used for assessing security controls in COTS information technology products employed within the information system. Even when iterative development is not employed, organizations may choose to begin assessing security controls prior to the complete implementation of all security controls listed in the security plan. This type of *incremental assessment* is appropriate if it is more efficient or cost-effective to do so. For example, policy, procedures, and plans may be assessed prior to the assessment of the technical security controls in the hardware and software. In many cases, common controls (i.e., security controls inherited by the information system) may be assessed prior to the security controls employed within the system.

The organization ensures that assessors have access to: (i) the information system and environment of operation where the security controls are employed; and (ii) the appropriate documentation, records, artifacts, test results, and other materials needed to assess the security controls. In addition, assessors have the required degree of independence as determined by the authorizing official (see Appendix D.13 and Appendix F.4). Security control assessments in support of initial and subsequent security authorizations are conducted by independent assessors. Assessor independence during continuous monitoring, although not mandated, facilitates reuse of assessment results when reauthorization is required. When security controls are provided to an organization by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization ensures that assessors have access to the information system/environment of operation where the controls are employed as well as appropriate information needed to carry out the assessment. The organization also obtains any information related to existing assessments that may have been conducted by the external provider and reuses such assessment information whenever possible in accordance with the reuse criteria established by the organization. Descriptive information about the information system is typically documented in the system identification section of the security plan or included by reference or as attachments to the plan. Supporting materials such as procedures, reports, logs, and records showing evidence of security control implementation are identified as well. In order to make the risk management process as timely and cost-effective as possible, the reuse of previous assessment results, when reasonable and appropriate, is strongly recommended. For example, a recent audit of an information system may have produced information about the effectiveness of selected security controls. Another opportunity to reuse previous assessment results comes from programs that test and evaluate the security features of commercial information technology products. Additionally, if prior assessment results from the system developer are available, the security control assessor, under appropriate circumstances, may incorporate those results into the assessment. And finally, assessment results are reused to support reciprocity where possible.

References: NIST Special Publication 800-53A.

SECURITY ASSESSMENT REPORT

TASK 4-3: Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Information System Owner or Common Control Provider; Information System Security Officer.

System Development Life Cycle Phase: Development/Acquisition; Implementation.

Supplemental Guidance: The results of the security control assessment, including recommendations for correcting any weaknesses or deficiencies in the controls, are documented in the *security assessment report*. The security assessment report is one of three key documents in the security authorization package developed for authorizing officials. The assessment report includes information from the assessor necessary to determine the effectiveness of the security controls employed within or inherited by the information system based upon the assessor's findings. The security assessment report is an important factor in an authorizing official's determination of risk to organizational operations and assets, individuals, other organizations, and the Nation. Security control assessment results are documented at a level of detail appropriate for the assessment in accordance with the reporting format prescribed by organizational and/or federal policies. The reporting format is also appropriate for the type of security control assessment conducted (e.g., developmental testing and evaluation, self-assessments, independent verification and validation, independent assessments supporting the security authorization process or subsequent reauthorizations, assessments during continuous monitoring, assessments subsequent to remediation actions, independent audits/evaluations).

Security control assessment results obtained during system development are brought forward in an interim report and included in the final security assessment report. This supports the concept that the security assessment report is an evolving document that includes assessment results from all relevant phases of the system development life cycle including the results generated during continuous monitoring. Organizations may choose to develop an *executive summary* from the detailed findings that are generated during a security control assessment. An executive summary provides an authorizing official with an abbreviated version of the assessment report focusing on the highlights of the assessment, synopsis of key findings, and/or recommendations for addressing weaknesses and deficiencies in the security controls.

References: NIST Special Publication 800-53A.

REMEDIATION ACTIONS

TASK 4-4: Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.

Primary Responsibility: Information System Owner or Common Control Provider; Security Control Assessor.

Supporting Roles: Authorizing Official or Designated Representative; Chief Information Officer; Senior Information Security Officer; Information Owner/Steward; Information System Security Officer; Information System Security Engineer; Security Control Assessor.

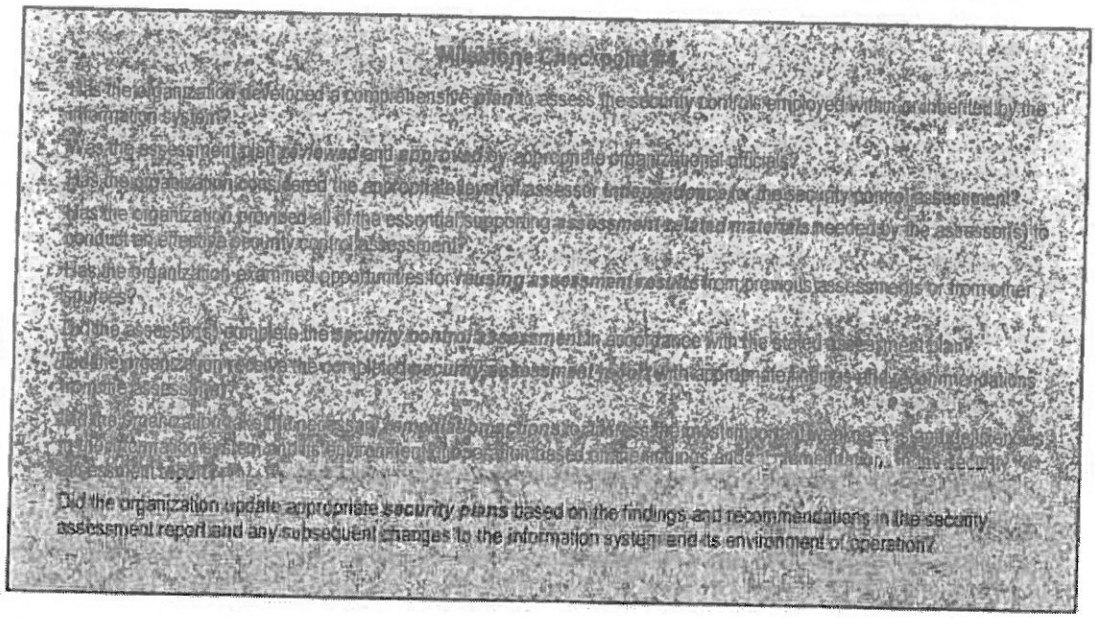
System Development Life Cycle Phase: Development/Acquisition; Implementation.

Supplemental Guidance: The security assessment report provides visibility into specific weaknesses and deficiencies in the security controls employed within or inherited by the information system that could not reasonably be resolved during system development. The findings generated during the security control assessment facilitate a disciplined and structured approach to mitigating risks in accordance with organizational priorities. Information system owners and common control providers, in collaboration with selected organizational officials (e.g., information system security engineer, authorizing official designated representative, chief information officer, senior information security officer, information owner/steward), may decide that certain findings are inconsequential and present no significant risk to the organization. Alternatively, the organizational officials may decide that certain findings are in fact, significant, requiring immediate remediation actions. In all cases, organizations review assessor findings and determine the severity or seriousness of the findings (i.e., the potential adverse impact on organizational operations and assets, individuals, other organizations, or the Nation) and whether the findings are sufficiently significant to be worthy of further investigation or remediation. An updated assessment of risk (either formal or informal) based on the results of the findings produced during the security control assessment and any inputs from the risk executive (function), helps to determine the initial remediation actions and the prioritization of such actions. Senior leadership involvement in the mitigation process may be necessary in order to ensure that the organization's resources are effectively allocated in accordance with organizational priorities, providing resources first to the information systems that are supporting the most critical and sensitive missions and business functions for the organization or correcting the deficiencies that pose

the greatest degree of risk. If weaknesses or deficiencies in security controls are corrected, the remediated controls are reassessed for effectiveness. Security control reassessments determine the extent to which the remediated controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. Exercising caution not to change the original assessment results, assessors update the security assessment report with the findings from the reassessment. The security plan is updated based on the findings of the security control assessment and any remediation actions taken. The updated security plan reflects the actual state of the security controls after the initial assessment and any modifications by the information system owner or common control provider in addressing recommendations for corrective actions. At the completion of the assessment, the security plan contains an accurate list and description of the security controls implemented (including compensating controls) and a list of residual vulnerabilities.

Organizations can prepare an optional addendum to the security assessment report that is transmitted to the authorizing official. The optional addendum provides information system owners and common control providers an opportunity to respond to the initial findings of assessors. The addendum may include, for example, information regarding initial remediation actions taken by information system owners or common control providers in response to assessor findings, or provide an owner's perspective on the findings (e.g., including additional explanatory material, rebutting certain findings, and correcting the record). The addendum to the security assessment report does not change or influence in any manner, the initial assessor findings provided in the original report. Information provided in the addendum is considered by authorizing officials in their risk-based authorization decisions. Organizations may choose to employ an *issue resolution process* to help determine the appropriate actions to take with regard to the security control weaknesses and deficiencies identified during the assessment. Issue resolution can help address vulnerabilities and associated risk, false positives, and other factors that may provide useful information to authorizing officials regarding the security state of the information system including the ongoing effectiveness of system-specific, hybrid, and common controls. The issue resolution process can also help to ensure that only substantive items are identified and transferred to the plan of actions and milestones.

References: NIST Special Publications 800-30, 800-53A.



3.5 RMF STEP 5 – AUTHORIZE INFORMATION SYSTEM

PLAN OF ACTION AND MILESTONES

TASK 5-1: Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.

Primary Responsibility: Information System Owner or Common Control Provider.

Supporting Roles: Information Owner/Steward; Information System Security Officer.

System Development Life Cycle Phase: Implementation.

Supplemental Guidance: The *plan of action and milestones*, prepared for the authorizing official by the information system owner or the common control provider, is one of three key documents in the security authorization package and describes the specific tasks that are planned: (i) to correct any weaknesses or deficiencies in the security controls noted during the assessment; and (ii) to address the residual vulnerabilities in the information system. The plan of action and milestones identifies: (i) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) the scheduled completion dates for the milestones. The plan of action and milestones is used by the authorizing official to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment. All security weaknesses and deficiencies identified during the security control assessment are documented in the security assessment report to maintain an effective audit trail. Organizations develop specific plans of action and milestones based on the results of the security control assessment and in accordance with applicable laws, Executive Orders, directives, policies, standards, guidance, or regulations. Plan of action and milestones entries are *not* required when weaknesses or deficiencies are remediated during the assessment or prior to the submission of the authorization package to the authorizing official.

Organizations define a strategy for developing plans of action and milestones that facilitates a prioritized approach to risk mitigation that is consistent across the organization. The strategy helps to ensure that organizational plans of action and milestones are based on: (i) the security categorization of the information system; (ii) the specific weaknesses or deficiencies in the security controls; (iii) the importance of the identified security control weaknesses or deficiencies (i.e., the direct or indirect effect the weaknesses or deficiencies may have on the overall security state of the information system, and hence on the risk exposure of the organization, or ability of the organization to perform its mission or business functions); and (iv) the organization's proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g., prioritization of risk mitigation actions, allocation of risk mitigation resources). A risk assessment guides the prioritization process for items included in the plan of action and milestones.

References: OMB Memorandum 02-01; NIST Special Publications 800-30, 800-53A.

SECURITY AUTHORIZATION PACKAGE

TASK 5-2: Assemble the security authorization package and submit the package to the authorizing official for adjudication.

Primary Responsibility: Information System Owner or Common Control Provider.

Supporting Roles: Information System Security Officer; Security Control Assessor.

System Development Life Cycle Phase: Implementation.

Supplemental Guidance: The *security authorization package* contains: (i) the security plan; (ii) the security assessment report; and (iii) the plan of action and milestones. The information in these key documents is used by authorizing officials to make risk-based authorization decisions. For information systems inheriting common controls for specific security capabilities, the security authorization package for the common controls or a reference to such documentation is also included in the authorization package. When security controls are provided to an organization by an external provider (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), the organization ensures that the information needed for authorizing officials to make risk-based decisions, is made available by the provider.

Additional information can be included in the security authorization package at the request of the authorizing official carrying out the authorization action. The contents of the security authorization package are protected appropriately in accordance with federal and organizational policies. Organizations are strongly encouraged to use automated support tools in preparing and managing the content of the security authorization package to help provide an effective vehicle

for maintaining and updating information for authorizing officials regarding the ongoing security status of information systems within the organization. Providing orderly, disciplined, and timely updates to the security plan, security assessment report, and plan of action and milestones on an ongoing basis, supports the concept of near real-time risk management and ongoing authorization. It also facilitates more cost-effective and meaningful reauthorization actions, if required. Organizations maintain strict version control as key documents in the authorization package are updated. With the use of automated tools and supporting databases, authorizing officials and other senior leaders within the organization are able to maintain awareness with regard to the security state of the information system including the ongoing effectiveness of system-specific, hybrid, and common controls.

References: None.

RISK DETERMINATION

TASK 5-3: Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.

Primary Responsibility: Authorizing Official or Designated Representative.

Supporting Roles: Risk Executive (Function); Senior Information Security Officer.

System Development Life Cycle Phase: Implementation.

Supplemental Guidance: The authorizing official or designated representative, in collaboration with the senior information security officer, assesses the information provided by the information system owner or common control provider regarding the current security state of the system or the common controls inherited by the system and the recommendations for addressing any residual risks. Risk assessments (either formal or informal) are employed at the discretion of the organization to provide needed information on threats, vulnerabilities, and potential impacts as well as the analyses for the risk mitigation recommendations. The risk executive (function) also provides information to the authorizing official that is considered in the final determination of risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the information system. Risk-related information includes the criticality of organizational missions and/or business functions supported by the information system and the risk management strategy for the organization. The risk management strategy typically describes: (i) how risk is assessed within the organization (i.e., tools, techniques, procedures, and methodologies); (ii) how assessed risks are evaluated with regard to severity or criticality; (iii) known existing aggregated risks from organizational information systems and other sources; (iv) risk mitigation approaches; (v) organizational risk tolerance; and (vi) how risk is monitored over time. When making the final risk determination, the authorizing official or designated representative considers information obtained from the risk executive (function) and the information provided by the information system owner or common control provider in the security authorization package (i.e., security plan, security assessment report, and plan of action and milestones). Conversely, information system-related security risk information derived from the execution of the RMF is available to the risk executive (function) for use in formulating and updating the organization-wide risk management strategy.

References: NIST Special Publications 800-30, 800-39.

RISK ACCEPTANCE

TASK 5-4: Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.

Primary Responsibility: Authorizing Official.

Supporting Roles: Risk Executive (Function); Authorizing Official Designated Representative; Senior Information Security Officer.

System Development Life Cycle Phase: Implementation.

Supplemental Guidance: The explicit acceptance of *risk* is the responsibility of the authorizing official and cannot be delegated to other officials within the organization. The authorizing official considers many factors when deciding if the risk to organizational operations (including mission, function, image, or reputation), organizational assets, individuals, other organizations, and the Nation, is acceptable. Balancing security considerations with mission and operational needs is paramount to achieving an acceptable authorization decision. The authorizing official issues an authorization decision for the information system and the common controls inherited by the system after reviewing all of the relevant information and, where appropriate, consulting with other organizational officials, including the organization's risk executive (function). Security authorization decisions are based on the content of the security authorization package and, where appropriate, any inputs received from key organizational officials, including the risk

executive (function). The authorization package provides relevant information on the security state of the information system including the ongoing effectiveness of the security controls employed within or inherited by the system. Inputs from the risk executive (function), including previously established overarching risk guidance to authorizing officials, provide additional organization-wide information to the authorizing official that may be relevant and affect the authorization decision (e.g., organizational risk tolerance, specific mission and business requirements, dependencies among information systems, and other types of risks not directly associated with the information system). Risk executive (function) inputs are documented and become part of the security authorization decision. Security authorization decisions, including inputs from the risk executive (function), are conveyed to information system owners and common control providers and made available to interested parties within the organization (e.g., information system owners and authorizing officials for interconnected systems, chief information officers, information owners/stewards, senior managers).

The *authorization decision document* conveys the final security authorization decision from the authorizing official to the information system owner or common control provider, and other organizational officials, as appropriate. The authorization decision document contains the following information: (i) authorization decision; (ii) terms and conditions for the authorization; and (iii) authorization termination date. The security *authorization decision* indicates to the information system owner whether the system is: (i) authorized to operate; or (ii) not authorized to operate. The *terms and conditions* for the authorization provide a description of any specific limitations or restrictions placed on the operation of the information system or inherited controls that must be followed by the system owner or common control provider. The *authorization termination date*, established by the authorizing official, indicates when the security authorization expires. Organizations may choose to eliminate the authorization termination date if the continuous monitoring program is sufficiently robust to provide the authorizing official with the needed information to conduct ongoing risk determination and risk acceptance activities with regard to the security state of the information system and the ongoing effectiveness of security controls employed within and inherited by the system.

Authorization termination dates are influenced by federal and/or organizational policies which may establish maximum authorization periods. For example, if the maximum authorization period for an information system is three years, then an organization establishes a continuous monitoring strategy for assessing a subset of the security controls employed within and inherited by the system during the authorization period. This strategy allows all security controls designated in the respective security plans to be assessed at least one time by the end of the three-year period. This also includes any common controls deployed external to organizational information systems. If the security control assessments are conducted by qualified assessors with the required degree of *independence* based on federal/organizational policies, appropriate security standards and guidelines, and the needs of the authorizing official, the assessment results can be cumulatively applied to the reauthorization, thus supporting the concept of ongoing authorization. Organizational policies regarding ongoing authorization and formal reauthorization, if/when required, are consistent with federal directives, regulations, and/or policies.

The authorization decision document is attached to the original security authorization package containing the supporting documentation and transmitted to the information system owner or common control provider. Upon receipt of the authorization decision document and original authorization package, the information system owner or common control provider acknowledges and implements the terms and conditions of the authorization and notifies the authorizing official. The organization ensures that authorization documents for both information systems and for common controls are made available to appropriate organizational officials (e.g., information system owners inheriting common controls, risk executive (function), chief information officers, senior information security officers, information system security officers). Authorization documents, especially information dealing with information system vulnerabilities, are: (i) marked and appropriately protected in accordance with federal and organizational policies; and (ii) retained in accordance with the organization's record retention policy. The authorizing official verifies, on an ongoing basis, that the terms and conditions established as part of the authorization are being followed by the information system owner or common control provider.

References: NIST Special Publication 800-39.

Milestone Checkpoint #5

- Did the organization develop a *plan of action and milestones* reflecting organizational priorities for addressing the remaining weaknesses and deficiencies in the information system and its environment of operation?
- Did the organization develop an appropriate *authorization package* with all key documents including the security plan, security assessment report, and plan of action and milestones (if applicable)?
- Did the final *risk determination* and *risk acceptance* by the authorizing official reflect the risk management strategy developed by the organization and conveyed by the risk executive (function)?
- Was the *authorization decision* conveyed to appropriate organizational personnel including information system owners and common control providers?

3.6 RMF STEP 6 – MONITOR SECURITY CONTROLS

INFORMATION SYSTEM AND ENVIRONMENT CHANGES

TASK 6-1: Determine the security impact of proposed or actual changes to the information system and its environment of operation.

Primary Responsibility: Information System Owner or Common Control Provider.

Supporting Roles: Risk Executive (Function); Authorizing Official or Designated Representative; Senior Information Security Officer; Information Owner/Steward; Information System Security Officer.

System Development Life Cycle Phase: Operation/Maintenance.

Supplemental Guidance: Information systems are in a constant state of change with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is an essential element of an effective security control monitoring program. Strict configuration management and control processes are established by the organization to support such monitoring activities. It is important to record any relevant information about specific changes to hardware, software, or firmware such as version or release numbers, descriptions of new or modified features/capabilities, and security implementation guidance. It is also important to record any changes to the environment of operation for the information system (e.g., modifications to hosting networks and facilities, mission/business use of the system, threats), or changes to the organizational risk management strategy. The information system owner and common control provider use this information in assessing the potential security impact of the changes. Documenting proposed or actual changes to an information system or its environment of operation and subsequently assessing the potential impact those changes may have on the security state of the system or the organization is an important aspect of security control monitoring and maintaining the security authorization over time. Information system changes are generally not undertaken prior to assessing the security impact of such changes. Organizations are encouraged to maximize the use of automation when managing changes to the information system or its environment of operation.

Security impact analysis conducted by the organization, determines the extent to which proposed or actual changes to the information system or its environment of operation can affect or have affected the security state of the system. Changes to the information system or its environment of operation may affect the security controls currently in place (including system-specific, hybrid, and common controls), produce new vulnerabilities in the system, or generate requirements for new security controls that were not needed previously. If the results of the security impact analysis indicate that the proposed or actual changes can affect or have affected the security state of the system, corrective actions are initiated and appropriate documents revised and updated (e.g., the security plan, security assessment report, and plan of action and milestones). The information system owner or common control provider consults with appropriate organizational officials/entities (e.g., configuration control board, senior information security officer, information system security officer) prior to implementing any security-related changes to the information system or its environment of operation. The authorizing official or designated representative uses the revised and updated security assessment report in collaboration with the senior information security officer and risk executive (function) to determine if a formal reauthorization action is necessary. Most routine changes to an information system or its environment of operation can be handled by the organization's continuous monitoring program, thus supporting the concept of ongoing authorization and near real-time risk management. Conducting security impact analyses is part of an ongoing assessment of risk. The authorizing official or designated representative, in collaboration with the risk executive (function), confirms as needed, determinations of residual risk. The risk executive (function) notifies the authorizing official of any significant changes in the organizational risk posture.

References: NIST Special Publications 800-30, 800-53A.

ONGOING SECURITY CONTROL ASSESSMENTS

TASK 6-2: Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.

Primary Responsibility: Security Control Assessor.

Supporting Roles: Authorizing Official or Designated Representative; Information System Owner or Common Control Provider; Information Owner/Steward; Information System Security Officer.

System Development Life Cycle Phase: Operation/Maintenance.

Supplemental Guidance: Organizations assess all security controls employed within and inherited by the information system during the initial security authorization. Subsequent to the initial authorization, the organization assesses a subset of the security controls (including management, operational, and technical controls) on an ongoing basis during continuous monitoring. The selection of appropriate security controls to monitor and the frequency of monitoring are based on the monitoring strategy developed by the information system owner or common control provider and approved by the authorizing official and senior information security officer. For ongoing security control assessments, assessors have the required degree of independence as determined by the authorizing official (see Appendix D.13 and Appendix F.4). Security control assessments in support of initial and subsequent security authorizations are conducted by independent assessors. Assessor independence during continuous monitoring, although not mandated, introduces efficiencies into the process and allows for reuse of assessment results when reauthorization is required. Organizations can use the current year's assessment results to meet the annual FISMA security control assessment requirement. To satisfy this requirement, organizations can draw upon the assessment results from any of the following sources, including but not limited to: (i) security control assessments conducted as part of an information system authorization, ongoing authorization, or formal reauthorization, if required; (ii) continuous monitoring activities; or (iii) testing and evaluation of the information system as part of the system development life cycle process or audit (provided that the testing, evaluation, or audit results are current, relevant to the determination of security control effectiveness, and obtained by assessors with the required degree of independence). Existing security assessment results are reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a cost-effective, fully integrated security program capable of producing the needed evidence to determine the security status of the information system. The use of automation to support security control assessments facilitates a greater frequency and volume of assessments that is consistent with the monitoring strategy established by the organization.

References: NIST Special Publication 800-53A.

ONGOING REMEDIATION ACTIONS

TASK 6-3: Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones.

Primary Responsibility: Information System Owner or Common Control Provider.

Supporting Roles: Authorizing Official or Designated Representative; Information Owner/Steward; Information System Security Officer; Information System Security Engineer; Security Control Assessor.

System Development Life Cycle Phase: Operation/Maintenance.

Supplemental Guidance: The assessment information produced by an assessor during continuous monitoring is provided to the information system owner and common control provider in an updated *security assessment report*. The information system owner and common control provider initiate remediation actions on outstanding items listed in the plan of actions and milestones and findings produced during the ongoing monitoring of security controls. The security control assessor may provide recommendations as to appropriate remediation actions. An assessment of risk (either formal or informal) informs organizational decisions with regard to conducting ongoing remediation actions. Security controls that are modified, enhanced, or added during the continuous monitoring process are reassessed by the assessor to ensure that appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate the identified risk.

References: NIST Special Publications 800-30, 800-53, 800-53A; CNSS Instruction 1253.

KEY UPDATES

TASK 6-4: Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.

Primary Responsibility: Information System Owner or Common Control Provider.

Supporting Roles: Information Owner/Steward; Information System Security Officer.

System Development Life Cycle Phase: Operation/Maintenance.

Supplemental Guidance: To facilitate the near real-time management of risk associated with the operation and use of the information system, the organization updates the security plan, security assessment report, and plan of action and milestones on an ongoing basis. The updated security plan reflects any modifications to security controls based on risk mitigation activities carried out by the information system owner or common control provider. The updated security assessment report reflects additional assessment activities carried out to determine security control effectiveness based

on modifications to the security plan and deployed controls. The updated plan of action and milestones: (i) reports progress made on the current outstanding items listed in the plan; (ii) addresses vulnerabilities discovered during the security impact analysis or security control monitoring; and (iii) describes how the information system owner or common control provider intends to address those vulnerabilities. The information provided by these key updates helps to raise awareness of the current security state of the information system (and the common controls inherited by the system) thereby supporting the process of ongoing authorization and near real-time risk management.

The frequency of updates to risk management-related information is at the discretion of the information system owner, common control provider, and authorizing officials in accordance with federal and organizational policies. Updates to information regarding the security state of the information system (and common controls inherited by the system) are accurate and timely since the information provided influences ongoing security-related actions and decisions by authorizing officials and other senior leaders within the organization. With the use of automated support tools and effective organization-wide security program management practices, authorizing officials are able to readily access the current security state of the information system including the ongoing effectiveness of system-specific, hybrid, and common controls. This facilitates near real-time management of risk to organizational operations and assets, individuals, other organizations, and the Nation, and provides essential information for continuous monitoring and ongoing authorization.

When updating key information in security plans, security assessment reports, and plans of action and milestones, organizations ensure that the original information needed for oversight, management, and auditing purposes is not modified or destroyed. Providing an effective method of tracking changes to information over time through strict configuration management and control procedures (including version control) is necessary to: (i) achieve transparency in the information security activities of the organization; (ii) obtain individual accountability for security-related actions; and (iii) better understand emerging trends in the organization's information security program.

References: NIST Special Publication 800-53A.

SECURITY STATUS REPORTING

TASK 6-5: Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.

Primary Responsibility: Information System Owner or Common Control Provider.

Supporting Roles: Information System Security Officer.

System Development Life Cycle Phase: Operation/Maintenance.

Supplemental Guidance: The results of monitoring activities are recorded and reported to the authorizing official on an ongoing basis in accordance with the monitoring strategy. Security status reporting can be: (i) event-driven (e.g., when the information system or its environment of operation changes or the system is compromised or breached); (ii) time-driven (e.g., weekly, monthly, quarterly); or (iii) both (event- and time-driven). Security status reports provide the authorizing official and other senior leaders within the organization, essential information with regard to the security state of the information system including the effectiveness of deployed security controls. Security status reports describe the ongoing monitoring activities employed by the information system owner or common control provider. Security status reports also address vulnerabilities in the information system and its environment of operation discovered during the security control assessment, security impact analysis, and security control monitoring and how the information system owner or common control provider intends to address those vulnerabilities. Organizations have significant latitude and flexibility in the breadth, depth, and formality of security status reports. Security status reports can take whatever form the organization deems most appropriate. The goal is cost-effective and efficient ongoing communication with senior leaders conveying the current security state of the information system and its environment of operation with regard to organizational missions and business functions. At a minimum, security status reports summarize key changes to security plans, security assessment reports, and plans of action and milestones. Use of automated management tools facilitates the effectiveness and timeliness of security status reporting. The frequency of security status reports is at the discretion of the organization and in accordance with federal and organizational policies. Status reports occur at appropriate intervals to transmit significant security-related information about the information system (including information regarding the ongoing effectiveness of security controls employed within and inherited by the system), but not so frequently as to generate unnecessary work. The authorizing official uses the security status reports in collaboration with the senior information security officer and risk executive (function) to determine if a formal reauthorization action is necessary. Security status reports are appropriately marked, protected, and handled in accordance with federal and organizational policies. At the discretion of the organization, security status reports can be used to help satisfy FISMA reporting requirements for documenting remedial actions for any security-related weaknesses or deficiencies. Note that this status reporting is intended to be ongoing, not to be interpreted as requiring

the time, expense, and formality associated with the information provided for the initial approval to operate. Rather, the reporting is conducted in the most cost-effective manner consistent with achieving the reporting objectives.

References: NIST Special Publication 800-53A.

ONGOING RISK DETERMINATION AND ACCEPTANCE

TASK 6-6: Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.

Primary Responsibility: Authorizing Official.

Supporting Roles: Risk Executive (Function); Authorizing Official Designated Representative; Senior Information Security Officer.

System Development Life Cycle Phase: Operation/Maintenance.

Supplemental Guidance: The authorizing official or designated representative reviews the reported security status of the information system (including the effectiveness of deployed security controls) on an ongoing basis, to determine the current risk to organizational operations and assets, individuals, other organizations, or the Nation. The authorizing official determines, with inputs as appropriate from the authorizing official designated representative, senior information security officer, and the risk executive (function), whether the current risk is acceptable and forwards appropriate direction to the information system owner or common control provider. The use of automated support tools to capture, organize, quantify, visually display, and maintain security status information promotes the concept of *near real-time risk management* regarding the overall risk posture of the organization. The use of metrics and dashboards increases an organization's ability to make risk-based decisions by consolidating data from automated tools and providing it to decision makers at different levels within the organization in an easy-to-understand format. The risks being incurred may change over time based on the information provided in the security status reports. Determining how the changing conditions affect the mission or business risks associated with the information system is essential for maintaining *adequate security*. By carrying out ongoing *risk determination* and *risk acceptance*, authorizing officials can maintain the security authorization over time. Formal reauthorization actions, if required, occur only in accordance with federal or organizational policies. The authorizing official conveys updated risk determination and acceptance results to the risk executive (function).

References: NIST Special Publications 800-30, 800-39.

INFORMATION SYSTEM REMOVAL AND DECOMMISSIONING

TASK 6-7: Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.

Primary Responsibility: Information System Owner.

Supporting Roles: Risk Executive (Function); Authorizing Official Designated Representative; Senior Information Security Officer; Information Owner/Steward; Information System Security Officer.

System Development Life Cycle Phase: Disposal.

Supplemental Guidance: When a federal information system is removed from operation, a number of risk management-related actions are required. Organizations ensure that all security controls addressing information system removal and decommissioning (e.g., media sanitization, configuration management and control) are implemented. Organizational tracking and management systems (including inventory systems) are updated to indicate the specific information system components that are being removed from service. Security status reports reflect the new status of the information system. Users and application owners hosted on the decommissioned information system are notified as appropriate, and any security control inheritance relationships are reviewed and assessed for impact. This task also applies to subsystems that are removed from information systems or decommissioned. The effects of the subsystem removal or decommissioning are assessed with respect to the overall operation of the information system where the subsystem resided, or in the case of dynamic subsystems, the information systems where the subsystems were actively employed.

References: NIST Special Publications 800-30, 800-53A.

Milestone Checkpoint #6

- Is the organization effectively monitoring changes to the *information system* and its *environment of operation* including the effectiveness of deployed *security controls* in accordance with the continuous monitoring strategy?
- Is the organization effectively analyzing the *security impacts* of identified changes to the information system and its environment of operation?
- Is the organization conducting *ongoing assessments of security controls* in accordance with the monitoring strategy?
- Is the organization taking the necessary *remediation actions* on an ongoing basis to address identified weaknesses and deficiencies in the information system and its environment of operation?
- Does the organization have an effective process in place to report the *security status* of the information system and its environment of operation to the authorizing officials and other designated senior leaders within the organization on an ongoing basis?
- Is the organization updating critical *risk management documents* based on ongoing monitoring activities?
- Are authorizing officials conducting *ongoing security authorizations* by employing effective continuous monitoring activities and communicating updated risk determination and acceptance decisions to information system owners and common control providers?

APPENDIX A

REFERENCES

LAWS, POLICIES, DIRECTIVES, INSTRUCTIONS, STANDARDS, AND GUIDELINES

LEGISLATION

1. E-Government Act [includes FISMA] (P.L. 107-347), December 2002.
2. Federal Information Security Management Act (P.L. 107-347, Title III), December 2002.
3. Paperwork Reduction Act (P.L. 104-13), May 1995.

POLICIES, DIRECTIVES, INSTRUCTIONS

1. Committee on National Security Systems (CNSS) Instruction 4009, *National Information Assurance Glossary*, June 2006.
2. Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, October 2009.
3. Office of Management and Budget, Circular A-130, Appendix III, Transmittal Memorandum #4, *Management of Federal Information Resources*, November 2000.
4. Office of Management and Budget Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001.

STANDARDS

1. National Institute of Standards and Technology Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
2. National Institute of Standards and Technology Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006.

GUIDELINES

1. National Institute of Standards and Technology Special Publication 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.
2. National Institute of Standards and Technology Special Publication 800-27, Revision A, *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, June 2004.
3. National Institute of Standards and Technology Special Publication 800-30, *Risk Management Guide for Information Technology Systems*, July 2002.
4. National Institute of Standards and Technology Special Publication 800-39 (Second Public Draft), *Managing Risk from Information Systems: An Organizational Perspective*, April 2008.
5. National Institute of Standards and Technology Special Publication 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009.

6. National Institute of Standards and Technology Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans*, July 2008.

7. National Institute of Standards and Technology Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System*, August 2003.

8. National Institute of Standards and Technology Special Publication 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008.

9. National Institute of Standards and Technology Special Publication 800-70, Revision 1, *National Checklist Program for IT Products--Guidelines for Checklist Users and Developers*, September 2009.

APPENDIX B

GLOSSARY

COMMON TERMS AND DEFINITIONS

Appendix B provides definitions for security terminology used within Special Publication 800-37. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Adequate Security [OMB Circular A-130, Appendix III]	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.
Agency	See *Executive Agency*.
Allocation	The process an organization employs to determine whether security controls are defined as system-specific, hybrid, or common. The process an organization employs to assign security controls to specific information system components responsible for providing a particular security capability (e.g., router, server, remote sensor).
Application	A software program hosted by an information system.
Assessment	See *Security Control Assessment*.
Assessor	See *Security Control Assessor*.
Assurance	The grounds for confidence that the set of intended security controls in an information system are effective in their application.
Authorization (to operate)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
Authorize Processing	See *Authorization*.

Authorizing Official	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Authorizing Official Designated Representative	An organizational official acting on behalf of an authorizing official in carrying out and coordinating the required activities associated with security authorization.
Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Chief Information Officer [PL 104-106, Sec. 5125(b)]	Agency official responsible for: (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. Note: Organizations subordinate to federal agencies may use the term *Chief Information Officer* to denote individuals filling positions with similar security responsibilities to agency-level Chief Information Officers.
Chief Information Security Officer	See *Senior Agency Information Security Officer*.
Common Control	A security control that is inherited by one or more organizational information systems. See *Security Control Inheritance*.
Common Control Provider	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).
Compensating Security Controls	The management, operational, and technical controls (i.e., safeguards or countermeasures) employed by an organization in lieu of the recommended controls in the low, moderate, or high baselines described in NIST Special Publication 800-53, that provide equivalent or comparable protection for an information system.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control [CNSSI 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Controlled Interface	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.
Countermeasures [CNSSI 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Cross Domain Solution	A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.
Domain [CNSSI 4009]	An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See *Security Domain.*
Dynamic Subsystem	A subsystem that is not continually present during the execution phase of an information system. Service-oriented architectures and cloud computing architectures are examples of architectures that employ dynamic subsystems.
Environment of Operation	The physical surroundings in which an information system processes, stores, and transmits information.
Executive Agency [41 U.S.C., Sec. 403]	An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.
External Information System (or Component)	An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service	An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.
External Information System Service Provider	A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain arrangements.

Federal Agency	See *Executive Agency*.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
High-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of high.
Hybrid Security Control	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See *Common Control* and *System-Specific Security Control*.
Information [FIPS 199]	An instance of an information type.
Information Owner [CNSSI 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Architect	Individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes.
Information Security Policy [CNSSI 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information Security Program Plan	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.

Information Steward	Individual or group that helps to ensure the careful and responsible management of federal information belonging to the Nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security-related federal policies, directives, regulations, standards, and guidance.
Information System [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Information System Boundary	See *Authorization Boundary*.
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Security Engineer	Individual assigned responsibility for conducting information system security engineering activities.
Information System Security Engineering	Process that captures and refines information security requirements and ensures their integration into information technology component products and information systems through purposeful security design or configuration.
Information System-related Security Risks	Information system-related security risks are those risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and consider impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See *Risk*.
Information System Security Officer [CNSSI 4009]	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.

Information Technology [40 U.S.C., Sec. 1401]	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Type [FIPS 199]	A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Joint Authorization	Security authorization involving multiple authorizing officials.
Low-Impact System [FIPS 200]	An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact value of low.
Management Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that focus on the management of risk and the management of information system security.
Moderate-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.

National Security System [44 U.S.C., Sec. 3542]	Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Net-centric Architecture	A complex system of systems composed of subsystems and services that are part of a continuously evolving, complex community of people, devices, information and services interconnected by a network that enhances information sharing and collaboration. Subsystems and services may or may not be developed or owned by the same entity, and, in general, will not be continually present during the full life cycle of the system of systems. Examples of this architecture include service-oriented architectures and cloud computing architectures.
Operational Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by people (as opposed to systems).
Organization [FIPS 200, Adapted]	An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).
Plan of Action and Milestones [OMB Memorandum 02-01]	A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a *limited* adverse effect (FIPS 199 low); (ii) a *serious* adverse effect (FIPS 199 moderate); or (iii) a *severe* or *catastrophic* adverse effect (FIPS 199 high) on organizational operations, organizational assets, or individuals.
Reciprocity	Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.

Risk [FIPS 200, Adapted]	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security.]
Risk Assessment	The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk Executive (Function)	An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.
Risk Management [FIPS 200, Adapted]	The process of managing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
Safeguards [CNSSI 4009]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Security Authorization	See *Authorization.*
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS 199 for other than national security systems.

Security Controls [FIPS 199]	The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.
Security Control Assessment	The testing and/or evaluation of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment.
Security Control Inheritance	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See *Common Control*.
Security Domain [CNSSI 4009]	A domain that implements a security policy and is administered by a single authority.
Security Impact Analysis	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See *System Security Plan* or *Information Security Program Plan*.
Security Policy [CNSSI 4009]	A set of criteria for the provision of security services.
Security Requirements [FIPS 200]	Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Senior (Agency) Information Security Officer [44 U.S.C., Sec. 3544]	Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers. Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.
Senior Information Security Officer	See *Senior Agency Information Security Officer*.
Subsystem	A major subdivision of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
System	See *Information System*.
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
System-Specific Security Control	A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to the security control baseline. See *Tailoring*.
Tailoring	The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.
Technical Controls [FIPS 200]	The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.
Threat [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Vulnerability [CNSSI 4009]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment [CNSSI 4009]	Formal description and evaluation of the vulnerabilities in an information system.

APPENDIX C

ACRONYMS

COMMON ABBREVIATIONS

CIO	Chief Information Officer
CNSS	Committee on National Security Systems
DoD	Department of Defense
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
NIST	National Institute of Standards and Technology
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
RMF	Risk Management Framework

APPENDIX D

ROLES AND RESPONSIBILITIES

KEY PARTICIPANTS IN THE RISK MANAGEMENT PROCESS

The following sections describe the roles and responsibilities of key participants involved in an organization's risk management process.[47] Recognizing that organizations have widely varying missions and organizational structures, there may be differences in naming conventions for risk management-related roles and how specific responsibilities are allocated among organizational personnel (e.g., multiple individuals filling a single role or one individual filling multiple roles).[48] However, the basic functions remain the same. The application of the Risk Management Framework described in this publication is flexible, allowing organizations to effectively accomplish the intent of the specific tasks within their respective organizational structures to best manage information system-related security risks. Many risk management roles defined in this publication have counterpart roles defined in the routine system development life cycle processes carried out by organizations. Whenever possible, organizations align the risk management roles with similar (or complementary) roles defined for the system development life cycle.[49]

D.1 HEAD OF AGENCY (CHIEF EXECUTIVE OFFICER)

The *head of agency* (or chief executive officer) is the highest-level senior official or executive within an organization with the overall responsibility to provide information security protections commensurate with the risk and magnitude of harm (i.e., impact) to organizational operations and assets, individuals, other organizations, and the Nation resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of: (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. Agency heads are also responsible for ensuring that: (i) information security management processes are integrated with strategic and operational planning processes; (ii) senior officials within the organization provide information security for the information and information systems that support the operations and assets under their control; and (iii) the organization has trained personnel sufficient to assist in complying with the information security requirements in related legislation, policies, directives, instructions, standards, and guidelines. Through the development and implementation of strong policies, the head of agency establishes the organizational commitment to information security and the actions required to effectively manage risk and protect the core missions and business functions being carried out by the organization. The head of agency establishes appropriate accountability for information security and provides active support and oversight of monitoring and improvement for the information security program. Senior leadership commitment to information security establishes a level of due diligence within the organization that promotes a climate for mission and business success.

---

[47] Organizations may define other roles (e.g., facilities manager, human resources manager, systems administrator) to support the risk management process.

[48] Caution is exercised when one individual fills multiples roles in the risk management process to ensure that the individual retains an appropriate level of independence and remains free from conflicts of interest.

[49] For example, the system development life cycle role of *system developer* or *program manager* can be aligned with *information system owner*; mission *owner/manager* can be aligned with *authorizing official*; and *system/software engineers* are complementary roles to *information system security engineers*.

D.2 RISK EXECUTIVE (FUNCTION)

The risk executive (function) is an individual or group within an organization that helps to ensure that: (i) risk-related considerations for individual information systems, to include authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success. The risk executive (function) coordinates with the senior leadership of an organization to:

- Provide a comprehensive, organization-wide, holistic approach for addressing risk—an approach that provides a greater understanding of the integrated operations of the organization;
- Develop a risk management strategy for the organization providing a strategic view of information security-related risks with regard to the organization as a whole;[50]
- Facilitate the sharing of risk-related information among authorizing officials and other senior leaders within the organization;
- Provide oversight for all risk management-related activities across the organization (e.g., security categorizations) to help ensure consistent and effective risk acceptance decisions;
- Ensure that authorization decisions consider all factors necessary for mission and business success;
- Provide an organization-wide forum to consider all sources of risk (including aggregated risk) to organizational operations and assets, individuals, other organizations, and the Nation;
- Promote cooperation and collaboration among authorizing officials to include authorization actions requiring shared responsibility;
- Ensure that the shared responsibility for supporting organizational mission/business functions using external providers of information and services receives the needed visibility and is elevated to the appropriate decision-making authorities; and
- Identify the organizational risk posture based on the aggregated risk to information from the operation and use of the information systems for which the organization is responsible.

The risk executive (function) presumes neither a specific organizational structure nor formal responsibility assigned to any one individual or group within the organization. The head of the agency/organization may choose to retain the risk executive (function) or to delegate the function to another official or group (e.g., an executive leadership council). The risk executive (function) has inherent U.S. Government authority and is assigned to government personnel only.

D.3 CHIEF INFORMATION OFFICER

The *chief information officer*[51] is an organizational official responsible for: (i) designating a senior information security officer; (ii) developing and maintaining information security policies,

[50] Authorizing officials may have narrow or localized perspectives in rendering authorization decisions, in some cases without fully understanding or explicitly accepting the risks being incurred from such decisions.

[51] When an organization has not designated a formal chief information officer position, FISMA requires the associated responsibilities to be handled by a comparable organizational official.

procedures, and control techniques to address all applicable requirements; (iii) overseeing personnel with significant responsibilities for information security and ensuring that the personnel are adequately trained; (iv) assisting senior organizational officials concerning their security responsibilities; and (v) in coordination with other senior officials, reporting annually to the head of the federal agency on the overall effectiveness of the organization's information security program, including progress of remedial actions. The chief information officer, with the support of the risk executive (function) and the senior information security officer, works closely with authorizing officials and their designated representatives to help ensure that:

- An organization-wide information security program is effectively implemented resulting in adequate security for all organizational information systems and environments of operation for those systems;
- Information security considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, and acquisition/system development life cycles;
- Information systems are covered by approved security plans and are authorized to operate;
- Information security-related activities required across the organization are accomplished in an efficient, cost-effective, and timely manner; and
- There is centralized reporting of appropriate information security-related activities.

The chief information officer and authorizing officials also determine, based on organizational priorities, the appropriate allocation of resources dedicated to the protection of the information systems supporting the organization's missions and business functions. For selected information systems, the chief information officer may be designated as an authorizing official or a co-authorizing official with other senior organizational officials. The role of chief information officer has inherent U.S. Government authority and is assigned to government personnel only.

D.4 INFORMATION OWNER/STEWARD

The *information owner/steward* is an organizational official with statutory, management, or operational authority for specified information and the responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal.[52] In information-sharing environments, the information owner/steward is responsible for establishing the rules for appropriate use and protection of the subject information (e.g., rules of behavior) and retains that responsibility even when the information is shared with or provided to other organizations. The owner/steward of the information processed, stored, or transmitted by an information system may or may not be the same as the system owner. A single information system may contain information from multiple information owners/stewards. Information owners/stewards provide input to information system owners regarding the security requirements and security controls for the systems where the information is processed, stored, or transmitted.

[52] Federal information is an asset of the Nation, not of a particular federal agency or its subordinate organizations. In that spirit, many federal agencies are developing policies, procedures, processes, and training needed to end the practice of *information ownership* and implement the practice of *information stewardship*. Information stewardship is the careful and responsible management of federal information belonging to the Nation as a whole, regardless of the entity or source that may have originated, created, or compiled the information. Information stewards provide maximum access to federal information to elements of the federal government and its customers, balanced by the obligation to protect the information in accordance with the provisions of FISMA and any associated security-related federal policies, directives, regulations, standards, and guidance.

D.5 SENIOR INFORMATION SECURITY OFFICER

The *senior information security officer* is an organizational official responsible for: (i) carrying out the chief information officer security responsibilities under FISMA; and (ii) serving as the primary liaison for the chief information officer to the organization's authorizing officials, information system owners, common control providers, and information system security officers. The senior information security officer: (i) possesses professional qualifications, including training and experience, required to administer the information security program functions; (ii) maintains information security duties as a primary responsibility; and (iii) heads an office with the mission and resources to assist the organization in achieving more secure information and information systems in accordance with the requirements in FISMA. The senior information security officer (or supporting staff members) may also serve as authorizing official designated representatives or security control assessors. The role of senior information security officer has inherent U.S. Government authority and is assigned to government personnel only.

D.6 AUTHORIZING OFFICIAL

The *authorizing official* is a senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations and assets, individuals, other organizations, and the Nation.[53] Authorizing officials typically have budgetary oversight for an information system *or* are responsible for the mission and/or business operations supported by the system. Through the security authorization process, authorizing officials are *accountable* for the security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Authorizing officials also approve security plans, memorandums of agreement or understanding, and plans of action and milestones and determine whether significant changes in the information systems or environments of operation require reauthorization. Authorizing officials can deny authorization to operate an information system or if the system is operational, halt operations, if unacceptable risks exist. Authorizing officials coordinate their activities with the risk executive (function), chief information officer, senior information security officer, common control providers, information system owners, information system security officers, security control assessors, and other interested parties during the security authorization process. With the increasing complexity of missions/business processes, partnership arrangements, and the use of external/shared services, it is possible that a particular information system may involve multiple authorizing officials. If so, agreements are established among the authorizing officials and documented in the security plan. Authorizing officials are responsible for ensuring that all activities and functions associated with security authorization that are delegated to authorizing official designated representatives are carried out. The role of authorizing official has inherent U.S. Government authority and is assigned to government personnel only.

D.7 AUTHORIZING OFFICIAL DESIGNATED REPRESENTATIVE

The *authorizing official designated representative* is an organizational official that acts on behalf of an authorizing official to coordinate and conduct the required day-to-day activities associated with the security authorization process. Authorizing official designated representatives can be empowered by authorizing officials to make certain decisions with regard to the planning and resourcing of the security authorization process, approval of the security plan, approval and monitoring the implementation of plans of action and milestones, and the assessment and/or

[53] The responsibility of authorizing officials described in FIPS 200, was extended in NIST Special Publication 800-53 to include risks to other organizations and the Nation.

determination of risk. The designated representative may also be called upon to prepare the final authorization package, obtain the authorizing official's signature on the authorization decision document, and transmit the authorization package to appropriate organizational officials. The only activity that cannot be delegated to the designated representative by the authorizing official is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation).

D.8 COMMON CONTROL PROVIDER

The *common control provider* is an individual, group, or organization responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems).[54] Common control providers are responsible for: (i) documenting the organization-identified common controls in a *security plan* (or equivalent document prescribed by the organization); (ii) ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence defined by the organization; (iii) documenting assessment findings in a *security assessment report*; and (iv) producing a *plan of action and milestones* for all controls having weaknesses or deficiencies. Security plans, security assessment reports, and plans of action and milestones for common controls (or a summary of such information) is made available to information system owners *inheriting* those controls after the information is reviewed and approved by the senior official or executive with oversight responsibility for those controls.

D.9 INFORMATION SYSTEM OWNER

The *information system owner* is an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system.[55] The information system owner is responsible for addressing the operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements) and for ensuring compliance with information security requirements. In coordination with the information system security officer, the information system owner is responsible for the development and maintenance of the security plan and ensures that the system is deployed and operated in accordance with the agreed-upon security controls. In coordination with the information owner/steward, the information system owner is also responsible for deciding who has access to the system (and with what types of privileges or access rights)[56] and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior). Based on guidance from the authorizing official, the information system owner informs appropriate organizational officials of the need to conduct the security authorization, ensures that the necessary resources are available for the effort, and provides the required information system access, information, and documentation to the security

---

[54] Organizations can have multiple common control providers depending on how information security responsibilities are allocated organization-wide. Common control providers may also be *information system owners* when the common controls are resident within an information system. Common controls are described in Section 2.4.

[55] The *information system owner* serves as the focal point for the information system. In that capacity, the information system owner serves both as an owner and as the central point of contact between the authorization process and the owners of components of the system including, for example: (i) applications, networking, servers, or workstations; (ii) owners/stewards of information processed, stored, or transmitted by the system; and (iii) owners of the missions and business functions supported by the system. Some organizations may refer to information system owners as program managers or business/asset owners.

[56] The responsibility for deciding who has access to specific information within an information system (and with what types of privileges or access rights) may reside with the information owner/steward.

control assessor. The information system owner receives the security assessment results from the security control assessor. After taking appropriate steps to reduce or eliminate vulnerabilities, the information system owner assembles the authorization package and submits the package to the authorizing official or the authorizing official designated representative for adjudication.[57]

D.10 INFORMATION SYSTEM SECURITY OFFICER

The *information system security officer*[58] is an individual responsible for ensuring that the appropriate operational security posture is maintained for an information system and as such, works in close collaboration with the information system owner. The information system security officer also serves as a principal advisor on all matters, technical and otherwise, involving the security of an information system. The information system security officer has the detailed knowledge and expertise required to manage the security aspects of an information system and, in many organizations, is assigned responsibility for the day-to-day security operations of a system. This responsibility may also include, but is not limited to, physical and environmental protection, personnel security, incident handling, and security training and awareness. The information system security officer may be called upon to assist in the development of the security policies and procedures and to ensure compliance with those policies and procedures. In close coordination with the information system owner, the information system security officer often plays an active role in the monitoring of a system and its environment of operation to include developing and updating the security plan, managing and controlling changes to the system, and assessing the security impact of those changes.

D.11 INFORMATION SECURITY ARCHITECT

The *information security architect* is an individual, group, or organization responsible for ensuring that the information security requirements necessary to protect the organization's core missions and business processes are adequately addressed in all aspects of enterprise architecture including reference models, segment and solution architectures, and the resulting information systems supporting those missions and business processes. The information security architect serves as the liaison between the enterprise architect and the information system security engineer and also coordinates with information system owners, common control providers, and information system security officers on the allocation of security controls as system-specific, hybrid, or common controls. In addition, information security architects, in close coordination with information system security officers, advise authorizing officials, chief information officers, senior information security officers, and the risk executive (function), on a range of security-related issues including, for example, establishing information system boundaries, assessing the severity of weaknesses and deficiencies in the information system, plans of action and milestones, risk mitigation approaches, security alerts, and potential adverse effects of identified vulnerabilities.

---

[57] Depending on how the organization has organized its security authorization activities, the authorizing official may choose to designate an individual other than the information system owner to compile and assemble the information for the security authorization package. In this situation, the designated individual must coordinate the compilation and assembly activities with the information system owner.

[58] Organizations may also define an *information system security manager* or *information security manager* role with similar responsibilities as an information system security officer or with oversight responsibilities for an information security program. In these situations, information system security officers may, at the discretion of the organization, report directly to information system security managers or information security managers.

D.12 INFORMATION SYSTEM SECURITY ENGINEER

The *information system security engineer* is an individual, group, or organization responsible for conducting information system security engineering activities. Information system security engineering is a process that captures and refines information security requirements and ensures that the requirements are effectively integrated into information technology component products and information systems through purposeful security architecting, design, development, and configuration. Information system security engineers are an integral part of the development team (e.g., integrated project team) designing and developing organizational information systems or upgrading legacy systems. Information system security engineers employ best practices when implementing security controls within an information system including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques. System security engineers coordinate their security-related activities with information security architects, senior information security officers, information system owners, common control providers, and information system security officers.

D.13 SECURITY CONTROL ASSESSOR

The *security control assessor*[59] is an individual, group, or organization responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system). Security control assessors also provide an assessment of the severity of weaknesses or deficiencies discovered in the information system and its environment of operation and recommend corrective actions to address identified vulnerabilities. In addition to the above responsibilities, security control assessors prepare the final security assessment report containing the results and findings from the assessment. Prior to initiating the security control assessment, an assessor conducts an assessment of the security plan to help ensure that the plan provides a set of security controls for the information system that meet the stated security requirements.

The required level of assessor independence is determined by the specific conditions of the security control assessment. For example, when the assessment is conducted in support of an authorization decision or ongoing authorization, the authorizing official makes an explicit determination of the degree of independence required in accordance with federal policies, directives, standards, and guidelines. Assessor independence is an important factor in: (i) preserving the impartial and unbiased nature of the assessment process; (ii) determining the credibility of the security assessment results; and (iii) ensuring that the authorizing official receives the most objective information possible in order to make an informed, risk-based, authorization decision. The information system owner and common control provider rely on the security expertise and the technical judgment of the assessor to: (i) assess the security controls employed within and inherited by the information system using assessment procedures specified in the security assessment plan; and (ii) provide specific recommendations on how to correct weaknesses or deficiencies in the controls and address identified vulnerabilities.

---

[59] Security control assessors may be called *certification agents* in some organizations. At the discretion of the organization, security control assessors may be given additional duties/responsibilities for the post processing and analysis of security control assessment findings and results. This may include, for example, making specific determinations for or recommendations to authorizing officials (known in some communities of interest as *certification recommendations* or *certification determinations*).

APPENDIX E

SUMMARY OF RMF TASKS

LISTING OF PRIMARY RESPONSIBILITIES AND SUPPORTING ROLES

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
RMF Step 1: Categorize Information System		
TASK 1-1 **Security Categorization** Categorize the information system and document the results of the security categorization in the security plan.	Information System Owner Information Owner/Steward	Risk Executive (Function) Authorizing Official *or* Designated Representative Chief Information Officer Senior Information Security Officer Information System Security Officer
TASK 1-2 **Information System Description** Describe the information system (including system boundary) and document the description in the security plan.	Information System Owner	Authorizing Official *or* Designated Representative Senior Information Security Officer Information Owner/Steward Information System Security Officer
TASK 1-3 **Information System Registration** Register the information system with appropriate organizational program/management offices.	Information System Owner	Information System Security Officer
RMF Step 2: Select Security Controls		
TASK 2-1 **Common Control Identification** Identify the security controls that are provided by the organization as common controls for organizational information systems and document the controls in a security plan (or equivalent document).	Chief Information Officer *or* Senior Information Security Officer Information Security Architect Common Control Provider	Risk Executive (Function) Authorizing Official *or* Designated Representative Information System Owner Information System Security Engineer
TASK 2-2 **Security Control Selection** Select the security controls for the information system and document the controls in the security plan.	Information Security Architect Information System Owner	Authorizing Official *or* Designated Representative Information Owner/Steward Information System Security Officer Information System Security Engineer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 2-3 **Monitoring Strategy** Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes to the information system and its environment of operation.	Information System Owner *or* Common Control Provider	Risk Executive (Function) Authorizing Official *or* Designated Representative Chief Information Officer Senior Information Security Officer Information Owner/Steward Information System Security Officer
TASK 2-4 **Security Plan Approval** Review and approve the security plan.	Authorizing Official *or* Designated Representative	Risk Executive (Function) Chief Information Officer Senior Information Security Officer
RMF Step 3: Implement Security Controls		
TASK 3-1 **Security Control Implementation** Implement the security controls specified in the security plan.	Information System Owner *or* Common Control Provider	Information Owner/Steward Information System Security Officer Information System Security Engineer
TASK 3-2 **Security Control Documentation** Document the security control implementation, as appropriate, in the security plan, providing a functional description of the control implementation (including planned inputs, expected behavior, and expected outputs).	Information System Owner *or* Common Control Provider	Information Owner/Steward Information System Security Officer Information System Security Engineer
RMF Step 4: Assess Security Controls		
TASK 4-1 **Assessment Preparation** Develop, review, and approve a plan to assess the security controls.	Security Control Assessor	Authorizing Official *or* Designated Representative Chief Information Officer Senior Information Security Officer Information System Owner *or* Common Control Provider Information Owner/Steward Information System Security Officer
TASK 4-2 **Security Control Assessment** Assess the security controls in accordance with the assessment procedures defined in the security assessment plan.	Security Control Assessor	Information System Owner *or* Common Control Provider Information Owner/Steward Information System Security Officer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 4-3 **Security Assessment Report** Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment.	Security Control Assessor	Information System Owner *or* Common Control Provider Information System Security Officer
TASK 4-4 **Remediation Actions** Conduct initial remediation actions on security controls based on the findings and recommendations of the security assessment report and reassess remediated control(s), as appropriate.	Information System Owner *or* Common Control Provider Security Control Assessor	Authorizing Official or Designated Representative Chief Information Officer Senior Information Security Officer Information Owner/Steward Information System Security Officer Information System Security Engineer
RMF Step 5: Authorize Information System		
TASK 5-1 **Plan of Action and Milestones** Prepare the plan of action and milestones based on the findings and recommendations of the security assessment report excluding any remediation actions taken.	Information System Owner *or* Common Control Provider	Information Owner/Steward Information System Security Officer
TASK 5-2 **Security Authorization Package** Assemble the security authorization package and submit the package to the authorizing official for adjudication.	Information System Owner *or* Common Control Provider	Information System Security Officer Security Control Assessor
TASK 5-3 **Risk Determination** Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.	Authorizing Official *or* Designated Representative	Risk Executive (Function) Senior Information Security Officer
TASK 5-4 **Risk Acceptance** Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable.	Authorizing Official	Risk Executive (Function) Authorizing Official Designated Representative Senior Information Security Officer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
Monitor Security Controls		
TASK 6-1 **Information System and Environment Changes** Determine the security impact of proposed or actual changes to the information system and its environment of operation.	Information System Owner *or* Common Control Provider	Risk Executive (Function) Authorizing Official *or* Designated Representative Senior Information Security Officer Information Owner/Steward Information System Security Officer
TASK 6-2 **Ongoing Security Control Assessments** Assess a selected subset of the technical, management, and operational security controls employed within and inherited by the information system in accordance with the organization-defined monitoring strategy.	Security Control Assessor	Authorizing Official *or* Designated Representative Information System Owner *or* Common Control Provider Information Owner/Steward Information System Security Officer
TASK 6-3 **Ongoing Remediation Actions** Conduct remediation actions based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in the plan of action and milestones.	Information System Owner *or* Common Control Provider	Authorizing Official *or* Designated Representative Information Owner/Steward Information System Security Officer Information System Security Engineer Security Control Assessor
TASK 6-4 **Key Updates** Update the security plan, security assessment report, and plan of action and milestones based on the results of the continuous monitoring process.	Information System Owner *or* Common Control Provider	Information Owner/Steward Information System Security Officer
TASK 6-5 **Security Status Reporting** Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the authorizing official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy.	Information System Owner *or* Common Control Provider	Information System Security Officer

RMF TASKS	PRIMARY RESPONSIBILITY	SUPPORTING ROLES
TASK 6-6 **Ongoing Risk Determination and Acceptance** Review the reported security status of the information system (including the effectiveness of security controls employed within and inherited by the system) on an ongoing basis in accordance with the monitoring strategy to determine whether the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation remains acceptable.	Authorizing Official	Risk Executive (Function) Authorizing Official Designated Representative Senior Information Security Officer
TASK 6-7 **Information System Removal and Decommissioning** Implement an information system decommissioning strategy, when needed, which executes required actions when a system is removed from service.	Information System Owner	Risk Executive (Function) Authorizing Official Designated Representative Senior Information Security Officer Information Owner/Steward Information System Security Officer

APPENDIX F

SECURITY AUTHORIZATION

AUTHORIZATION DECISIONS AND SUPPORTING EVIDENCE

This appendix provides information on the security authorization process to include: (i) the content of the authorization package; (ii) types of authorization decisions; (iii) the content of the authorization decision document; and (iv) maintenance of authorizations through continuous monitoring processes and conditions for reauthorization.

F.1 AUTHORIZATION PACKAGE

The security *authorization package* documents the results of the security control assessment and provides the authorizing official with essential information needed to make a risk-based decision on whether to authorize operation of an information system or a designated set of common controls. Unless specifically designated otherwise by the chief information officer or authorizing official, the information system owner or common control provider is responsible for the assembly, compilation, and submission of the authorization package. The information system owner or common control provider receives inputs from the information system security officer, security control assessor, senior information security officer, and risk executive (function) during the preparation of the authorization package. The authorization package[60] contains the following documents:

- Security plan;
- Security assessment report; and
- Plan of action and milestones.

The *security plan*, prepared by the information system owner or common control provider, provides an overview of the security requirements and describes the security controls in place or planned for meeting those requirements. The plan provides sufficient information to understand the intended or actual implementation of each security control employed within or inherited by the information system.[61] The security plan also contains as supporting appendices or as references to appropriate sources, other risk and security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, incident response plan, and continuous monitoring strategy. In accordance with the *near real-time* risk management objectives of the security authorization process, the security plan is updated whenever events dictate changes to the security controls employed within or inherited by the information system. Updates to the security plan may be triggered by a variety of events, including for example: (i) a vulnerability scan of the information system or vulnerability assessment of the environment of operation; (ii) new threat information; (iii) weaknesses or deficiencies discovered in currently deployed security controls

[60] The authorizing official determines what additional supporting documentation or references may be required to be included in the security authorization package. Appropriate measures are employed to protect information contained in security authorization packages in accordance with federal and organizational policy.

[61] The *security plan* is a conceptual body of information which may be accounted for within one or more repositories and include documents (electronic or hard copy) that come from a variety of sources produced throughout the system development life cycle. For example, information system owners inheriting common controls can either document the implementation of the controls in their respective security plans or reference the controls contained in the security plans of common control providers.

after an information system breach; (iv) a redefinition of mission priorities or business objectives invalidating the results of the previous security categorization process; and (v) a change in the information system (e.g., adding new hardware, software, or firmware; establishing new connections) or its environment of operation (e.g., moving to a new facility).

The *security assessment report*, prepared by the security control assessor, provides the results of assessing the implementation of the security controls identified in the security plan to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the specified security requirements. The security assessment report also contains a list of recommended corrective actions for any weaknesses or deficiencies identified in the security controls.[62] Supporting the near real-time risk management objectives of the security authorization process, the security assessment report is updated on an ongoing basis whenever changes are made to the security controls employed within or inherited by the information system.[63] Updates to the security assessment report help to ensure that the information system owner, common control provider, and authorizing officials maintain the appropriate awareness with regard to security control effectiveness. The overall effectiveness of the security controls directly affects the ultimate security state of the information system and decisions regarding explicit acceptance of risk.

The *plan of action and milestones*, prepared by the information system owner or common control provider, describes the specific measures planned: (i) to correct weaknesses or deficiencies noted in the security controls during the assessment; and (ii) to address known vulnerabilities in the information system.[64] The content and structure of plans of action and milestones are informed by the organizational risk management strategy developed as part of the risk executive (function) and is consistent with the plans of action and milestones process established by the organization and any specific requirements defined in federal policies, directives, memoranda, or regulations. The most effective plans of action and milestones contain a robust set of actual weaknesses or deficiencies identified in the security controls employed within or inherited by the information system. Assuming that most information systems and the environments in which those systems are deployed, have more vulnerabilities than available resources can realistically address, organizations define a strategy for developing and implementing plans of action and milestones that facilitates a prioritized approach to risk mitigation and that is consistent across the organization. This strategy helps to ensure that plans of action and milestones are based on:

- The security categorization of the information system;
- The specific weaknesses or deficiencies in the security controls;
- The importance of the identified security control weaknesses or deficiencies (i.e., the direct or indirect effect the weaknesses or deficiencies may have on the overall security state of the information system and hence on the risk exposure[65] of the organization);

[62] Organizations may choose to develop an *executive summary* from the detailed findings that are generated during a security control assessment. An executive summary provides an authorizing official with an abbreviated version of the security assessment report focusing on the highlights of the assessment, synopsis of key findings, and recommendations for addressing weaknesses and deficiencies in the security controls.

[63] Organizations maintain strict version control as critical documents in the authorization package are updated.

[64] Organizations may choose to document the specific measures *implemented* to correct weaknesses or deficiencies in security controls in the plan of action and milestones, thereby providing an historical record of actions completed.

[65] In general, risk exposure is the degree to which an organization is threatened by the potential adverse effects on organizational operations and assets, individuals, other organizations, or the Nation.

- The organization's proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (e.g., prioritization of risk mitigation actions, allocation of risk mitigation resources); and
- The organization's rationale for accepting certain weaknesses or deficiencies in the security controls.[66]

Organizational strategies for plans of action and milestones are guided by the security categories of the respective information systems affected by the risk mitigation activities. Organizations may decide, for example, to allocate the vast majority of risk mitigation resources initially to the *highest-impact* information systems because a failure to correct the weaknesses or deficiencies in those systems could potentially have the most significant adverse effects on the organization's missions or business operations. Organizations also prioritize weaknesses or deficiencies using information from organizational assessments of risk and the risk management strategy developed as part of the risk executive (function). Therefore, a high-impact system would have a prioritized list of weaknesses or deficiencies for that system, as would moderate-impact and low-impact systems. In general, the plan of action and milestones strategy always addresses the highest-priority weaknesses or deficiencies within those prioritized systems.

After completion of the security plan, security assessment report, and plan of action and milestones, the information system owner or common control provider submits the final security authorization package to the authorizing official or designated representative. Figure F-1 illustrates the key sections of the authorization package.

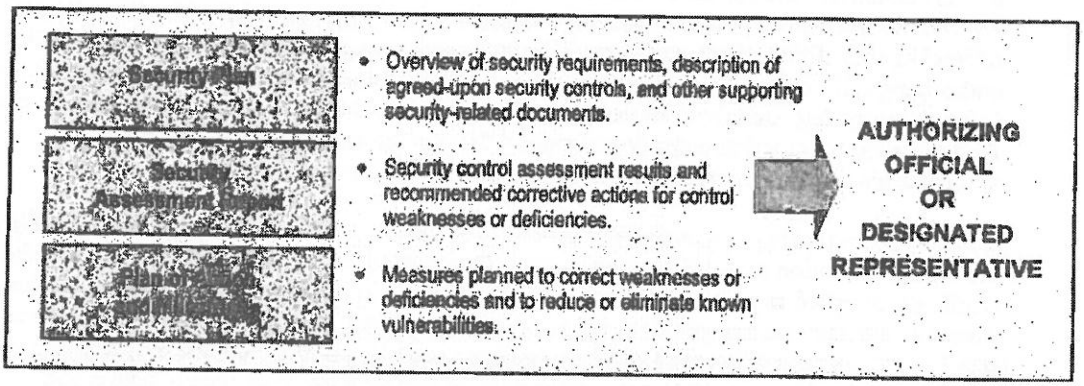


FIGURE F-1: SECURITY AUTHORIZATION PACKAGE

F.2 AUTHORIZATION DECISIONS

Authorization decisions are based on the content of the authorization package including inputs from the organization's risk executive (function) and any additional supporting documentation required by the authorizing official. The security authorization package provides comprehensive information on the security state of the information system. Risk executive (function) inputs, including the previously established overarching risk guidance derived from the risk management strategy, provide additional information to the authorizing official that may be relevant and affect the final authorization decision (e.g., organizational risk tolerance, organization's overall risk mitigation strategy, core mission and business requirements, dependencies among information

[66] Organizations document their rationale for accepting security control weakness or deficiencies.

systems, ongoing risk monitoring requirements, and other types of risks not directly associated with the information system or its environment of operation). Risk executive (function) inputs are documented and become part of the authorization decision. Organizations determine how the risk management strategy and risk-related guidance from the risk executive (function) influences/impacts the authorization decisions of authorizing officials. Security authorization decisions are conveyed to information system owners and common control providers and are made available to selected officials within the organization (e.g., information system owners inheriting common controls, authorizing officials for interconnected systems, chief information officers, senior information security officers, information owners/stewards). There are two types of authorization decisions that can be rendered by authorizing officials:

- Authorization to operate;[67] and
- Denial of authorization to operate.

Authorization to Operate

If the authorizing official, after reviewing the authorization package and any additional inputs provided by the risk executive (function), deems that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable, an *authorization to operate* is issued for the information system or for the common controls inherited by organizational information systems. The information system is authorized to operate for a specified time period in accordance with the terms and conditions established by the authorizing official.[68] For common control providers external to an information system, the authorization decision means that the common controls under their control are approved for *inheritance* by organizational information systems. An *authorization termination date* is also established by the authorizing official as a condition of authorization. The authorization termination date can be adjusted by the authorizing official to reflect an increased level of concern regarding the security state of the information system including the security control employed within or inherited by the system. Authorization termination dates do not exceed the maximum allowable time periods for authorization established by federal or organizational policy.

The authorizing official takes specific actions to reduce or eliminate vulnerabilities identified during the execution of the Risk Management Framework unless the vulnerabilities have been explicitly accepted as part of the authorization decision. In addition, the information system owner or common control provider establishes a disciplined, structured, and repeatable process to monitor the ongoing effectiveness of the deployed security controls and the progress of any actions taken to correct or eliminate weaknesses or deficiencies. The plan of action and milestones submitted by the information system owner is used by the authorizing official to monitor the progress in correcting deficiencies and weaknesses noted during the security control assessment.

---

[67] An *interim authorization to test* is a special type of authorization decision allowing an information system to operate in an operational environment for the express purpose of testing the system with actual operational (i.e., live) data for a specified time period. An interim authorization to test is granted by an authorizing official only when the operational environment or live data is required to complete specific test objectives.

[68] Some organizations may choose to use the term *interim authorization to operate* to focus attention on the increased risk being accepted by the authorizing official in situations where there are significant weaknesses or deficiencies in the information system, but an overarching mission necessity requires placing the system into operation or continuing its operation.

Denial of Authorization to Operate

If the authorizing official, after reviewing the authorization package and any additional inputs provided by the risk executive (function), deems that the risk to organizational operations and assets, individuals, other organizations, and the Nation is unacceptable and immediate steps cannot be taken to reduce the risk to an acceptable level, a *denial of authorization to operate* is issued for the information system or for the common controls inherited by organizational information systems. The information system is not authorized to operate and is not placed into operation. If the system is currently in operation, all activity is halted. For common control providers external to an information system, the authorization decision means that the common controls under their control are *not* approved for *inheritance* by organizational information systems. Failure to receive an authorization to operate indicates that there are major weaknesses or deficiencies in the security controls employed within or inherited by the information system. The authorizing official or designated representative works with the information system owner or common control provider to revise the plan of action and milestones to ensure that appropriate measures are taken to correct the identified weaknesses or deficiencies.

A special case of a denial of authorization to operate is an *authorization rescission*. Authorizing officials can rescind a previous authorization decision at any time in situations where there is a specific violation of: (i) federal/organizational security policies, directives, regulations, standards, guidance, or practices; or (ii) the terms and conditions of the original authorization. For example, failure to maintain an effective continuous monitoring program may be grounds for rescinding an authorization decision. Authorizing officials consult with the risk executive (function) and the senior information security officer before rescinding security authorizations.

F.3 AUTHORIZATION DECISION DOCUMENT

The *authorization decision document* transmits the final security authorization decision from the authorizing official to the information system owner or common control provider and other key organizational officials, as appropriate. The authorization decision document contains the following information:

- Authorization decision;
- Terms and conditions for the authorization;
- Authorization termination date; and
- Risk executive (function) input (if provided).

The security *authorization decision* indicates whether the information system is: (i) authorized to operate; or (ii) not authorized to operate. For common controls, the authorization decision means that the controls are approved for *inheritance* by organizational information systems. The *terms and conditions* for the authorization provide a description of any limitations or restrictions placed on the operation of the information system or the implementation of common controls that must be followed by the system owner or common control provider. The *authorization termination date*, established by the authorizing official, indicates when the security authorization expires and reauthorization is required. An authorizing official designated representative prepares the authorization decision document for the authorizing official with authorization recommendations, as appropriate. The authorization decision document is attached to the original authorization package and transmitted to the information system owner or common control provider.[69]

[69] Authorization decision documents may be digitally signed to ensure authenticity.

Upon receipt of the authorization decision document and authorization package, the information system owner or common control provider acknowledges and implements the terms and conditions of the authorization and notifies the authorizing official. The information system owner or common control provider retains the original authorization decision document and authorization package.[70] The organization ensures that authorization documents for information systems and for common controls are available to appropriate organizational officials (e.g., information system owners inheriting common controls, the risk executive [function], chief information officers, senior information security officers, information system security officers). The contents of the security authorization documentation, especially information regarding information system vulnerabilities, are: (i) marked and appropriately protected in accordance with federal/organizational policy; and (ii) retained in accordance with the organization's record retention policy. The authorizing official verifies on an ongoing basis, that the terms and conditions established as part of the authorization are being followed by the information system owner or common control provider.

F.4 ONGOING AUTHORIZATION

A robust and comprehensive continuous monitoring[71] strategy integrated into the organization's system development life cycle process, promotes risk management on an ongoing basis and can significantly reduce the resources required for reauthorization, if required. Using automation and state-of-the-practice tools, techniques, and procedures, risk management can become *near real-time* with ongoing monitoring of security controls and changes to the information system and its environment of operation. When monitoring is conducted in accordance with the needs of the authorizing official, that monitoring results in the production of key information needed to determine: (i) the current security state of the information system (including the effectiveness of the security controls employed within and inherited by the system); (ii) the resulting risks to organizational operations, organizational assets, individuals, other organizations, and the Nation; and (iii) whether to authorize continued operation of the system or continued use of common controls inherited by organizational information systems.

Continuous monitoring also helps to amortize the resource expenditures for reauthorization activities over the authorization period. The ultimate objective is to achieve a state of *ongoing authorization* where the authorizing official maintains sufficient knowledge of the current security state of the information system (including the effectiveness of the security controls employed within and inherited by the system) to determine whether continued operation is acceptable based on ongoing risk determinations, and if not, which step or steps in the Risk Management Framework needs to be re-executed in order to adequately mitigate the additional risk. Formal reauthorization actions are avoided in situations where the continuous monitoring process provides authorizing officials the necessary information to manage the potential risk arising from changes to the information system or its environment of operation. Organizations maximize the use of status reports and security state information produced during the continuous monitoring process to minimize the level of effort required if a formal reauthorization action is required. Formal reauthorization actions occur at the discretion of the authorizing official in accordance with federal or organizational policy. If a formal reauthorization action is required, organizations maximize the use of security and risk-related information produced during the continuous monitoring and ongoing authorization processes currently in effect.

[70] Organizations may choose to employ automated tools to support the development, distribution, and archiving of risk management documentation to include artifacts associated with the security authorization process.

[71] Continuous monitoring is described in Appendix G.

Reauthorization actions, if initiated, can be either *time-driven* or *event-driven*. Time-driven reauthorizations occur when the authorization termination date is reached. Authorization termination dates are influenced by federal and/or organizational policies and by the requirements of authorizing officials which may establish maximum authorization periods. For example, if the maximum authorization period for an information system is three years, then an organization establishes a continuous monitoring strategy for assessing a subset of the security controls employed within and inherited by the system during the authorization period. This strategy allows all security controls designated in the respective security plans to be assessed at least one time by the end of the three-year period. This also includes any common controls deployed external to organizational information systems. If the security control assessments are conducted by qualified assessors with the required degree of *independence* based on federal/organizational policies, appropriate security standards and guidelines, and the needs of the authorizing official, the assessment results can be cumulatively applied to the reauthorization, thus supporting the concept of ongoing authorization.[72] The reauthorization action can be as simple as updating the security status information in the authorization package (i.e., the security plan, security assessment report, and plan of action and milestones). The authorizing official subsequently signs an updated authorization decision document based on the current determination and acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation.[73]

Unless otherwise handled by continuous monitoring and ongoing authorization, event-driven reauthorizations can occur when there is a significant change to an information system or its environment of operation. A significant change is defined as a change that is likely to affect the security state of an information system. Significant changes to an information system may include for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations.[74] If a formal reauthorization action is initiated, the organization targets only the specific security controls affected by the changes and reuses previous assessment results wherever possible. Most routine changes to an information system or its environment of operation can be handled by the organization's continuous monitoring program, thus supporting the concept of ongoing authorization. An effective monitoring program can significantly reduce the overall cost and level of effort of reauthorization actions.

In the event that there is a change in authorizing officials, the new authorizing official reviews the current authorization decision document, authorization package, and any updated documents created as a result of the ongoing monitoring activities. If the new authorizing official is willing to accept the currently documented risk, then the official signs a new authorization decision document, thus formally transferring responsibility and accountability for the information system

[72] NIST Special Publication 800-53A describes the specific conditions when security-related information can be reused in security authorizations, ongoing authorizations, and reauthorizations.

[73] Decisions to initiate a formal reauthorization action include inputs from the risk executive (function) and the senior information security officer.

[74] The examples of changes listed above are only *significant* when they meet the threshold established in the definition of significant change (i.e., a change that is likely to affect the security state of the information system).

or the common controls inherited by organizational information systems and explicitly accepting the risk to organizational operations and assets, individuals, other organizations, and the Nation. If the new authorizing official is not willing to accept the previous authorization results (including identified level of risk), a *reauthorization* action may need to be initiated or the new authorizing official may instead establish new terms and conditions for continuing the original authorization, but not extend the original authorization termination date. In all situations where there is a decision to reauthorize an information system or the common controls inherited by organizational information systems, the maximum reuse of authorization information is strongly encouraged to minimize the time and expense associated with the reauthorization effort.[75]

F.5 TYPE AUTHORIZATION

A *type authorization* is an official authorization decision to employ identical copies of an information system or subsystem (including hardware, software, firmware, and/or applications) in specified environments of operation.[76] This form of authorization allows a single authorization package (i.e., security plan, security assessment report, and plan of action and milestones) to be developed for an archetype (common) version of an information system that is deployed to multiple locations, along with a set of installation and configuration requirements or operational security needs, that will be assumed by the hosting organization at a specific location. The type authorization is used in conjunction with the authorization of site-specific controls (e.g., physical and environmental protection controls, personnel security controls) inherited by the information system.[77] The RMF tasks listed in Chapter 3 address the authorization activities associated with the employment of system-specific, hybrid, and common controls.

F.6 AUTHORIZATION APPROACHES

Organizations can choose from three different approaches when planning for and conducting security authorizations to include: (i) an authorization with a *single* authorizing official; (ii) an authorization with *multiple* authorizing officials; or (iii) *leveraging* an existing authorization.[78] The first approach is the traditional authorization process defined in this appendix where a single organizational official in a senior leadership position is both responsible and accountable for an information system. The organizational official also accepts the information system-related security risks that may impact organizational operations and assets, individuals, other organizations, or the Nation.

The second approach, or *joint authorization*, is employed when multiple organizational officials either from the same organization or different organizations, have a shared interest in authorizing an information system. The organizational officials collectively are responsible and accountable for the information system and jointly accept the information system-related security risks that

---

[75] The decision to initiate a formal reauthorization action can be based on a variety of factors, including for example, the acceptability of the previous authorization information provided in the authorization package, the length of time since the previous authorization decision, the risk tolerance of the new authorizing official, and current organizational requirements and/or priorities.

[76] Examples of type authorizations include: (i) an authorization of the hardware and software applications for a standard financial system deployed in several locations around the world; or (ii) an authorization of a common workstation or operating environment (i.e., hardware, operating system, middleware, and applications) deployed to all operating units within an organization.

[77] Site-specific controls are typically implemented by an organization as *common controls*.

[78] Authorization approaches can be applied to both information systems and to common controls inherited by one or more organizational information systems.

may adversely impact organizational operations and assets, individuals, other organizations, and the Nation. A similar authorization process is followed as in the first approach with the essential difference being the addition of multiple authorizing officials. Organizations choosing a joint authorization approach are expected to work together on the planning and the execution of RMF tasks (see Appendix H) and to document their agreement and progress in implementing the tasks. Collaborating on the security categorization, selection of security controls, plan for assessing the controls to determine effectiveness, plan of action and milestones, and continuous monitoring strategy, is necessary for a successful joint authorization. The specific terms and conditions of the joint authorization are established by the participating parties in the joint authorization including for example, the process for ongoing determination and acceptance of risk. The joint authorization remains in effect only as long as there is mutual agreement among authorizing officials and the authorization meets the requirements established by federal and/or organizational policies.

The final approach, *leveraged authorization*, is employed when a federal agency[79] chooses to accept some or all of the information in an existing authorization package generated by another federal agency (hereafter referred to as the *owning* organization[80]) based on a need to use the same information resources (e.g., information system and/or services provided by the system). The leveraging organization reviews the owning organization's authorization package as the basis for determining risk to the leveraging organization.[81] When reviewing the authorization package, the leveraging organization considers risk factors such as the time elapsed since the authorization results were produced, the environment of operation (if different from the environment of operation reflected in the authorization package), the criticality/sensitivity of the information to be processed, stored, or transmitted, as well as the overall risk tolerance of the leveraging organization. If the leveraging organization determines that there is insufficient information in the authorization package or inadequate security measures in place for establishing an acceptable level of risk, the leveraging organization may negotiate with the owning organization for additional security measures and/or security-related information.[82] Additional security measures may include, for example, increasing the number of security controls, conducting additional assessments, implementing compensating controls, or establishing constraints on the use of the information system or services provided by the system. Security-related information may include, for example, other information that the owning organization may have discerned in the use or assessment of the information system that is not reflected in the authorization package. The additional security measures and/or security-related information may be provided by the leveraging organization, the information system developer, some other external third party, or some combination of the above.

The leveraged authorization approach provides opportunities for significant cost savings and avoids a potentially costly and time-consuming authorization process by the leveraging

[79] In this situation, federal agency includes any organizations that are subordinate to the agency. For example, NIST is a subordinate organization to the Department of Commerce.

[80] The term *owning* organization refers to the federal agency or subordinate organization that owns the authorization package. The information system may not be owned by the same organization that owns the authorization package, for example, in situations where the system/services are provided by an external provider.

[81] The sharing of the authorization package (including the security plan, security assessment report, plan of action and milestones, and authorization decision document) is accomplished under terms and conditions agreed upon by all parties (i.e., the owning organization and the leveraging organization).

[82] Negotiations with the owning organization may include other organizations (e.g., when the information system and/or services are provided to the owning organization in full or in part, by an external provider).

organization. Leveraging organizations generate an authorization decision document and reference, as appropriate, information in the authorization package from the owning organization. In situations where addition security measures are implemented, the leveraging organization documents those measures by creating an addendum to the original authorization package of the owning organization. This addendum may include, as appropriate, updates to the security plan, security assessment report, and/or plan of action and milestones. Consistent with the traditional authorization process described above, a single organizational official in a senior leadership position in the leveraging organization is both responsible and accountable for accepting the information system-related security risks that may impact the leveraging organization's operations and assets, individuals, other organizations, or the Nation. The leveraged authorization remains in effect as long as the leveraging organization accepts the information system-related security risks and the authorization meets the requirements established by federal and/or organizational policies. This requires the sharing of information resulting from continuous monitoring activities conducted by the owning organization (e.g., updates to the security plan, security assessment report, plan of action and milestones, and security status reports). To enhance the security of all parties, the leveraging organization can also share with the owning organization, the results from any RMF-related activities it conducts to supplement the authorization results produced by the owning organization.

For all three authorization approaches described above, risk management-related activities (including RMF tasks) involving external providers are carried out in accordance with the guidance provided in Appendices H and I.

APPENDIX G

CONTINUOUS MONITORING

MANAGING AND TRACKING THE SECURITY STATE OF INFORMATION SYSTEMS

A critical aspect of managing risk to information from the operation and use of information systems involves the continuous monitoring of the security controls employed within or inherited by the system.[83] Conducting a thorough point-in-time assessment of the deployed security controls is a necessary but not sufficient condition to demonstrate security due diligence. An effective organizational information security program also includes a rigorous continuous monitoring program integrated into the system development life cycle. The objective of the continuous monitoring program is to determine if the set of deployed security controls continue to be effective over time in light of the inevitable changes that occur. Continuous monitoring is a proven technique to address the security impacts on an information system resulting from changes to the hardware, software, firmware, or operational environment. A well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status-related information to organizational officials in order to take appropriate risk mitigation actions and make cost-effective, risk-based decisions regarding the operation of the information system. Continuous monitoring programs provide organizations with an effective mechanism to update *security plans*, *security assessment reports*, and *plans of action and milestones*.

G.1 MONITORING STRATEGY

Organizations develop a strategy and implement a program for the continuous monitoring of security control effectiveness including the potential need to change or supplement the control set, taking into account any proposed/actual changes to the information system or its environment of operation. The monitoring program is integrated into the organization's system development life cycle processes. A robust continuous monitoring program requires the active involvement of information system owners and common control providers, chief information officers, senior information security officers, and authorizing officials. The monitoring program allows an organization to: (i) track the security state of an information system on a continuous basis; and (ii) maintain the security authorization for the system over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and represents a significant change in the way security authorization activities have been employed in the past. Near real-time risk management of information systems can be facilitated by employing automated support tools to execute various steps in the RMF including authorization-related activities. In addition to vulnerability scanning tools, system and network monitoring tools, and other automated support tools that can help to determine the security state of an information system, organizations can employ automated security management and reporting tools to update key documents in the authorization package including the security plan, security assessment report, and plan of action and milestones. The documents in the authorization package are considered "living documents" and updated accordingly based on actual events that may affect the security state of the information system.

[83] A continuous monitoring program within an organization involves a different set of activities than Security Incident Monitoring or Security Event Monitoring programs.

Timeliness is critical for near-real time risk management. Organizations are encouraged to consolidate available information into measures that can be displayed as trend reports or other types of dashboard visualization to assist decision makers with timely review and decision making. Transitioning to a near real-time risk management environment will require the increased use of automated support tools over time as organizations integrate these technologies into their information security programs in accordance with available resources.

An effective organization-wide continuous monitoring program includes:

- Configuration management and control processes for organizational information systems;
- Security impact analyses on proposed or actual changes to organizational information systems and environments of operation;[84]
- Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the organization-defined continuous monitoring strategy;[85]
- Security status reporting to appropriate organizational officials;[86] and
- Active involvement by authorizing officials in the ongoing management of information system-related security risks.

With regard to configuration management and control, it is important to document the proposed or actual changes to the information system and its environment of operation and to subsequently determine the impact of those proposed or actual changes on the overall security state of the system. Information systems and the environments in which those systems operate are typically in a constant state of change (e.g., upgrading hardware, software, or firmware; redefining the missions and business processes of the organization; discovering new threats). Documenting information system changes as part of routine SDLC processes and assessing the potential impact those changes may have on the security state of the system is an essential aspect of continuous monitoring, maintaining the current authorization, and supporting a decision for reauthorization when appropriate.

G.2 SELECTION OF SECURITY CONTROLS FOR MONITORING

The criteria for selecting which security controls to monitor and for determining the frequency of such monitoring are established by the information system owner or common control provider in collaboration with the authorizing official or designated representative, chief information officer, senior information security officer, and risk executive (function). The selection criteria reflect the organization's priorities and importance of the information system (or in the case of common

[84] Although the primary focus of continuous monitoring activities is on the effectiveness of security controls employed within and inherited by an information system, there are other equally important external factors in the environment of operation for a system that also require monitoring on an ongoing basis. These factors include, for example, changes in the organization's missions or business processes, changes in the threat space, and changes in tolerance for previously accepted risks).

[85] Through the use of automation, it is possible to monitor a greater number of security controls on an ongoing basis than is feasible using manual processes. As a result, organizations may choose to monitor a greater number of security controls with increased frequency.

[86] Organizations have significant latitude and flexibility in the breadth, depth, and formality of security status reports. At a minimum, security status reports describe or summarize key changes to security plans, security assessment reports, and plans of action and milestones. At the discretion of the organization, security status reports on information systems can be used to help satisfy the FISMA reporting requirement for documenting remedial actions on any security-related weaknesses or deficiencies.

controls, the information systems inheriting the controls) to organizational operations and assets, individuals, other organizations, and the Nation in accordance with FIPS 199 or CNSS Instruction 1253. Organizations may use recent risk assessments (including current threat and vulnerability information), history of cyber attacks, results of previous security assessments, and operational requirements in guiding the selection of security controls to be monitored and the frequency of the monitoring process.

Priority for security control monitoring is given to the controls that have the greatest volatility and the controls that have been identified in the organization's plan of action and milestones. Security control volatility is a measure of how frequently a control is likely to change over time subsequent to its implementation. For example, security policies and procedures in a particular organization may not be likely to change from one year to the next and thus would likely be security controls with lower volatility. Access controls or other (technical) security controls that are subject to the direct effects or side effects of frequent changes in hardware, software, and/or firmware components of an information system would, therefore, likely be controls with higher volatility. Security controls identified in the plan of action and milestones are also a priority in the continuous monitoring process, due to the fact that these controls have been deemed to be ineffective to some degree. Organizations also consider specific threat information including known attack vectors (i.e., specific vulnerabilities exploited by threat sources) when selecting the set of security controls to monitor and the frequency of such monitoring. The authorizing official or designated representative approves the set of security controls that are to be monitored on an ongoing basis as well as the frequency of the monitoring activities.

G.3 KEY DOCUMENT UPDATES AND STATUS REPORTING

Continuous monitoring results are considered with respect to any necessary updates to the security plan, security assessment report, and plan of action and milestones, since these documents are used to guide future risk management activities. Updated security plans reflect any modifications to security controls based on the risk mitigation activities carried out by information system owners or common control providers. Updated security assessment reports reflect additional assessment activities conducted by assessors to determine security control effectiveness based on modifications to the security plan and deployed controls. Updated plans of action and milestones: (i) report progress made on the current outstanding items listed in the plan; (ii) address vulnerabilities discovered during the security impact analysis or security control monitoring; and (iii) describe how the information system owner or common control provider intends to address those vulnerabilities. The results of monitoring activities are reported to authorizing officials on an ongoing basis in the form of status reports. Other key organizational officials (e.g., risk executive [function], senior information security officer) receive the results of continuous monitoring activities as needed or as requested. With the use of automated support tools and effective organization-wide security program management practices, authorizing officials have the capability to access the most recent documentation in the authorization package at any time to determine the current security state of the information system, to help manage risk, and to provide essential information for potential reauthorization decisions. The monitoring of security controls and changes to the information system and its environment of operation, continues throughout the system development life cycle. Summaries of monitoring results are provided to the senior information security officer and the risk executive (function).

APPENDIX H

OPERATIONAL SCENARIOS

APPLYING THE RISK MANAGEMENT FRAMEWORK IN DIFFERENT ENVIRONMENTS

Managing risk to information from the operation and use of information systems in modern computing environments with a diverse set of potential business relationships can be challenging for organizations. Relationships are established and maintained in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, lines of business arrangements, interagency and intra-agency agreements), licensing agreements, and supply chain arrangements.[87] The Risk Management Framework (RMF) applies only to federal information systems. There are two distinct types of operational scenarios that affect how organizations address the RMF steps and associated tasks:

- Information systems used or operated by *federal agencies*;[88] and
- Information systems used or operated by *other organizations*[89] on behalf of federal agencies.

SCENARIO 1: For an information system that is used or operated by a federal agency, the system boundary is defined by the agency. The agency conducts all RMF tasks to include information system authorization. The agency maintains control over the security controls employed within and inherited by the information system.

SCENARIO 2: For an information system that is used or operated by *another organization* on behalf of a federal agency, the system boundary is defined by the agency in collaboration with the other organization and one of the following situations applies:

- If the organization is contracted to a federal agency, the contractor can conduct all RMF tasks except those tasks which must be carried out by the federal agency as part of its inherent governmental responsibilities.[90] The agency provides RMF-related inputs to the contractor, as needed, and maintains strict oversight on all contractor-executed RMF tasks. The contractor provides appropriate evidence in the security authorization package for the authorization decision by the authorizing official from the federal agency.
- If the organization is a federal agency, the organization can conduct all RMF tasks to include the information system authorization. The information system authorization can also be a joint authorization if both parties agree to share the authorization responsibilities. In situations where a federal agency uses or operates an information system on behalf of multiple federal agencies, the joint authorization can include all participating agencies.

---

[87] NIST Special Publication 800-53 provides additional guidance on the application and use of security controls in external environments to include relationships with external service providers.

[88] References to federal agencies include organizations that are *subordinate* to those agencies.

[89] Organizations that use or operate an information system on behalf of a federal agency or one of its subordinate organizations can include, for example, other federal agencies or their subordinate organizations, state and local government agencies, contractors, and academic institutions.

[90] Organizations ensure that requirements for conducting the specific tasks in the RMF are included in appropriate contractual vehicles, including requirements for independent assessments, when appropriate.

APPENDIX I

SECURITY CONTROLS IN EXTERNAL ENVIRONMENTS

PARTNERSHIPS, OUTSOURCING, AND SUPPLY CHAIN CONSIDERATIONS

Organizations are becoming increasingly reliant on information system services provided by external providers to carry out important missions and business functions. External information system services are services implemented outside of the authorization boundaries established by the organization for its information systems. These external services may be used by, but are not part of, organizational information systems. In some situations, external information system services may completely replace the functionality of internal information systems. Organizations are responsible and accountable for the *risk* incurred by use of services provided by external providers and address this risk by implementing compensating controls when the risk is greater than the authorizing official or the organization is willing to accept.

Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The growing dependence on external service providers and new relationships being forged with those providers present new and difficult challenges for the organization, especially in the area of information system security. These challenges include:

- Defining the types of external services provided to the organization;
- Describing how the external services are protected in accordance with the security requirements of the organization; and
- Obtaining the necessary assurances that the risk to organizational operations and assets, individuals, other organizations, and the Nation arising from the use of the external services is acceptable.

FISMA and OMB policy require external providers handling federal information or operating information systems on behalf of the federal government to meet the same security requirements as federal agencies. Security requirements for external providers including the security controls for information systems processing, storing, or transmitting federal information are expressed in appropriate contracts or other formal agreements. Organizations can require external providers to implement all steps in the RMF with the exception of the security authorization step, which remains an inherent federal responsibility that is directly linked to the management of risk related to the use of external information system services.[91]

The assurance or confidence that the risk from using external services is at an acceptable level depends on the trust[92] that the organization places in the external service provider. In some cases, the level of trust is based on the amount of direct control the organization is able to exert on the

[91] If the external provider is a federal agency, the provider can conduct all RMF tasks to include the information system authorization (see Appendix H).

[92] The level of trust that an organization places in an external service provider can vary widely, ranging from those who are highly trusted (e.g., business partners in a joint venture that share a common business model and common goals) to those who are less trusted and represent greater sources of risk (e.g., business partners in one endeavor who are also competitors in another market sector).

external service provider with regard to employment of security controls necessary for the protection of the service and the evidence brought forth as to the effectiveness of those controls. The level of control is usually established by the terms and conditions of the contract or service-level agreement with the external service provider and can range from extensive (e.g., negotiating a contract or agreement that specifies detailed security control requirements for the provider) to very limited (e.g., using a contract or service-level agreement to obtain commodity services[93] such as commercial telecommunications services). In other cases, the level of trust is based on factors that convince the organization that the requisite security controls have been employed and that a determination of control effectiveness exists. For example, a separately authorized external information system service provided to an organization through a well-established line of business relationship may provide a degree of trust in the external service within the tolerable risk range of the authorizing official.

The provision of services by external providers may result in some services without explicit agreements between the organization and the external entities responsible for the services. Whenever explicit agreements are feasible and practical (e.g., through contracts, service-level agreements, etc.), the organization develops such agreements and requires the use of the security controls in NIST Special Publication 800-53. When the organization is not in a position to require explicit agreements with external providers (e.g., the service is imposed on the organization or the service is commodity service), the organization establishes explicit assumptions about the service capabilities with regard to security. In situations where an organization is procuring information system services or technologies through a centralized acquisition vehicle (e.g., government-wide contract by the General Services Administration or other preferred and/or mandatory acquisition organization), it may be more efficient and cost-effective for the originator of the contract to establish and maintain a stated level of trust with the external provider (including the definition of required security controls and level of assurance with regard to the provision of such controls). Organizations subsequently acquiring information system services or technologies from the centralized contract can take advantage of the negotiated trust level established by the procurement originator and thus avoid costly repetition of the activities necessary to establish such trust.[94] Contracts and agreements between the organization and external providers may also require the active participation of the organization. For example, the organization may be required by the contract to install public key encryption-enabled client software recommended by the service provider.

Ultimately, the responsibility for adequately mitigating unacceptable risks arising from the use of external information system services remains with the authorizing official. Organizations require that an appropriate *chain of trust* be established with external service providers when dealing with the many issues associated with information system security. A chain of trust requires that the organization establish and retain a level of confidence that each participating service provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The chain of trust can be complicated due to the number of

[93] Commercial providers of commodity-type services typically organize their business models and services around the concept of shared resources and devices for a broad and diverse customer base. Therefore, unless organizations obtain fully dedicated services from commercial service providers, there may be a need for greater reliance on compensating security controls to provide the necessary protections for the information system that relies on those external services. The organization's risk assessment and risk mitigation activities reflect this situation.

[94] For example, a procurement originator could authorize an information system providing external services to the federal government under specific terms and conditions of the contract. A federal agency requesting information system services under the terms of the contract would not be required to reauthorize the information system when acquiring such services (unless the request included services outside the scope of the original contract).

entities participating in the consumer-provider relationship and the type of relationship between the parties. External service providers may also in turn outsource the services to other external entities, making the chain of trust even more complicated and difficult to manage. Depending on the nature of the service, it may simply be unwise for the organization to place significant trust in the provider—not due to any inherent untrustworthiness on the provider's part, but due to the intrinsic level of risk in the service. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization: (i) employs compensating controls; (ii) accepts a greater degree of risk; or (iii) does not obtain the service (i.e., performs missions or business operations with reduced levels of functionality or possibly no functionality at all).

Exhibit "C"

Summary of NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations

Kelley Dempsey
Computer Security Division
Information Technology Laboratory

Greg Witte
Doug Rike
G2, Inc.
Annapolis Junction, MD

February 19, 2014

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Abstract

This white paper provides an overview of NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, which was published April 30, 2013.

Keywords

assurance; computer security; FIPS Publication 199; FIPS Publication 200, FISMA; Privacy Act; Risk Management Framework; security controls; security requirements

Disclaimer

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.

Additional Information

For additional information on NIST's Computer Security Division programs, projects and publications, visit the Computer Security Resource Center, csrc.nist.gov. Information on other efforts at NIST and in the Information Technology Laboratory (ITL) is available at www.nist.gov and www.nist.gov/itl.

Table of Contents

List of Figures

1 Introduction

In April, 2013, NIST published an update, Revision 4, to NIST Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organization.* The guide was developed and is maintained by the Joint Task Force Transformation Initiative Interagency Working Group, part of an ongoing information security partnership among the U.S. Department of Defense, the Intelligence Community, the Committee on National Security Systems, the Department of Homeland Security, and U.S. federal civil agencies.

SP 800-53 Revision 4 has been updated to reflect the evolving technology and threat space. Example areas include issues particular to mobile and cloud computing; insider threats; applications security; supply chain risks; advanced persistent threat; and trustworthiness, assurance, and resilience of information systems. The revision also contains a new appendix of privacy controls, and related implementation guidance (Appendix J), based on the Fair Information Practice Principles (FIPPs), a widely accepted framework of defining principles to be used in the evaluation and consideration of systems, processes, or programs that affect individual privacy.

SP 800-53 Revision 4 is part of the NIST Special Publication 800-series that reports on the NIST Information Technology Laboratory's (ITL) computer security-related research, guidelines, and outreach. The publication provides a comprehensive set of security controls, three security control baselines (low, moderate, and high impact), and guidance for tailoring the appropriate baseline to specific needs according to the organization's missions, environments of operation, and technologies used.

As the risk to an information system's confidentiality, integrity and/or availability increases, the need for additional controls to protect the system may also increase accordingly. SP 800-53 Revision 4 provides the security control baselines as the starting point for the security control selection process. The baselines are chosen based on the security category and associated impact level of information systems as described in Federal Information Processing Standard Publication (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems,* and FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems.*

A separate guideline, SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations,* provides specific guidelines that facilitate periodic assessment of security controls to ensure that controls have been implemented correctly, are operating as intended, and are meeting the organization's security requirements.

2 NIST SP 800-53 Revision 4 and the Risk Management Framework (RMF)

NIST SP 800-39, *Managing Information Security Risk*, defines risk management as "the program and supporting processes to manage information security risk to organizational operations (including mission, functions, and reputation), organizational assets, individuals, other organizations, and the Nation". To integrate the risk management process throughout an organization and to address its mission and business concerns, a three-tiered approach is employed. The process is carried out across three tiers with the objective of continuous improvement in the organization's risk-related activities, with effective communication among tiers and stakeholders. Figure 1 illustrates the three-tiered approach to risk management.

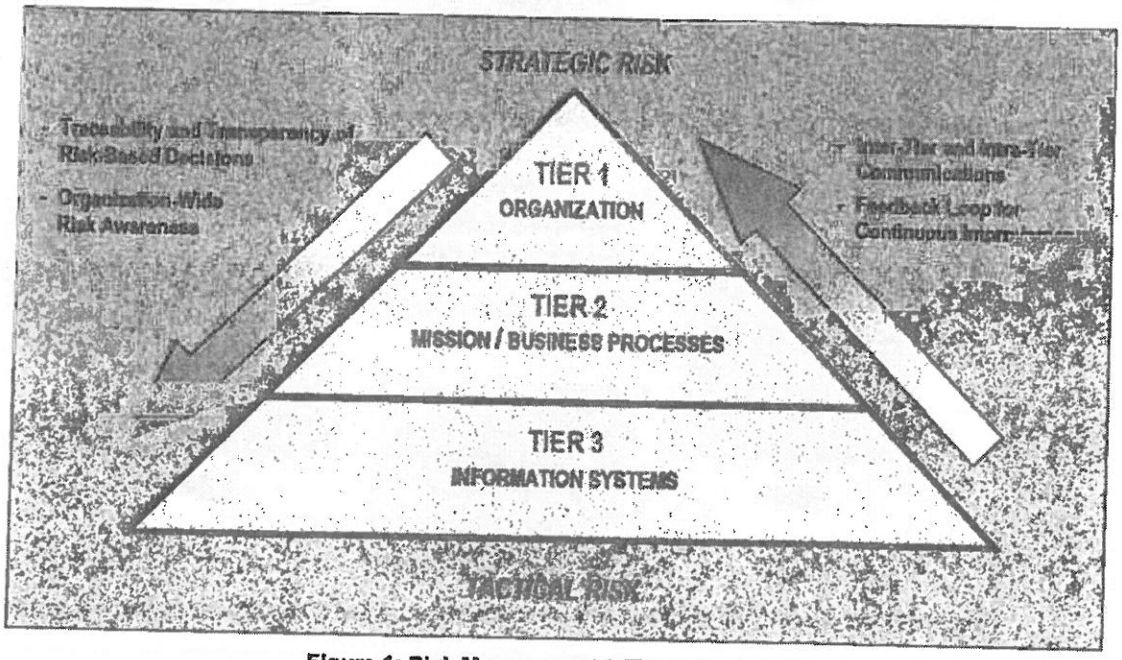


Figure 1: Risk Management 3-Tiered Approach

The NIST Risk Management Framework (RMF), described in NIST Special Publication 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach*, is a methodology for implementing risk management at the information systems tier. The RMF (depicted in Figure 2) identifies six distinct steps that provide a disciplined and structured process to integrate information security risk management activities into the system development life cycle. The RMF addresses security concerns of organizations related to the design, development, implementation, operation, and disposal of information systems and the environments in which those systems operate.

The security controls in SP 800-53 Rev. 4 support Step Two of the RMF, and a detailed catalog of these controls is provided in Appendix F. For ease of use in the security control selection and specification process, controls are organized into eighteen families, each containing security controls related to the general security topic of the family. Security controls involve aspects of policy, oversight, supervision, manual processes, individual actions, or automated mechanisms implemented by information systems/devices. The security control structure consists of the

following components: (i) a control section; (ii) a supplemental guidance section; (iii) a control enhancements section; (iv) a references section; and (v) a priority and baseline allocation section.

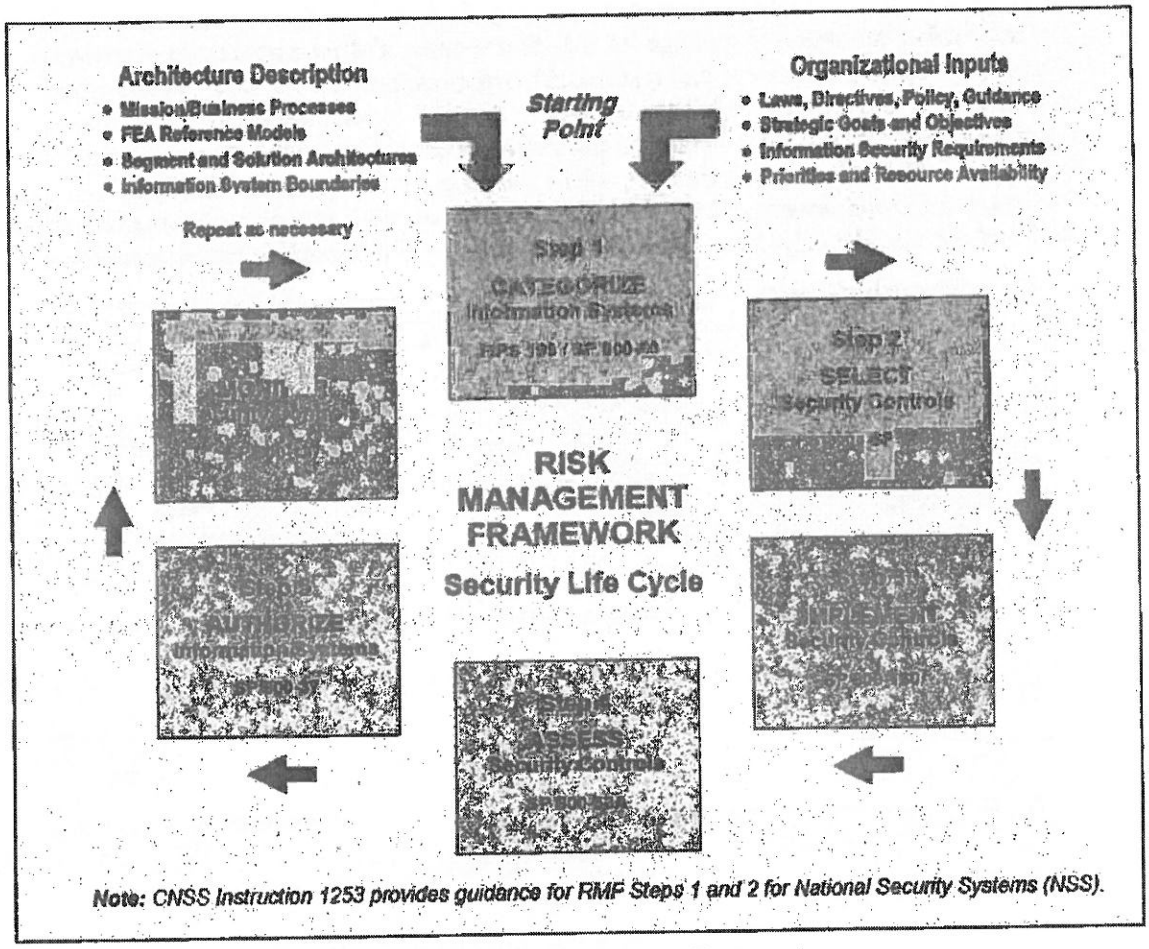


Figure 2: The Risk Management Framework

3 Control Baselines and Tailoring

To assist organizations in making the appropriate selection of security controls for information systems, the concept of security control baselines is introduced. Security control baselines are the starting point for the security control selection process and are chosen based on the security category and associated impact level of information systems determined in accordance with FIPS Publication 199 and FIPS Publication 200, respectively (Step One of the RMF). SP 800-53 Rev. 4 states that "the security controls and control enhancements listed in the initial baselines are not a minimum— but rather a proposed starting point from which controls and controls enhancements may be removed or added." Appendix D provides a listing of baseline security controls corresponding to the low-impact, moderate-impact, and high-impact information systems, using the high water mark defined in FIPS Publication 200.

The security control baselines address the security needs of a broad and diverse set of constituencies, and are developed based on a number of general assumptions, including common environmental, operational, and functional considerations. The baselines also assume typical threats facing common information systems. Articulating the underlying assumptions is a key element in the initial risk framing step of the risk management process described in NIST SP 800-39. To ensure that an appropriate set of controls is identified to provide security commensurate with risk, organizations tailor the controls to align with specific security needs. Organizations may perform tailoring at the organization level for all information systems, in support of a particular line of business or mission/business process, at the individual information system level, or by using a combination of the above. The tailoring process is comprised of several steps, as described in SP 800-53 Rev. 4 Section 3.2. These actions include:

- Identifying and designating common controls - controls that may be inherited by one or more information systems. If an information system inherits a common control, such as environmental controls within a data center, that system does not need to explicitly implement that control.
- Applying scoping considerations – these, when applied in conjunction with risk management guidance, can eliminate unnecessary security controls from the initial security control baselines and help ensure that organizations select *only* those controls needed to provide the appropriate level of protection for information systems. When scoping considerations are applied, compensating controls may need to be selected to provide alternative means to achieve security requirements.
- Supplementing baselines - additional security controls and control enhancements are selected if needed to address specific threats and vulnerabilities.

4 Documenting the Control Selection Process

To aid in review activities, security planning, and risk assessments, organizations document the relevant decisions taken during the security control selection process, providing a sound rationale for those decisions. This documentation is essential when examining the security considerations for organizational information systems with respect to the potential impact on an organization's mission and business.

The resulting tailored baseline set of security controls and the supporting rationale for the selection decisions (including any information system use restrictions required by organizations) are documented in system security plans. Documenting significant risk management decisions in the security control selection process is imperative so that authorizing officials have access to necessary information to make informed authorization decisions for organizational information systems, as demonstrated in Figure 3.

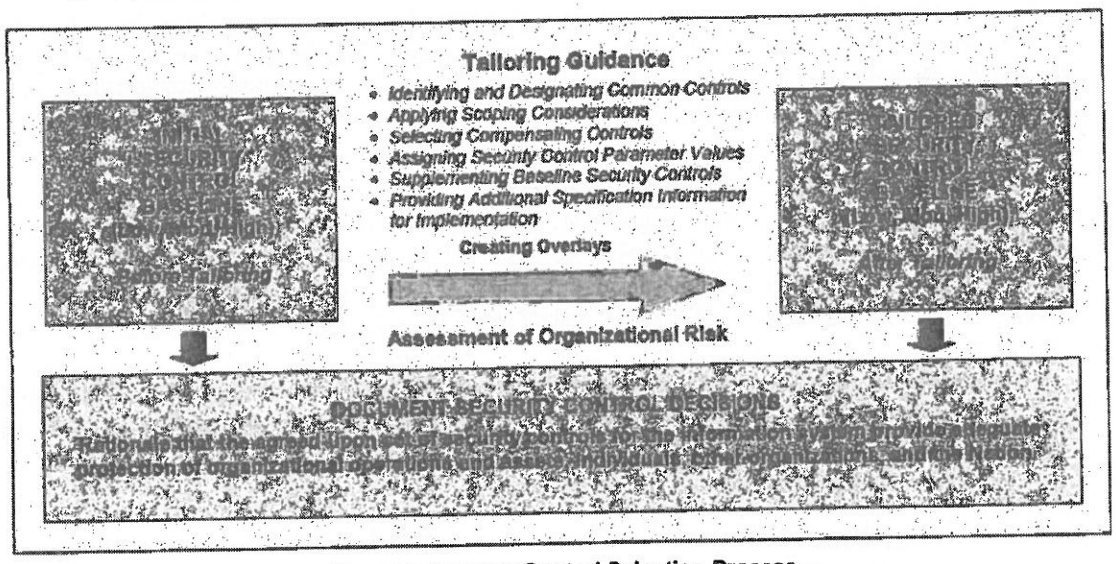


Figure 3: Security Control Selection Process

5 Assurance

Appendix E in SP 800-53 Revision 4 provides an update to guidance regarding security assurance. This section outlines methods for agencies to establish measures of confidence that the implemented security controls provide the security capability required to protect critical missions and business operations.

The criteria for whether a security control is assurance- or functionality-related is based on the overall characteristics of the control. In general, assurance-related controls are controls that: (i) define processes, procedures, techniques, or methodologies for designing and developing information systems and system components; (ii) provide supporting operational processes including improving the quality of systems, components, or processes; (iii) produce security evidence from developmental or operational activities; (iv) determine security control effectiveness or risk; or (v) improve personnel skills, expertise, and understanding.

Appendix E provides three tables that identify specific assurance-related controls that are included in the low-, moderate-, and high-impact baselines described in Appendix D. The controls described assist organizations in defining the controls needed to satisfy minimum assurance requirements. Where additional assurance is desired to achieve risk management objectives, Table E-4 provides additional security controls and control enhancements to achieve enhanced assurance. Implementers should note that designation of assurance-related controls is not intended to imply a greater level of importance for such controls. Achieving adequate security for organizational information systems requires the correct combination of both functionality- and assurance-related security controls.

6 Security Controls

Appendix F, the Security Control Catalog, provides a comprehensive range of countermeasures for organizations and information systems. The security controls are designed to be technology-neutral such that the focus is on the *fundamental* countermeasures needed to protect organizational information during processing, storage, or transmission. SP 800-53 Rev. 4, therefore, does not provide guidance on the application of security controls to specific technologies, environments of operation, or missions/business functions. These specific areas may be addressed using overlays (see below).

Control enhancements are included with many security controls and are selected in order to increase the strength of the base control. Control enhancements are intended to be implemented only in conjunction with implementation of the base control.

Some security controls and control enhancements include one or more *assignment* and *selection* statements. These are variable parameters that organizations define, providing them with the ability to tailor security controls based on specific security requirements, environments of operation, and organizational risk tolerance. Parameters assigned and/or selected by organizations for a given base control also apply to all control enhancements associated with that control.

The first security control in each family (referred to as the dash-1control) addresses policies and procedures needed for effective implementation of all the other controls within each family. Therefore, requirements to develop policies and procedures are not repeated in individual controls.

Many security controls and enhancements include supplemental guidance. The supplemental guidance provides additional information about a control or enhancement to help organizations define, develop, and/or implement security controls but does not include any additional requirements.

SP 800-53 Rev. 4 includes many changes from SP 800-53 Rev. 3 – 295 controls and control enhancements were added while approximately 100 controls and control enhancements were withdrawn or incorporated into others. Of the eighteen security control families in SP 800-53 Rev. 4, seventeen families are described in the security control catalog in Appendix F, and are closely aligned with the seventeen minimum security requirements for federal information and information systems in FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.

One additional family, the Program Management (PM) family, provides controls for information security programs themselves. This family is described in Appendix G of SP 800-53 Rev. 4. While it is not specifically referenced in FIPS 200, the PM section provides security controls at the organization level rather than the information system level. The PM controls are typically implemented at the organization level and not directed at individual organizational information systems. They complement the security controls in Appendix F and focus on the programmatic, organization-wide information security requirements that are independent of any particular information system and are essential for managing information security programs. Tailoring guidance can be applied to the program management controls in a manner similar to how the guidance is applied to security controls in Appendix F.

7 International Information Security Standards

Many organizations use well-known international information security standards as the basis or as a supplemental source of security controls for risk management. To aid in selection and comparison, SP 800-53 Rev. 4 provides mapping tables to provide organizations with a general indication of security control coverage with respect to ISO/IEC 27001, *Information technology–Security techniques–Information security management systems–Requirements* and ISO/IEC 15408, *Information technology -- Security techniques -- Evaluation criteria for IT security*. ISO/IEC 27001 applies to all types of organizations and specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented information security management system (ISMS) within the context of business risks. ISO/IEC 15408 (also known as the Common Criteria) provides functionality and assurance requirements for developers of information systems and information system components (i.e., information technology products). Since many of the technical security controls defined in Appendix F are implemented in hardware, software, and firmware components of information systems, organizations can obtain significant benefit from the acquisition and employment of information technology products evaluated against the requirements of ISO/IEC 15408. The use of such products can provide evidence that certain security controls are implemented correctly, operating as intended, and producing the desired effect in satisfying stated security requirements.

8 Overlays

To help ensure that selected and implemented controls are sufficient to adequately mitigate risks to organizational operations and assets, SP 800-53 Rev. 4 introduces the concept of *overlays*. An overlay provides a set of security controls, control enhancements, and supplemental guidance for community-wide use or to address specialized requirements, technologies, or unique missions and environments of operation. For example, the federal government may decide to establish a government-wide set of security controls and implementation guidance for public key infrastructure (PKI) systems that could be uniformly applied to information systems.

Multiple overlays can be applied to a single security control baseline. The tailored baselines that result from the overlay development process may be more or less stringent than the original security control baselines. Risk assessments provide information necessary to determine if the risk from implementing the tailored baselines falls within the risk tolerance of the organizations or communities of interest developing the overlays.

General guidance on overlays is provided in section 3.3 and an overlay template is provided in Appendix I. The template is included as an example only—organizations may choose to use other formats or modify the format in this appendix based on organizational needs and the type of overlay being developed. The level of detail included in the overlay is at the discretion of the organization initiating the overlay but should be of sufficient breadth and depth to provide an appropriate rationale and justification for the resulting tailored baseline developed, including any risk-based decisions made during the overlay development process.

The sample overlay template consists of eight sections:

- Identification;
- Overlay Characteristics;
- Applicability;
- Overlay Summary;
- Detailed Overlay Control Specifications;
- Tailoring Considerations;
- Definitions; and
- Additional Information or Instructions.

9 Privacy

Federal agencies are required to ensure that privacy protections are incorporated into information security planning. To that end, SP 800-53 Rev. 4 features eight new families of privacy controls that are based on the internationally accepted Fair Information Practice Principles (FIPPs). The proliferation of social media, Smart Grid, mobile, and cloud computing, as well as the transition from structured to unstructured data and metadata environments, have added significant complexities and challenges for federal organizations in safeguarding privacy. These challenges extend well beyond the traditional information technology security view of protecting privacy, which focused primarily on ensuring confidentiality.

The families of controls are described in a similar manner to those of Appendix F (Security Controls) and Appendix G (Information Security Programs Organization-Wide Information Security Program Management Controls). SP 800-53 Rev. 4 reminds readers to view the privacy controls in Appendix J from the same perspective as the Program Management controls in Appendix G—that is, the controls are implemented for each organizational information system irrespective of the FIPS 199 categorization for that system. Appendix J defines controls, control enhancements, guidance, and references for the following new families:

- Authority and Purpose (AP);
- Accountability, Audit, and Risk Management (AR);
- Data Quality and Integrity (DI);
- Data Minimization and Retention (DM);
- Individual Participation and Redress (IP);
- Security (SE);
- Transparency (TR); and,
- Use Limitation (UL).

The use of these standardized privacy controls will provide a more disciplined and structured approach for satisfying federal privacy requirements and demonstrating compliance with those requirements. Organizations should decide when to apply control enhancements to support their particular missions and business functions. Specific overlays for privacy can also be considered to facilitate the tailoring of the security control baselines in Appendix D with the requisite privacy controls to ensure that both security and privacy requirements can be satisfied by organizations.

Exhibit "D"

144

Critical Security Controls

Critical Security Controls for Effective Cyber Defense

Over the years, many security standards and requirements frameworks have been developed in attempts to address risks to enterprise systems and the critical data in them. However, most of these efforts have essentially become exercises in reporting on compliance and have actually diverted security program resources from the constantly evolving attacks that must be addressed. In 2008, this was recognized as a serious problem by the U.S. National Security Agency (NSA), and they began an effort that took an "offense must inform defense" approach to prioritizing a list of the controls that would have the greatest impact in improving risk posture against real-world threats. A consortium of U.S. and international agencies quickly grew, and was joined by experts from private industry and around the globe. Ultimately, recommendations for what became the Critical Security Controls (the Controls) were coordinated through the SANS Institute. In 2013, the stewardship and sustainment of the Controls was transferred to the Council on CyberSecurity (the Council), an independent, global non-profit entity committed to a secure and open Internet.

The Critical Security Controls focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness. Standardization and automation is another top priority, to gain operational efficiencies while also improving effectiveness. The actions defined by the Controls are demonstrably a subset of the comprehensive catalog defined by the National Institute of Standards and Technology (NIST) SP 800-53. The Controls do not attempt to replace the work of NIST, including the Cybersecurity Framework developed in response to Executive Order 13636. The Controls instead prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy. Since the Controls were derived from the most common attack patterns and were vetted across a very broad community of government and industry, with very strong consensus on the resulting set of controls, they serve as the basis for immediate high-value action.

Critical Security Controls - Version 5

1: Inventory of Authorized and Unauthorized Devices
2: Inventory of Authorized and Unauthorized Software
3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4: Continuous Vulnerability Assessment and Remediation
5: Malware Defenses
6: Application Software Security
7: Wireless Access Control
8: Data Recovery Capability
9: Security Skills Assessment and Appropriate Training to Fill Gaps
10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11: Limitation and Control of Network Ports, Protocols, and Services
12: Controlled Use of Administrative Privileges
13: Boundary Defense
14: Maintenance, Monitoring, and Analysis of Audit Logs
15: Controlled Access Based on the Need to Know
16: Account Monitoring and Control
17: Data Protection
18: Incident Response and Management
19: Secure Network Engineering
20: Penetration Tests and Red Team Exercises

Home
Critical Security Controls
Guidelines
History
Solution Directory
Vendor Perspective

Critical Security Controls Mapping

- NERC CIP
- NERC CIP (Excel)
- Verizon Vocabulary for Event Recording and Incident Sharing - VERIS

Critical Security Controls Survey

- Moving From Awareness to Action

Downloads

- The Critical Security Controls for Effective Cyber Defense

You may use the following code to embed the 20 Critical Controls on your site:

```
<iframe src="http://www.sans.org/critical-security-controls/" width="1000"
height="1200" />
```

- Critical Security Controls Poster - Fall 2014

Feedback

Send Comments and Feedback to cca@sans.org

Latest Whitepapers

Ninth Log Management Survey Report
By Jerry Shenk

Creating a Threat Profile for Your Organization
By Stephen Irwin

A Practical Big Data Kill Chain Framework
By Brian Nafziger

Last 25 Papers »

Latest Tweets @SANSInstitute

#HackFestSummit = 100% Pentesting Education! Plus a SECRET o [...]
October 7, 2014 - 1:45 PM

All #cybersecurity professionals! Visit http://t.co/IMVCBT5S [...]
October 7, 2014 - 12:59 PM

.@alanpeller to deliver the keynote at Cyber Defense San Die [...]
October 7, 2014 - 12:58 PM

Contact Us

301-654-SANS(7267)
Mon-Fri 9am - 8pm EST/EDT
Info@sans.org

"It has really been an eye opener concerning the depth of security training and awareness that SANS has to offer."
- Michael Hall, Drivesavers

"As a security professional, this info is foundational to do a competent job, let alone be successful."
- Michael Foster, Providence Health and Security

"The perfect balance of theory and hands-on experience."
- James D. Perry II, University of Tennessee

Exhibit E - Security Content Automation Protocol (SCAP) 1.2 Validated Products

Product Vendor	Product Name	SCAP 1.2 Validations	Tested Platforms	Validation Date
BMC Software	BMC Client Management 12.0.0	• Authenticated Configuration Scanner • Common Vulnerabilities and Exposures (CVE) Option	• Microsoft Windows 7, 64 bit • Microsoft Windows 7, 32 bit • Microsoft Windows Vista, SP2 • Microsoft Windows XP Pro, SP3 • Red Hat Enterprise Linux 5.9 Desktop, 64 bit (x86_64) • Red Hat Enterprise Linux 5.9 Desktop, 32 bit (x86)	9/26/14
Intel Security	Policy Auditor 6.2	• Authenticated Configuration Scanner • Common Vulnerabilities and Exposures (CVE) Option	• Microsoft Windows 7, 64 bit • Microsoft Windows 7, 32 bit • Microsoft Windows Vista, SP2 • Microsoft Windows XP Pro, SP3 • Red Hat Enterprise Linux 5.9 Desktop, 64 bit (x86_64) • Red Hat Enterprise Linux 5.9 Desktop, 32 bit (x86)	9/17/14
Redhat	OpenSCAP 1.0.8	• Authenticated Configuration Scanner • Common Vulnerabilities and Exposures (CVE) Option	• Red Hat Enterprise Linux 5.9 Desktop, (x86_64) • Red Hat Enterprise Linux 5.9 Desktop, (x86)	4/17/14
Center for Internet Security	Configuration Assessment Tool (CIST-CAT) 3	• Authenticated Configuration Scanner • Common Vulnerabilities and Exposures (CVE) Option	• Microsoft Windows 7, 64 bit • Microsoft Windows 7, 32 bit • Microsoft Windows Vista, SP2 • Microsoft Windows XP Pro, SP3 • Red Hat Enterprise Linux 5 Desktop, 64 bit • Red Hat Enterprise Linux 5 Desktop, 32 bit	3/24/14
Tripwire	Tripwire Enterprise 8	• Authenticated Configuration Scanner • Common Vulnerabilities and Exposures (CVE) Option	• Microsoft Windows 7, 64 bit • Microsoft Windows 7, 32 bit • Red Hat Enterprise Linux 5 Desktop, 64 bit • Red Hat Enterprise Linux 5 Desktop, 32 bit	11/7/13

Rev. 04/14

State of West Virginia

VENDOR PREFERENCE CERTIFICATE

Certification and application* is hereby made for Preference in accordance with ***West Virginia Code***, §5A-3-37. (Does not apply to construction contracts). ***West Virginia Code***, §5A-3-37, provides an opportunity for qualifying vendors to request (at the time of bid) preference for their residency status. Such preference is an evaluation method only and will be applied only to the cost bid in accordance with the ***West Virginia Code***. This certificate for application is to be used to request such preference. The Purchasing Division will make the determination of the Vendor Preference, if applicable.

1. **Application is made for 2.5% vendor preference for the reason checked:**

____ Bidder is an individual resident vendor and has resided continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or,**

____ Bidder is a partnership, association or corporation resident vendor and has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; or 80% of the ownership interest of Bidder is held by another individual, partnership, association or corporation resident vendor who has maintained its headquarters or principal place of business continuously in West Virginia for four (4) years immediately preceding the date of this certification; **or,**

✓ Bidder is a nonresident vendor which has an affiliate or subsidiary which employs a minimum of one hundred state residents and which has maintained its headquarters or principal place of business within West Virginia continuously for the four (4) years immediately preceding the date of this certification; **or,**

2. **Application is made for 2.5% vendor preference for the reason checked:**

____ Bidder is a resident vendor who certifies that, during the life of the contract, on average at least 75% of the employees working on the project being bid are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

3. **Application is made for 2.5% vendor preference for the reason checked:**

✓ Bidder is a nonresident vendor employing a minimum of one hundred state residents or is a nonresident vendor with an affiliate or subsidiary which maintains its headquarters or principal place of business within West Virginia employing a minimum of one hundred state residents who certifies that, during the life of the contract, on average at least 75% of the employees or Bidder's affiliate's or subsidiary's employees are residents of West Virginia who have resided in the state continuously for the two years immediately preceding submission of this bid; **or,**

4. **Application is made for 5% vendor preference for the reason checked:**

✓ Bidder meets either the requirement of both subdivisions (1) and (2) or subdivision (1) and (3) as stated above; **or,**

5. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**

____ Bidder is an individual resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard and has resided in West Virginia continuously for the four years immediately preceding the date on which the bid is submitted; **or,**

6. **Application is made for 3.5% vendor preference who is a veteran for the reason checked:**

____ Bidder is a resident vendor who is a veteran of the United States armed forces, the reserves or the National Guard, if, for purposes of producing or distributing the commodities or completing the project which is the subject of the vendor's bid and continuously over the entire term of the project, on average at least seventy-five percent of the vendor's employees are residents of West Virginia who have resided in the state continuously for the two immediately preceding years.

7. **Application is made for preference as a non-resident small, women- and minority-owned business, in accordance with *West Virginia Code* §5A-3-59 and *West Virginia Code of State Rules*.**

____ Bidder has been or expects to be approved prior to contract award by the Purchasing Division as a certified small, women- and minority-owned business.

Bidder understands if the Secretary of Revenue determines that a Bidder receiving preference has failed to continue to meet the requirements for such preference, the Secretary may order the Director of Purchasing to: (a) reject the bid; or (b) assess a penalty against such Bidder in an amount not to exceed 5% of the bid amount and that such penalty will be paid to the contracting agency or deducted from any unpaid balance on the contract or purchase order.

By submission of this certificate, Bidder agrees to disclose any reasonably requested information to the Purchasing Division and authorizes the Department of Revenue to disclose to the Director of Purchasing appropriate information verifying that Bidder has paid the required business taxes, provided that such information does not contain the amounts of taxes paid nor any other information deemed by the Tax Commissioner to be confidential.

Under penalty of law for false swearing (West Virginia Code, §61-5-3), Bidder hereby certifies that this certificate is true and accurate in all respects; and that if a contract is issued to Bidder and if anything contained within this certificate changes during the term of the contract, Bidder will notify the Purchasing Division in writing immediately.

Bidder: Verizon Business Network Svcs Inc, on behalf of MCI Comm Svc Inc d/b/a Verizon Business Svcs **Signed:** Marsha K. Harrell

Date: 1/21/15 **Title:** Marsha K Harrell, Senior Consultant, Pricing/Contract Management

RFQ No. CPR1500000001

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

MANDATE: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE: Verizon Business Network Svc Inc, on behalf of MCI Communications Svc Inc

Vendor's Name: d/b/a Verizon Business Svcs

Authorized Signature: Marsha K. Harrell Date: 1/21/15

State of Mississippi

County of Warren, to-wit:

Taken, subscribed, and sworn to before me this 21st day of January, 2015.

My Commission expires 4/30/18, 20___.

AFFIX SEAL HERE

LYNNE MYERS
NOTARY PUBLIC
ID No. 80995
My Comm. Expires
Apr 30, 2018
WARREN COUNTY
STATE OF MISSISSIPPI

NOTARY PUBLIC Lynne Myers

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. 6
☑ Addendum No. 2	☐ Addendum No. 7
☐ Addendum No. 3	☐ Addendum No. 8
☐ Addendum No. 4	☐ Addendum No. 9
☐ Addendum No. 5	☐ 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.

Verizon Business Network Svc Inc., on behalf of MCI Communications Svc Inc d/b/a Verizon Business Svc
Company

Marsha K. Harrell
Authorized Signature

Marsha K Harrell
Senior Consultant
Pricing/Contract Management

1/21/15

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

CERTIFICATIONAND SIGNATURE PAGE

By signing below, or submitting documentation through wvOASIS, I certify that I have reviewed this Solicitation in its entirety; understand the requirements, terms and conditions, and other information contained herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

Verizon Business Network Svc Inc
on behalf of MCI Communications Svc Inc
d/b/a Verizon Business Svcs
(Company)

Marsha K. Harrell
(Authorized Signature) (Representative Name, Title)

Marsha K Harrell
Senior Consultant
Pricing/Contract Management

1/21/15

304 356 3393 / 304 356 3590
(Phone Number) (Fax Number) (Date)

Routing Code: PS
Contract ID #_____

PROFESSIONAL SERVICES
STATEMENT OF WORK NO. 1

Verizon Business Network Services Inc.	**West Virginia Consolidated Public Retirement Board**
22001 Loudoun County Parkway	**4101 MacCorkle Avenue, SE**
Ashburn, VA 20147	**Charleston, WV 25304**
By: Marsha K. Harrell	By: _____
Name: **Marsha K Harrell**	Name: _____
Title: Senior Consultant	Title: _____
Date: Pricing/Contract Management 1/21/15	Date: _____

This Statement of Work ("SOW") is a part of the agreement (the "Agreement"), identified by Contract Identification Number CPR1500000001 by and between Verizon Business Network Services Inc., on behalf of MCI Communications Services Inc., d/b/a Verizon Business Services ("Verizon") and State of West Virginia Consolidated Public Retirement Board.

1. **Description of Project.**

This SOW defines the professional services and Deliverables that Verizon will provide to Customer under the terms of the Agreement ("Project") and forms the basis for the pricing in the Rates and Charges section. Verizon will perform the Project at the locations identified herein. This SOW and the Agreement constitute the entire agreement between the parties with respect to the Project and supersedes all other prior or contemporaneous representations, understandings or agreements. Except as otherwise expressly stated herein, no amendment to this SOW is valid unless in writing and signed by both parties. The Project is limited to the services, Deliverables, documentation and conditions stated herein and in the Agreement.

2. **Description of Services.**

Verizon will provide the following services as further described below (collectively, the "Services"):

2.1 Threat & Vulnerability Professional Security Services, consisting of:

External Network Penetration Test
Internal Network Penetration Test
Host Configuration Review
Firewall Ruleset Review
Security Architecture Review
Penetration Testing Post Mortem

2.2 Data Loss Protection (DLP) Review, consisting of:

Prework
Validation
Solution Governance Review
Deployment
Operations Review
Subject Matter Expertise Consulting

3. **Scope of Work.**

3.1 **Description of Services**

3.1.1 **Threat & Vulnerability Professional Security Services**

Verizon will provide Threat & Vulnerability Professional Security Services as further described below.

3.1.1.1 **External Network Penetration Test**

Verizon will perform an External Network Penetration Test with the objective to identify and exploit network and host based security vulnerabilities on Customer's externally facing (internet accessible) networked infrastructures, which may include systems Customer has identified as containing important information, and/or systems Customer has identified which provide a Customer presence, process orders, or facilitate sensitive communications. Verizon will use a variety of proprietary, freeware, and commercial tools and techniques to perform the test, based on industry-specific guidance, best practices and standards. The External Network Penetration Test consists of the following significant phases:

- **Active host identification (device discovery) -** Verizon will establish a profile of Customer provided Internet Protocol ("IP") subnets to identify the active devices within those subnets.
- **Vulnerability Scanning -** Verizon will analyze available network services and the IP stack fingerprints of active devices identified.
- **Vulnerability Validation -** Verizon will attempt to validate the results of vulnerability scanning in order to identify (and disregard) false-positive results and validate other positive results from automated testing.
- **Exploitation -** Once an understanding of devices roles, potential trust relationships, accessible network services and potential vulnerabilities is established, Verizon will attempt to gain access to target systems.
- **Application Specific Penetration Tests –** In addition to the network penetration tests, Verizon will perform application security testing of the Customer's applications through unauthenticated and automated web application scanning. Some of the testing techniques include (where applicable):
  - *Input validation bypass* – Client side validation routines and bounds-checking restrictions are removed to confirm controls are implemented on application parameters sent to the server.
  - *SQL injection* – Specially crafted SQL commands are submitted in input fields to validate input controls are in place to properly protect database data.
  - *Cross-site scripting* – Active content is submitted to the application in an attempt to cause a user's web browser to execute unauthorized and unfiltered code. This test is meant to validate user input controls.
  - *Parameter tampering* - Query strings, POST parameters, and hidden fields are modified in an attempt to gain unauthorized access to user data or application functionality.
  - *Cookie poisoning* – Data sent in cookies is modified in order to test application response to receiving unexpected cookie values.
  - *User privilege escalation* – Verizon attempts to gain unauthorized access to administrator or other users' privileges.
  - *Credential manipulation* – Verizon modifies identification and authorization credentials in an attempt to gain unauthorized access to other users' data and application functionality.
  - *Forceful browsing* – Verizon enumerates files located on a web server in an attempt to access files and user data not explicitly shown to the user within the application interface.
  - *Backdoors and debug options* – Many applications contain code left by developers for debugging purposes. Debugging code typically runs with a higher level of access, making

it a target for potential exploitation. Application developers may leave backdoors in their code. Verizon will identify these options that could potentially allow an intruder to gain additional levels of access.

- *Configuration subversion* – Improperly configured web servers and application servers are common attack vectors. Verizon assesses the software features, as well as the Customer's application and server configuration for poor configurations.

Verizon will perform the External Network Penetration Test in five (5) assessments. The scope of each assessment is as follows:

Assessment 1: up to ten (10) active devices within one (1) Class 'C' subnets or equivalent IP address space and up to five (5) unauthenticated web applications.

Assessment 2: up to twenty (20) active devices within two (2) Class 'C' subnets or equivalent IP address space and up to five (5) unauthenticated web applications..

Assessment 3: up to fifty (50) active devices within two (2) Class 'C' subnets or equivalent IP address space and up to five (5) unauthenticated web applications.

Assessment 4: up to fifty (50) active devices within two (2) Class 'C' subnets or equivalent IP address space and up to five (5) unauthenticated web applications.

Assessment 5: up to fifty (50) active devices within two (2) Class 'C' subnets or equivalent IP address space and up to five (5) unauthenticated web applications.

For purposes of this SOW, the term "device" also refers to the functional equivalent of a device, so that the assessment of two distinct and different device-equivalents associated with a single piece of hardware will be counted as the assessment of two devices.

3.1.1.2 **Internal Network Penetration Test**

Verizon will perform an External Network Penetration Test with the objective to identify and exploit network and host based security vulnerabilities within the Customer's internal networked infrastructures, which may include systems Customer has identified as containing important information, and/or systems Customer has identified which provide a Customer presence, process orders, or facilitate sensitive communications. Verizon will use a variety of proprietary, freeware, and commercial tools and techniques to perform the test, based on industry-specific guidance, best practices and standards. The Internal Network Penetration Test consists of the following significant phases:

- **Active host identification (device discovery) -** Verizon will establish a profile of Customers provided Internal accessible Internet Protocol ("IP") subnets to identify the active devices within those subnets.
- **Vulnerability Scanning -** Verizon will analyze available network services and the IP stack fingerprints of active devices identified.
- **Vulnerability Validation -** Verizon will attempt to validate the results of vulnerability scanning in order to identify (and disregard) false-positive results and validate other positive results from automated testing.
- **Exploitation -** Once an understanding of devices roles, potential trust relationships, accessible network services and potential vulnerabilities is established, Verizon will attempt to gain access to target systems.
- **Application Specific Penetration Tests –** In addition to the network penetration tests, Verizon will perform application security testing of the Customer's applications through unauthenticated and automated web application scanning. Some of the testing techniques include (where applicable):

- *Input validation bypass* – Client side validation routines and bounds-checking restrictions are removed to confirm controls are implemented on application parameters sent to the server.
- *SQL injection* – Specially crafted SQL commands are submitted in input fields to validate input controls are in place to properly protect database data.
- *Cross-site scripting* – Active content is submitted to the application in an attempt to cause a user's web browser to execute unauthorized and unfiltered code. This test is meant to validate user input controls.
- *Parameter tampering* - Query strings, POST parameters, and hidden fields are modified in an attempt to gain unauthorized access to user data or application functionality.
- *Cookie poisoning* – Data sent in cookies is modified in order to test application response to receiving unexpected cookie values.
- *User privilege escalation* – Verizon attempts to gain unauthorized access to administrator or other users' privileges.
- *Credential manipulation* – Verizon modifies identification and authorization credentials in an attempt to gain unauthorized access to other users' data and application functionality.
- *Forceful browsing* – Verizon enumerates files located on a web server in an attempt to access files and user data not explicitly shown to the user within the application interface.
- *Backdoors and debug options* – Many applications contain code left by developers for debugging purposes. Debugging code typically runs with a higher level of access, making it a target for potential exploitation. Application developers may leave backdoors in their code. Verizon will identify these options that could potentially allow an intruder to gain additional levels of access.
- *Configuration subversion* – Improperly configured web servers and application servers are common attack vectors. Verizon assesses the software features, as well as the Customer's application and server configuration for poor configurations.

Verizon will perform the Internal Network Penetration Test in five (5) assessments. The scope of each assessment is as follows:

Assessment 1: up to fifty (50) active devices from up to two (2) physical Customer location from which Verizon will have direct IP connectivity to all active devices in scope.

Assessment 2: up to one hundred (100) active devices from up to two (2) physical Customer location from which Verizon will have direct IP connectivity to all active devices in scope.

Assessment 3: up to one hundred (100) active devices from up to two (2) physical Customer location from which Verizon will have direct IP connectivity to all active devices in scope.

Assessment 4: up to one hundred (100) active devices from up to two (2) physical Customer location from which Verizon will have direct IP connectivity to all active devices in scope.

Assessment 5: up to one hundred (100) active devices from up to two (2) physical Customer location from which Verizon will have direct IP connectivity to all active devices in scope.

3.1.1.3 **Host Configuration Review**

Verizon will perform a Host Configuration Review to identify security weaknesses in Customer's server configurations. The Host Configuration Review consists of manual review of system configurations and interviews with key personnel who manage the systems.

The Host Configuration Review consists of automated scanning in two phases:

- network-based, unauthenticated scanning to determine the network footprint (if necessary),
- local, authenticated tests to determine patch level, service version, and software libraries, or;
- An off-site configuration review for network and security devices based on a full configuration output.

Verizon will perform the Host Configuration Review in five (5) assessments. The scope of each assessment is as follows:

Assessment 1 will consist of examining a sampling of up to five (5) workstations and servers running Microsoft Windows or Linux operating systems.

Assessment 2 will consist of examining a sampling of up to ten (10) workstations and servers running Microsoft Windows or Linux operating systems.

Assessment 3 will consist of examining a sampling of up to ten (10) workstations and servers running Microsoft Windows or Linux operating systems.

Assessment 4 will consist of examining a sampling of up to ten (10) workstations and servers running Microsoft Windows or Linux operating systems.

Assessment 5 will consist of examining a sampling of up to ten (10) workstations and servers running Microsoft Windows or Linux operating systems.

3.1.1.4 **Firewall Ruleset Review**

Verizon will perform a Firewall Security Review to identify improper firewall rules and configurations. This review is performed using the following methodology.

Firewall Security Review Methodology

Firewall Security Review consists of determining the appropriate firewall policy that needs to be configured on a firewall, according to industry standard security practices as well as the type of services and access needed for operations.

The Verizon Firewall Security Review consists of three significant phases, as follows:

- **Phase I: Information Collection.** Verizon will gather information/documentation on each networked service that needs to traverse the firewalls, where possible.
- **Phase II: Analysis.** Verizon will review the firewall rules and configurations to identify weaknesses such as overly permissive or redundant rules. Additionally, Verizon will review the configuration of each firewall to identify insecure configurations.
- **Phase III: Reporting and Knowledge Transfer.** Verizon will provide documentation detailing the optimal firewall policy, i.e., the individual rules that permit the least amount of access without compromising service functionality. The documentation will contain information that can be used by the customer to make changes to the firewall policy based on the recommendations.

  Verizon will perform the Firewall Ruleset Review in five (5) assessments. The scope of each assessment is as follows:

  Assessment 1: review of up to two hundred fifty (250) access control entries on one (1) Cisco ASA 5505 firewall.

  Assessment 2: review of up to two hundred fifty (250) access control entries on one (1) Cisco ASA 5505 firewall.

  Assessment 3: review of up to two hundred fifty (250) access control entries on one (1) Cisco ASA 5505 firewall.

  Assessment 4: review of up to two hundred fifty (250) access control entries on one (1) Cisco ASA 5505 firewall.

Assessment 5: review of up to two hundred fifty (250) access control entries on one (1) Cisco ASA 5505 firewall.

3.1.1.5 **Security Architecture Review**

Verizon will perform a Security Architecture Review (SAR), consisting of a security analysis of the Customer's network design including a review of the type of current documentation, data flows, device placement, proper filtering and segmentation, intrusion detection and monitoring, encryption employed, interconnections with vendors and internet connections. The assessment consists of the following phases:

- **Information Gathering.** Verizon will obtain and examine documentation from the Customer including, design diagrams, network description, device placement, data flows, host information, security and network device types and configuration, and other documentation provided by Customer related to the environment to be assessed.

- **Configuration Review.** Verizon will perform a Configuration Review of a sampling of supporting infrastructure components and security devices, such as firewalls and routers, as determined by the Verizon consultant. This configuration review will focus on identifying security weaknesses in the Customer's networking and security equipment. The Configuration Review consists of manual review of network and security device configurations to identify improper access control rules and insecure configurations and (at Verizon's determination) interviews with key personnel who manage the systems.

- **Configuration Review.** Verizon may request a limited sampling of network and security device configurations to review the supporting infrastructure components and security devices, such as firewalls and routers, as necessary and determined by the Verizon consultant. This configuration review will focus on gaining an understanding of data flows, access control policies applied, address translation, IP schemas, and other information to aide in the consultants' understanding of the network and potentially identifying security weaknesses in the design.

- **Architectural - Design review.** Verizon will review Customer's design for possible weaknesses in the overall architecture. This typically includes:

    - Insecure protocols for communication
    - Monitoring and logging
    - Data flows
    - Segmentation and filtering
    - Security device placement
    - Perimeter security including VPN and other external connections
    - Tiered designs for external accessible environments
    - Defense in Depth
    - Insecure management access to equipment and logging

- **Stakeholder Interviews.** Once the documentation has been reviewed, Verizon will conduct interviews with the Customer stakeholders (as identified by Customer)to clarify architectural and configuration documentation. This part of the review consists of obtaining a better understanding of the history of the network and security decisions, critical components and data flows within the environment, and clarify any other areas where there are gaps in documentation or inconsistencies. This part of the assessment includes 'white board' sessions with Customer's technical personnel as well as other influences into the security design such as budgetary constraints, pending network and security equipment refreshes, and other potential constraints. Interviews can be performed remotely or on-site depending on the Customer's availability.

- **Reporting.** Once the documentation has been reviewed and interviews with stakeholders have taken place, Verizon will compile a report describing each of the security findings, their associated impact, and possible recommendations for the short and long term.

Verizon will perform the Security Architecture Review in five (5) assessments. The scope of each assessment is as follows:

Assessment 1: Verizon will perform the assessment for up to two (2) business days (inclusive of reporting) in which the assessment will be performed remotely and potentially from one (1) Customer location as needed.

Assessment 2: Verizon will perform the assessment for up to two (2) business days (inclusive of reporting) in which the assessment will be performed remotely and potentially from one (1) Customer location as needed.

Assessment 3: Verizon will perform the assessment for up to five (5) business days (inclusive of reporting) in which the assessment will be performed remotely and potentially from one (1) Customer location as needed.

Assessment 4: Verizon will perform the assessment for up to five (5) business days (inclusive of reporting) in which the assessment will be performed remotely and potentially from one (1) Customer location as needed.

Assessment 5: Verizon will perform the assessment for up to five (5) business days (inclusive of reporting) in which the assessment will be performed remotely and potentially from one (1) Customer location as needed.

3.1.1.6 **Penetration Testing Post-Mortem**

Verizon will perform Threat & Vulnerability Consulting, which consists of providing a post-mortem security analysis of the Customer's detection and response capabilities to the Services provided by Verizon.

The assessment consists of the following phases:

- **Information Gathering.** Verizon will obtain and examine documentation from Customer related to the Services that were performed and Customer's capabilities to detect and respond. Customer will provide a report detailing which alerts and potential attacks were detected, which response actions were performed, and their capabilities to prevent the attack.

- **Review and Analyze.** Verizon will analyze the timeline of events Customer provides and compare this to the actual attack events such as scanning timeframes, attempted exploitation, successful compromises, and post exploitation activities to determine the extent Customer was able to detect and prevent these attacks.

- **Stakeholder Interviews (as necessary).** Once the documentation has been reviewed and compared to the attack scenarios from the internal and external penetration testing, interviews with the necessary Customer stakeholders may be held to clarify any questions on the provided documentation.

- **Reporting.** Once Customer-provided documentation has been reviewed and interviews with stakeholders have taken place Verizon will compile a report describing the different testing phases (discovery, scanning, exploitation, post exploitation) from the external and internal assessments, Customer's detection capabilities, as well as the effectiveness of the response to these activities. In addition, Verizon will provide a maturity ranking on the Customer's overall response capabilities, based on the information provided from Customer. The ranking will be on a scale from one (1) to five (5) whereas a 1 is undocumented or 'unaware' of an attack to a level of 5 which is a very mature program with effective or 'complete' response capabilities.

Verizon will perform the Penetration Testing Post Mortem in five (5) assessments. The scope of each assessment will constitute up to forty (40) consultant hours of time performing the above phases. Verizon will conduct the Penetration Testing Post Mortem remotely from a Verizon location in the United States.

3.1.2 **Data Loss Protection (DLP) Review**

Verizon will perform a Data Loss Protection (DLP) Review consisting of six (6) distinct tracks, as further described below.

3.1.2.1 **Track 0: Pre-Work**

During Track 0, Verizon and Customer will formally define program governance, escalation paths, and program checkpoints.

Verizon will provide a preparatory document containing a document and preliminary hardware and software checklist, and. Customer will provide pertinent policy documents as well as any previously generated program documentation for Verizon review prior to arrival on-site.

3.1.2.2 **Track 1: Validation**

During Track 1, Verizon will commence formal program delivery and tasks designed to understand and validate Customer's data protection use-cases and derive associated requirements for discovery or control within Customer tool and capabilities.

3.1.2.3 **Track 2: Solution Governance Review**

During Track 2, the Verizon DLP analyst will review the Customer's current DLP hierarchy against customer objectives, common industry practices, and Verizon's recommended state for Customer.

The Verizon DLP analyst will also review Customer's current DLP rule creation process, and determine the extent to which to determine the Customer's governance of DLP rule creation is documented and controlled, from initial request thru rule creation, testing, deployment and periodic evaluation.

The Verizon DLP analyst will also assess whether Customer's incident response process is clearly defined and authorized in accordance with Customer's policies.

The Verizon DLP Analyst will review DLP communications and training materials throughout the organization. Training and communications will be reviewed for executive, user base, help desk, DLP personnel, and enterprise wide notifications.

Where appropriate, the Verizon DLP analyst will provide written recommendations regarding potential improvements by Customer to Customer's DLP hierarchy, incident response process, communications, and training materials.

3.1.2.4 **Track 3: Deployment**

Verizon will not do a detailed component by component installation review; however the Verizon DLP analyst will coordinate and conduct validation of installation documentation, repeatability, and auditability. This will include up to three environments such as test, User Acceptance ("UAT"), and production environments. This includes all vectors of DLP.

Installation will be reviewed as stated above and for the current deployment's ability to meet use cases.

3.1.2.5 **Track 4: Operations Review**

Verizon will conduct a review of Customer's DLP console configuration and management functions. The review will include user and role creation, rule and report creation and management, scheduled and unscheduled operational tasks, workflow creation and effectiveness, backup and restore functionality, and health and status checking.

3.1.2.6 **Track 5: Subject Matter Expertise Consulting**

In addition to Tracks one thru five, Verizon will provide general subject matter expertise and consultative services related to DLP and other data protection technologies in the form of verbal communications, email, and white boarding. These services will be provided as mutually agreed during the term of the Project.

3.2 **Service Time and Customer Locations.**

3.2.1 **Service Times**

The Services will be conducted during mutually agreed upon times between Verizon and the Customer.

3.2.2 **Customer Locations: Threat & Vulnerability Professional Security Services**

The External Network Penetration Test and Penetration Testing Post-Mortem will take place from the following Verizon location in the United States:

22001 Loudoun County Parkway, Ashburn, VA 20147

The remaining services will take place from the following Customer locations:

4101 MacCorkle Av SE, Charleston, WV 25304
1900 Kanawha Blvd E, Charleston, WV 25305

3.2.3 **Customer Locations: Data Loss Protection Review**

The Data Loss Protection Review services will be performed at locations to be agreed between Verizon and Customer.

3.3 **Project Management**

Verizon will designate an engagement manager, who will be responsible for the performance of the Project, the schedule and the budget. The engagement manager will also manage the change control process.

Verizon will also work with designated personnel to develop a project plan that specifies resources, dates, times, and locations for the tasks described. Verizon will obtain a final approval of the project plan prior to proceeding with project activities.

Customer will appoint a Single Point of Contact / Program Management team for co-ordination of the project activities for interaction with Verizon and ensuring smooth data flow and exchange of information required for execution of the project within the time-frame.

4. **Deliverables and Documentation to be produced by Verizon.**

4.1 **Threat & Vulnerability Professional Security Services**

Verizon will provide a report of findings that outlines discovered vulnerabilities in order of severity (the "Report"). Each finding will include a discussion of the vulnerability and the potential security impact to Customer's network, as well as recommended remediation steps. Screen shots and log excerpts may be included, if applicable.

The Report will include an Executive Summary, which contains an analysis of the results of the Services. Findings will be discussed, and graphs and charts will break down findings by severity and difficulty, as well as by root cause. If the network has been assessed previously by Verizon, a trend analysis will be included, with a graphic of progress in securing the network. The results and security posture of the network are analyzed, with recommendations for remediation of vulnerabilities, policy, procedures and governance and proactively preventing future network security issues.

The contents of the provided written Report and findings will also be communicated to the Customer remotely via telephone. An onsite presentation of the material to Customer may be requested at an additional cost.

Any Verizon report(s) are intended for Customer and Verizon use only. Customer may disclose a deliverable to a third party as long as such third party is subject to a written nondisclosure agreement, requiring such third party to maintain the confidentiality of such deliverable and use such deliverable only for the benefit of the internal business purposes of Customer. Customer shall be responsible for breaches of such confidentiality agreement by such third party.

4.2 **Data Loss Protection Review**

Verizon will provide a DLP engagement summary and recommendations document which discusses:

- Current State
  - Current use-cases
  - Current operations
  - Current documentation, communications, and training levels
- Recommended State
  - Target intermediate state and final state objectives
  - Recommended use cases
  - Currently achievable recommendations
  - Alternate paths with current capabilities
  - New technical or operational recommendations
- Next Steps
- Summary

5. **Documentation to be produced by Customer and Customer Obligations.**

Successful delivery of the Services by Verizon is dependent on Customer's performance of the following tasks:

5.1 **General**

Access to the systems, applications, and Customer contacts must be available to Verizon during designated time frames, which will be established during the project kick-off meeting. Customer's failure to provide this timely access could delay completion of the Services.

Customer will make available all necessary personnel to Verizon during the period of performance. Customer understands that the following must be provided to Verizon, seventy-two (72) hours or more prior to the scheduled commencement of the Services.

- A list of appropriate contact personnel with "after hours" emergency contacts numbers.
- Addresses of, and appropriate access to any networked devices to be tested within the scope of the Services.

- Appropriate on-site authorization documentation (where applicable).

When requested by Verizon, Customer shall provide review and feedback on documents within three business days or as otherwise agreed.

5.2 **Additional Requirements for Threat & Vulnerability Professional Security Services**

Customer shall notify appropriate Business Partner(s) (as defined below) of testing at the Business Partner site (including where testing is conducted via remote access to the Business Partner site), at least seventy-two (72) hours or more prior to the scheduled commencement of the testing.

Third Party Locations: In the event Customer requests that Verizon perform the Services at Customer's third party business partner ("Business Partner") site (including via remote access to the site), Customer hereby represents and warrants that prior to Verizon's commencement of Services hereunder, such Business Partner provided Customer authorization to engage Verizon to perform the Services at such Business Partner's location (including via remote access to the location). Customer shall at its expense defend and indemnify Verizon through and in the amount of final judgment or settlement of any claim, suit or other demand asserted against Verizon by Customer's Business Partner alleging that Verizon had no authority to perform the Services at such Business Partner's site.

5.3 **Additional Requirements for Data Loss Protection Review**

Customer shall provide:

- All documentation associated with Customer owned DLP systems
- Previously generated program documents
- Existing processes, procedures and policies that may be relevant to the operation of the Customer's DLP installation
- Access to Customer's support contacts within DLP Vendor
- Customer personnel to provide hands on access to scanning systems for configuration or scanning status checks as necessary at all locations

6. **Assumptions.**

Delivery of the Services by Verizon is predicated on the following assumptions:

- The Services are based on Verizon's understanding of Customer's requirements. Should the scope of the project change, then Verizon will provide Customer with a new estimate via change control and will continue work, subject to availability of personnel, only after receiving written authorization from Customer.
- The Services will be provided only during Business Hours unless otherwise agreed by the parties. Provision of the Services outside of Business Hours may be subject to additional costs, to be defined in an amendment to this Statement of Work. For the purposes of this SOW, "Business Hours" are defined as the hours between 9am and 5pm from Monday through Friday, excluding Saturdays, Sundays and public or generally observed holidays at Verizon offices and/or the locale where services are to be provided.

7. **Rates and Charges.**

7.1 **Threat & Vulnerability Professional Security Services.**

The Threat & Vulnerability Professional Security Services will be provided on a Fixed Price basis for the Fees below:

Service	Customer Location(s)	Fixed Price
		$56,950

Assessment 1: External Network Penetration Test Internal Network Penetration Test Host Configuration Review Firewall Ruleset Review Security Architecture Review Penetration Testing Post-Mortem The Data Loss Prevention Review Services will be provided on a Fixed Price basis billed in arrears upon completion of the assessment.	*Services to be performed remotely from a Verizon location in the United States.* *Portions to be performed at Customer addresses in Section 1.3.*	$68,500
Assessment 2: External Network Penetration Test Internal Network Penetration Test Host Configuration Review Firewall Ruleset Review Security Architecture Review Penetration Testing Post-Mortem	*Services to be performed remotely from a Verizon location in the United States.* *Portions to be performed at Customer addresses in Section 1.3.*	$56,950
Assessment 3: External Network Penetration Test Internal Network Penetration Test Host Configuration Review Firewall Ruleset Review Security Architecture Review Penetration Testing Post-Mortem	*Services to be performed remotely from a Verizon location in the United States.* *Portions to be performed at Customer addresses in Section 1.3.*	$72,780
Assessment 4: External Network Penetration Test Internal Network Penetration Test	*Services to be performed remotely from a Verizon location in the United States.* *Portions to be performed at Customer addresses in Section 1.3.*	$72,780

Host Configuration Review Firewall Ruleset Review Security Architecture Review Penetration Testing Post-Mortem		
Assessment 5: External Network Penetration Test Internal Network Penetration Test Host Configuration Review Firewall Ruleset Review Security Architecture Review Penetration Testing Post-Mortem	*Services to be performed remotely from a Verizon location in the United States.* *Portions to be performed at Customer addresses in Section 1.3.*	$72,780
SERVICE TOTAL		**$400,740**

Verizon will invoice Customer in arrears upon the completion of each Assessment as shown in the table above.

7.3 **Expenses.**

The Services provided herein may be subject to tax, which will be billed separately , exempt customer will be expected to provide tax exemption form.

There are no additional charges for travel, lodging and other associated expenses for the Threat & Vulnerability Professional Security Services.

For the Data Loss Protection Review services, any services outside the scope of this SOW will be handled on a change order request and agreed to by both parties.

7.4 **Purchase Order.**

Customer shall indicate below as to whether or not its internal procedures require the issuance of a purchase order ("Purchase Order" or "PO") to process invoices and/or payment. If neither option is marked by Customer, Customer confirms that a Purchase Order is NOT required:

_____Yes (If yes, a copy of the PO is required at the time of signature)

Purchase Order #

_____No (If no, please provide invoice address below):

Invoice Address
Company:
Name:

Address:
City/State/Zip:

Verizon's acceptance of a Customer PO is for the sole purpose of facilitating Customer's payment procedures. All Services furnished in conjunction with a PO shall be governed solely by the terms and conditions of the Agreement, the PSA and this SOW (together, the "Contract"). The terms of the Contract shall supersede and replace any terms and conditions contained in the PO and such terms and conditions shall not modify the Contract and shall not be binding on Verizon.

8. **Term of SOW.**

Contract becomes effective on award and extends for a period of two years. Contract may be renewed upon mutual written consent of the Agency, and the Vendor, with approval of the Purchasing Division and the Attorney General's office. Any request for renewal should be 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. Renewal of the Contract is limited to four (4) successive one (1) year periods or multiple renewal periods of less than one year, provided that the multiple renewal periods do not exceed 48 months in total. Automatic renewal of this Contract is prohibited.

9. **Validity of this SOW.**

Pricing and/ or promotional benefits in this SOW may not be available unless it is signed and delivered to Verizon prior to April 1, 2015.

VERIZON
PROFESSIONAL SERVICES ATTACHMENT

Routing Code: PS

PROVISIONS APPLICABLE TO ALL PROFESSIONAL SERVICES:

1. **Scope of Services.**

1.1 **Service Provider.** The products and services under this services attachment ("Service Attachment") and related Statements of Work ("SOW") and service order forms ("SOF") are provided by the entities indicated in the applicable SOF (referred to herein, individually and collectively, as "Verizon") except as otherwise explicitly noted. References to Verizon in this Agreement include all Verizon agents and contractors providing services hereunder.

1.2 **Professional Services.** Verizon will provide the technical and consultative services, as well as deliver any reports or other deliverables (collectively, "Deliverables"), specified in the applicable SOW and related SOF and agreed to under this Service Attachment. Such services and Deliverables are collectively referred to in this Service Attachment as the "Professional Services". The Professional Services under a particular SOW are referred to as a "Project".

1.3 **SOW and Terms and Conditions.** The SOW, as supplemented by this Service Attachment, and the master services agreement (which may be a Verizon Service Agreement, an International Master Services Agreement, Worldwide Services Agreement, Security Services Agreement, Asia Pacific Services Agreement, or other form of Verizon master services agreement) ("Master Terms") of which it is a part, sets forth the terms and conditions for each Project (collectively, the "Agreement"). To the extent there is any conflict between a SOW, the Service Attachment and the Master Terms, the order of precedence is: (a) Service Attachment, (b) Master Terms and (c) SOW. All SOWs must be in writing, be accompanied by an SOF signed by an authorized representative of each party, and refer to the Agreement by number or by title and date.

1.4 **Conditions.** A SOW may identify assumptions, expectations and dependencies on which the SOW is based ("Conditions"). Each Party will notify the other promptly if it determines that a Condition has not been met or is unlikely to be met. If Verizon reasonably determines that the failure of a Condition to be met has adversely impacted Verizon's likely costs, required effort, timelines or other any aspect of the performance of the Professional Services and delivery of the Deliverables, and Verizon proposes a SOW amendment to cure it, the parties will work diligently to reach agreement on a SOW amendment to cure the impact on Verizon, and, without limiting any other Verizon right or remedy under this Agreement or at law, Verizon may suspend work on the Project until the parties have reached that agreement. The preceding sentence does not apply if Verizon reasonably could have caused the Condition to be met but did not.

1.5 **Amendments to SOW.**

1.5.1 Either party may propose an amendment to a SOW by submitting a written request for a change to the other party's project manager. All written submissions proposing an amendment may be by email.

1.5.2 Verizon will document the request for change via a formal project change request, which will set forth the terms and conditions for the changes requested.

1.5.3 If Customer agrees in writing to the project change request and authorised representatives of both the Customer and Verizon execute the formal change request, then the SOW is thereby deemed amended by the change request and both parties will perform their obligations under the SOW as amended.

1.6 **Performance.** Verizon controls the means, methods, places and time of its performance of the Professional Services (including the use of subcontractors and consultants). While working on a Customer site, Verizon will abide by Customer's stated security rules for the site provided those rules

are provided to Verizon in advance of any site visits. Except as stated otherwise in a SOW, each Deliverable and the Professional Services altogether are deemed accepted and complete upon the earlier of either: (a) use by Customer, or (b) 5 days after delivery/performance unless Customer promptly demonstrates to the reasonable satisfaction of Verizon that the Deliverable or Professional Services altogether (as applicable) fails to meet the acceptance criteria in SOW (if any) or the requirements of the Agreement.

2. **Customer Obligations.**

2.1 **Assistance.** Customer agrees to provide working space and facilities and any other assistance and support that Verizon may reasonably request in order to perform the Professional Services. Without limiting the foregoing, Customer will (a) make any systems to be tested as part of the Professional Services available through the duration of the testing period; (b) ensure that any systems to be tested will have normal operating throughput; (c) make any systems to be tested available from the Internet, or provide alternative means of connectivity to the Verizon testing location; (d) provide all systems, policy, process and other documentation reasonably requested; (e) make available all necessary personnel (including Customer customers, business partners, and vendors, as appropriate) to Verizon during the period of performance; (f) provide Verizon with a list of appropriate contact personnel including after-hours emergency contact numbers, if requested; and (f) participate in meetings requested by Verizon as may be reasonably required to perform the Professional Services. Customer shall comply with all other obligations set forth in the Agreement. Without limiting any other Verizon right or remedy under this Agreement or at law, Verizon is excused from any failure or delay resulting from Customer's failure to fulfill its obligations under the Agreement in a timely manner.

2.2 **Authority to Permit Professional Services.** Customer represents and warrants that: (a) it has and will continue to have full rights, power, and authority to consent to having the Professional Services provided in the manner as agreed upon in the SOW; (b) it has obtained in writing all consents, approvals and licenses necessary from any third party to allow Verizon to provide the Professional Services in the manner as agreed in the SOW; and (c) it will use the Professional Services for lawful purposes only. Customer agrees to indemnify, defend and hold harmless Verizon from any loss, damages, liabilities, costs and expenses (including reasonable attorneys' fees and expenses and those of other professionals) incurred by Verizon as a direct or indirect result of Customer's breach of the foregoing representation and warranty.

3. **Term.** An SOW will automatically expire upon completion of the Project or upon reaching the end of the contract term as indicated in the SOF, whichever comes first. Either party may terminate a SOW (even before it is completed) according to the same terms under which the Agreement could be terminated, except to the extent the SOW states otherwise. Upon termination of a SOW or the Agreement for any reason, each party will promptly return to the other all copies of any data, records, or materials of whatever nature or kind, owned by the other party (or its subcontractors, consultants, or suppliers). Verizon also will furnish to Customer any Customer-owned work in progress for which payment has been received. Verizon may terminate a SOW if the parties have not agreed on a proposed SOW amendment to cure the impact on Verizon from an unmet Condition within 45 days of Verizon providing the applicable project change request to Customer. Without limiting any other Verizon right or remedy under this Agreement or at law, if a SOW is terminated by Customer for any reason other than Cause or by Verizon for Cause or pursuant to this Section 3, Customer agrees to pay Verizon: (a) all accrued but unpaid charges incurred through the date of such termination; and (b) an amount equal to seventy five per cent (75%) of any remaining fixed charges under the SOW. Customer acknowledges any payment to be made pursuant to the preceding sentence is a genuine pre-estimate of the loss suffered by Verizon as a result of the early termination of the SOW and not a penalty and will become due and payable by Customer immediately upon receipt of an invoice.

4. **Rates and Charges.** Verizon will submit invoices to Customer for amounts due under the SOW as shown in a SOF. Payment terms may include recurring, nonrecurring, work time (per hour), materials, travel, lodging, shipping, handling, insurance and other charges, as provided in the SOW.

1 4.1 **Purchase Orders.** If Customer indicates on the SOF that a purchase order is required, Customer must issue such purchase order to Verizon on or before the Customer signature date shown on the SOW. However, if the SOF is properly executed, but no purchase order is issued as provided above, Verizon is authorized to proceed with invoicing of any amounts due under the

relevant SOF, and Customer shall pay the same, without the need for, or reference to, the purchase order. In any case, the terms and conditions of the Agreement will solely govern the Professional Services and the terms and conditions of Customer's purchase order or similar document have no force or effect except for provisions evidencing an intent to be bound by the terms and conditions of an agreement between Customer and Verizon. Customer must address its purchase order to the Verizon Legal Entity named above.

2 4.2 **Invoicing and Payment.** Verizon will invoice Customer in accordance with the SOF and Customer will pay all invoiced amounts in accordance with the Agreement.

3 4.3 **Expenses**. Subject to compliance with Customer's normal and customary policies regarding substantiation and verification of business expenses, travel and expense is incorporated into the Professional Services rate.

5. **Confidentiality.** Verizon may disclose Confidential Information to subcontractors and consultants for the purpose of performing the Professional Services.

6. **Customer's Use of Deliverables.**

6.1 **License to use Deliverables.** Verizon grants to Customer a non-exclusive, nontransferable, license to use any Deliverables solely for Customer's internal business purposes during the term of any related Verizon service, including the right to make a reasonable number of copies of such Deliverables, if applicable, except as otherwise agreed to in a SOW.

6.2 **Ownership and Confidentiality of Deliverables.** As between Verizon and Customer, all right, title and interest in any Deliverable is owned by Verizon and both the Deliverable and any information, materials, methodologies or know-how used by Verizon in connection with any Deliverable, is the Confidential Information of Verizon, except for (a) any Customer-owned information or materials that pre-existed the signing of the applicable SOF, and (b) as otherwise agreed to in a SOW.

6.3 **Verizon Reservation of Rights.** Except as expressly granted herein, Customer receives no ownership, license, or other interest in any intellectual property or proprietary information created or delivered by Verizon, whether in connection with its performance of this Agreement or otherwise.

7. **Warranties and Disclaimers.**

7.1 **Verizon Warranty.** Verizon warrants that it will perform each Project in a good and workmanlike manner substantially in accordance with accepted industry standards, and that any Deliverables will comply with the specifications agreed to by the parties in a SOW.

7.2 **Customer Warranty.** Customer warrants that it owns all right, title, and interest in and to, or has the license for and the right to grant Verizon access to, any programs, systems, data, materials, IP addresses, domains or other information furnished by Customer to Verizon for the purpose of enabling Verizon to perform the Professional Services. Customer hereby assumes the sole responsibility for the accuracy of the IP addresses, domains, programs, systems, data, materials or other information furnished by Customer to Verizon.

7.3 **Verizon's Disclaimer of Warranties.** Without limiting anything else in this Service Attachment, the disclaimer of warranties in the Master Terms applies to this Service Attachment. Any Verizon warranty applies to Customer only.

8. **Intellectual Property Infringement Indemnity.**

8.1 **Verizon Service Indemnity.** Verizon will at its expense defend Customer, through final judgment or settlement against all third party claims, actions, or suits asserted against Customer alleging that any Professional Service as furnished by Verizon infringes a third party's rights under any United States patent, copyright, trademark, or trade secret ("Verizon Service Infringement Claims"). Verizon will

indemnify and hold Customer harmless for damages, costs, and expenses, including reasonable attorneys' fees, finally awarded against Customer for such Verizon Service Infringement Claims or amounts agreed to by Verizon in settlement of Verizon Service Infringement Claims.

8.2 **Exceptions and Cross Indemnity.** Verizon is under no obligation to defend, indemnify, or hold Customer harmless to the extent that a third party claim, action or suit arises out of or relates to: (i) Verizon's compliance with Customer's specifications; (ii) a combination of any Professional Service by or on behalf of Customer with products, services, or other information or materials not provided by Verizon; (iii) a modification of any Deliverable by or on behalf of Customer by anyone other than Verizon or its authorized agents; (iv) a use or operation of one or more of the Deliverables by or on behalf of Customer that is inconsistent with this Agreement or Verizon's written instructions; or (v) information, data, or other content provided by or on behalf of Customer and not provided by Verizon. To the extent that a third party claim, action or suit arising out of (a) one or more conditions stated in Subsection 8.2.(i) through (v) or (b) claims for libel, slander, invasion of privacy, or other torts based on the content transmitted by or for Customer, is asserted against Verizon "Customer Infringement Claims"), Customer shall at its expense defend Verizon and indemnify and hold Verizon harmless for damages, costs, and expenses, including reasonable attorneys' fees, finally awarded against Verizon for such Customer Infringement Claims or amounts agreed to by Customer in settlement of Customer Infringement Claims.

8.3 **License, Modification, Replacement, and Termination of Infringing Service.** With respect to any pending or threatened Verizon Service Infringement Claim, Verizon may in its discretion and at its own expense obtain for Customer the right to continue using the affected Professional Service or alternatively replace or modify the affected Professional Service, so that it is functionally equivalent but non-infringing. If achievement of the foregoing is not commercially reasonable, Verizon may, in its sole discretion, terminate the affected Professional Service, without liability of either party to the other for such termination, except for Customer's obligation to pay all charges for the affected Professional Service incurred up to the time of such termination.

8.4 **Exclusive Remedy.** This Section 8 provides the sole remedies of Customer and the exclusive obligations of Verizon in connection with any third party claim, action, suit or other demand asserted against Customer described in this Section 8 or which otherwise asserts a violation of a third party's intellectual property rights, and Verizon disclaims all other warranties and obligations with respect thereto.

8.5 **Notice, Cooperation and Control.** The indemnifying party under Sections 8.1 or 8.2 is excused from its obligations under the applicable section if the indemnified party fails to (i) provide prompt written notice of the third party claim, action, or suit to the indemnifying party, provided that the failure of the indemnified party to provide such notice materially prejudices the indemnifying party's defense and/or settlement of such claim, action or suit; (ii) cooperate with all reasonable requests of the indemnifying party in connection with the defense and/or settlement of such claim, action or suit, at the indemnifying party's reasonable expense; and/or (iii) surrender exclusive control to the indemnifying party of the defense and/or settlement of such claim, action, or suit.

8.6 **Consent to Settlement.** The indemnifying party under Sections 8.1 or 8.2 shall secure the prior consent of the indemnified party before settling any claim, suit, or action that includes an admission of liability by the indemnified party or imposes material obligations on the indemnified party other than cessation of infringing activity and/or permitting Verizon removal of the infringing Professional Service, confidential treatment of the settlement, and/or payment of money that is fully indemnified by the indemnifying party under Sections 8.1 or 8.2. The indemnified party shall not unreasonably withhold or delay consent.

9. **Limitation of Liability.**

9.1 **Third Party Products and Services.** Verizon may direct Customer to third parties having products or services which may be of interest to Customer for use in conjunction with the Professional Services. Notwithstanding any Verizon recommendation, referral or introduction, Customer will independently investigate and test third-party products and services and will have sole responsibility for determining suitability for use of third-party products and services, and for any contracts Customer enters into with third parties. Verizon has no liability with respect to claims related to or arising from use of third-party

products and services. This provision does not apply to the work of subcontractors or other agents that is done on Verizon's behalf.

9.2 **Disclaimer of Liability.** Without limiting the liability disclaimers in the Master Terms, Verizon is not liable for any loss of or damage to Customer data. Customer is responsible for backing up all data.

9.3 **Extent of Verizon's Liability.** Without limiting the liability disclaimers in the preceding subsection and the Master Terms, the total liability of Verizon to Customer may not exceed the lesser of (a) direct damages proven by the moving Party or (b) the aggregate amounts due from Customer to Verizon under the Agreement for the 6 month period prior to accrual of the claim for the portion of the Professional Service which forms the basis for such claim, except that this limitation does not apply to actual, direct damages to real property or tangible personal property or for personal injury or death, resulting from Verizon's negligence or willful misconduct. Under no circumstances will either party be liable for damages that could have been avoided by the other party's exercise of reasonable diligence. No cause of action, howsoever arising, which accrued more than 1 year prior to the institution of a legal proceeding alleging such cause of action, may be asserted by either party against the other, to the extent permitted by law.

10. **Interconnection.** Customer will permit Verizon to connect diagnostic software and equipment ("Diagnostic Facilities") to Customer's communications network and equipment ("Customer Network") for purposes of performing the Professional Services. Verizon has no liability or obligation for: (a) the installation, operation or maintenance of the Customer Network; (b) the availability, capacity and/or condition of the Customer Network; or (c) any adverse impact of the Professional Services on the Customer Network. The Diagnostic Facilities will remain the property of Verizon and Customer will not have any right or interest in them. Customer may not move, alter, or attach anything to the Diagnostic Facilities without Verizon's prior written consent. Customer is responsible for any damage to or loss of the Diagnostic Facilities, unless caused solely by Verizon's negligence or willful misconduct.

11. **Independent Contractors.** The parties are independent contractors to one another, and nothing in the Agreement and no action taken pursuant to the Agreement creates an agency, partnership, association, joint venture, or other co-operative entity relationship between them. Nothing in this Agreement creates an employer-employee relationship between Customer and either Verizon or any employee or agent of Verizon.

12. **Hours of Performance**. Unless otherwise agreed in a SOW, Professional Services will be performed between the hours of 9:00 a.m. and 6:00 pm (local time where Professional Services are performed) Monday through Friday excluding public and generally observed holidays where the Professional Services are performed.

13. **Geographic Limitations.** Unless expressly stated to the contrary in the SOW, Professional Services are offered to Customer only within those jurisdiction(s) where the Verizon entities identified in the SOW as performing the Professional Services are incorporated and are legally entitled to perform the Professional Services. Unless expressly stated to the contrary in the SOW, if the foregoing conditions are not met in relation to the SOW, Verizon may terminate the SOW by notice in writing to Customer and the SOW has no further effect.

14. **Compliance with Laws.** The Professional Services are provided subject to all applicable laws and regulations. Customer will comply, and ensure that users of the Services comply, with all applicable laws and regulations including without limitation: (i) local license or permit requirements; and (ii) applicable export/re-export, sanctions, import and customs laws and regulations. Verizon makes no representation as to whether any regulatory approvals required by Customer to use the Professional Services will be granted.

15. **Non-Solicitation of Employees.** Except with the prior written consent of the other party, both parties agree that, during the term of a Project and for a period of 12 months thereafter, they shall not directly solicit, divert or recruit any employee of the other, who is or was involved in the performance of the Project at any time during the term of the Project, to leave such employment. This restriction does not prevent a party from considering for employment any individual, whether or not an employee of the other party, who has responded to a general public solicitation.

16. **Professional Services relating to Security.**

16.1 **Customer Acknowledgement.** Customer accepts and agrees that Professional Services relating to security are only one component of Customer's overall security program and are not a comprehensive security solution, and Customer is always responsible for exercising care reasonable under the circumstances in monitoring and managing its security environment and mitigating the risks associated with any potential or actual security hazard. Customer acknowledges, in particular, that (a) it is impossible to detect, disclose and/or resolve every vulnerability or security hazard, (b) that unauthorized access may occur and (c) that impenetrable security can not be attained.

16.2 **Risks Associated with Assessment Services.** Professional Services relating to security may include penetration testing, ethical hacking, scanning, vulnerability assessment, war dialing, social engineering or similar activities ("Assessment Services") targeting certain IP addresses, network domains or segments, telecommunications, hardware, software or other utilities, applications, processes, data, groups or individuals ("Service Target"). Assessment Services may also include testing the effectiveness of the security policies, training, procedures and controls of Customer's organization or the organization of a third party, whether an outside service provider to Customer or another type of Customer business partner ("Customer OSP"), and/or testing and auditing the security awareness of Customer's and Customer OSP's employees and personnel. Such activities also include deceptive testing activities to gain "unauthorized access" to Customer's network systems or confidential security related information ("CS Information"). Such "unauthorized access" is used to describe Verizon's attempts to gain access to Customer's network and information through testing activities that are not authorized by Customer's network security policies so as to exploit Customer's network and CS Information security vulnerabilities. Reference to "unauthorized access" does not mean that Customer has prohibited authorization of the testing activities themselves. Customer acknowledges that certain risks are inherent in Assessment Services and, without limiting the foregoing, that Assessment Services may, in some circumstances, result in adverse consequences including, without limitation, performance degradation, loss of, disruption to or unavailability of, the Service Target or loss of connection, data or utilities. Customer agrees to assume all risk for any adverse consequences resulting from or associated with: (a) the Assessment Services; and (b) the timeframe within which it elects or authorizes Verizon to perform the Assessment Services. Verizon shall take reasonable steps to mitigate risks from Assessment Services; however, Customer understands that such risks cannot be eliminated. Customer agrees to indemnify, defend and hold harmless Verizon from any loss, damages, liabilities, costs and expenses (including reasonable attorneys' fees and expenses and those of other professionals) incurred by Verizon as a direct or indirect result of Verizon's performance of the Assessment Services, including, without limitation, assessment of assets that are not controlled directly by Customer (e.g., servers hosted by third parties). The foregoing indemnity does not apply to the extent any such loss, damage, liability cost or expense arises from Verizon's actions or omissions that are or are found to be (a) knowingly outside the scope of the Assessment Services agreed upon, or (ii) reckless, wanton, malicious, illegal or deliberately negligent.

Contract ID_____
Routing Code: PS

Attachment 1 – Service Order Form
Service Order Details - Professional Services

Verizon Legal Entity (Verizon Signatory)	**Customer Legal Entity (Customer Signatory)**
Registered Office Address: Verizon register address	**Registered Office Address:** Customer register address
Verizon Signature:	**Customer Signature:**
Name:	**Name:**
Title:	**Title:**
Date:	**Date:**

Service Provided by:

Order Information:

Verizon Legal Entity Address	*Address, City, State, Post Code, Country*
Contract ID	Contract ID
SOF#	Quote ID #
SOW#	SOW #
Service Order Effective Date	**Drop Down:** Calendar – for choice to be displayed as January 1, 2014 or Upon Full Execution of SOF
Term	XX months

Service Details:

Customer Information

Service Delivered to:

Site 1 – Headquarters			
Registered Company Name		XXXXXXXXXX	
VAT/GST/Consumption Tax Number (as applicable)		XXXXXXXXXX	
CIN/Registration Number (as applicable)		XXXXXXXXXX	
Site Address		XXXXXXXXXX	
Town/City		XXXXXXXXXX	
Province/County/State (as applicable)		XXXXXXXXXX	
Postal Code		XXXXXXXXXX	
Country		XXXXXXXXXX	
Contact Name: XXXXXXXXXX		Email: XXXXXXXXXX	
Contact Phone: XXXXXXXXXX		Fax No: XXXXXXXXXX	
Onsite	X	Remote	X
Site 2		Name	
Site Address		Address, City, State, Post Code, Country	
Onsite	X	Remote	X
Site 3		Name	
Site Address		Address, City, State, Post Code, Country	
Onsite	X	Remote	X

Site 4		Name	
Site Address		Address, City, State, Post Code, Country	
Onsite	X	Remote	X
Contact Managing Principal if additional sites are needed			

Service Billed to:

Registered Company Name	XXXXXXXXXX		
VAT/GST/Consumption Tax Number (as applicable)	XXXXXXXXXX		
Tax exempt: *(if yes, valid exemption certificate must be provided for invoiced entity)*		Yes	No
CIN/Registration Number (as applicable)	XXXXXXXXXX		
Bill To Address	XXXXXXXXXX		
Town/City	XXXXXXXXXX		
Province/County/State (as applicable)	XXXXXXXXXX		
Postal Code	XXXXXXXXXX		
Country	XXXXXXXXXX		
Billing Language:	XXXXXXXXXX		
Billing Currency:	XXXXXXXXXX		
Ban No: XXXXXXXXXX(as applicable)	Existing: Yes/No	XXX	
Billing Contact Name: XXXXXXXXXX	Email: XXXXXXXXXX		
Telephone No: XXXXXXXXXX	Fax No: XXXXXXXXXX		

Contract Information:

Standalone Professional Services Agreement. Note: Include Terms and Conditions or reference link to Guide	Yes	No	Contract ID	Contract ID
Master Agreement name / type				MSA/VSA/GSA/WWSA
Master Agreement – contract ID no				Contract ID
Professional Services Service Attachment to Master Agreement – Document ID.:				Document ID

Purchase Order Details:

Please indicate whether or not Customer requires issuing a purchase order or providing a purchase order number ("PO") to facilitate payment under this Service Order by checking/ticking the relevant box below. Unless indicated otherwise below, Customer will be deemed not to require a PO.			
X	NO: PO is not required	X	YES: PO is required / PO No: Enter PO Number

Currency:

Currency	
All charges and amounts in this attachment are expressed in the following currency:	Currency – Drop Down

Rates and Charges:

Pricing or promotional benefits in this Service Order Form ("SOF") may not be available unless it is signed and delivered to Verizon prior to [**insert date**].

Part A: Professional Services on Time and Materials Basis				
Time and Materials – Type				
Please indicate by checking the relevant box below if the professional services will be provided on a capped or uncapped basis. Unless indicated otherwise below, the professional services will be provided on an uncapped basis.				
X	Uncapped time and materials (Estimate)		X	Capped time and material
X	Pool/Bucket	Pool/Bucket SOF ID		Pool/Bucket SOF ID no.

Resource	Description	Hourly rate	Number of Hours (estimate)	Charges
Role – Drop Down	Invoice Literal – Drop Down for applicable Practice	$XXX	XXX	$XX,XXX.XX
Role – Drop Down	Invoice Literal – Drop Down for applicable Practice	$XXX	XXX	$XX,XXX.XX
Role – Drop Down	Invoice Literal – Drop Down for applicable Practice	$XXX	XXX	$XX,XXX.XX
Totals				$XX,XXX.XX

Invoicing schedule	
Professional services provided on a time and materials basis:	monthly in arrears of performance / consumption

Part B: Professional Services Fixed
The professional services will be invoiced in a lump sum/milestone or periodic billing arrangement. This is indicated by line item for each site. Milestones can be an achievement of Deliverables or dates and are invoiced upon such achievement, as indicated below. Lump sum payments are invoiced upon the Service Order Effective Date or upon completion of the Project, as indicated below.

Customer Location	Description	Invoicing Schedule	Labor Type	Milestone or Period Charge
Site Name - Drop Down Name from Delivered to Section	Invoice Literal – Drop Down for applicable Practice or Milestone	-Drop Down Selections 1. **'Lump Sum Upon Service Order Effective Date'** 2. **'Lump Sum Upon Completion'** 3. **'Milestone'** + «text to describe deliverable» 4. **'Milestone'** + «text or calendar to enter future month/year 5. **'Periodic Annual'** 6. **'Periodic Semi-Annual'** 7. **'Periodic Quarterly'** 8. **'Periodic Monthly'**	Drop Down Onsite or Remote	$XX,XXX.XX
Site Name - Drop Down Name from Delivered to Section	Invoice Literal – Drop Down for applicable Practice or	-Drop Down Selections 1. **'Lump Sum Upon Service Order Effective**	Drop Down Onsite or Remote	$XX,XXX.XX

	Milestone	**Date'** 2. **'Lump Sum Upon Completion'** 3. **'Milestone'** + «text to describe deliverable» 4. **'Milestone'** + «text or calendar to enter future month/year 5. **'Periodic Annual'** 6. **'Periodic Semi-Annual'** 7. **'Periodic Quarterly'** 8. **'Periodic Monthly'**		
Totals				**$XX,XXX.XX**
Invoicing schedule – Periodic				
Professional services provided on a recurrent basis:		Drop Down Selection 1. Payment in advance of period. 2. Payment in arrears of period.		

~~**Part C: Professional Services Travel and Expenses**~~					
~~If a fixed amount is shown below, Verizon may invoice this amount to Customer, and Customer will pay, for travel and expenses without further travel and expense detail. Travel and expenses in excess of this amount may be reimbursed upon Customer's prior written authorization.~~					
~~Fixed~~	~~$XX,XXX.XX~~	~~Actual~~	~~Y/N~~	~~Actual Capped~~	~~$XX,XXX.XX~~
~~**Invoicing schedule**~~					
~~Travel and Expenses – actuals/actuals capped~~		~~monthly in arrears of incurrence~~			
~~Travel and Expenses – lump sum:~~		~~in full upon the Service Order Effective Date –OR- upon completion of the Project (drop down)~~			

Part D: Payment Terms	
.Payment Terms:	Payment terms as indicated in the Master Agreement / PSA unless otherwise indicated here.

AGREEMENT ADDENDUM FOR SOFTWARE

WV-96A
Rev. 12/12

In the event of conflict between this addendum and the agreement, this addendum shall control:

1. **DISPUTES** - Any references in the agreement to arbitration or to the jurisdiction of any court are hereby deleted. Disputes arising out of the agreement shall be presented to the West Virginia Court of Claims.
2. **HOLD HARMLESS** - Any provision requiring the Agency to indemnify or hold harmless any party is hereby deleted in its entirety.
3. **GOVERNING LAW** - The agreement shall be governed by the laws of the State of West Virginia. This provision replaces any references to any other State's governing law.
4. **TAXES** - Provisions in the agreement requiring the Agency to pay taxes are deleted. As a State entity, the Agency is exempt from Federal, State, and local taxes and will not pay taxes for any Vendor including individuals, nor will the Agency file any tax returns or reports on behalf of Vendor or any other party.
5. **PAYMENT** - Any references to prepayment are deleted. Fees for software licenses, subscriptions, or maintenance are payable annually in advance. Payment for services will be in arrears.
6. **INTEREST** - Any provision for interest or charges on late payments is deleted. The Agency has no statutory authority to pay interest or late fees.
7. **NO WAIVER** - Any language in the agreement requiring the Agency to waive any rights, claims or defenses is hereby deleted.
8. **FISCAL YEAR FUNDING** - Service performed under the agreement may be continued in succeeding fiscal years for the term of the agreement, contingent upon funds being appropriated by the Legislature or otherwise being available for this service. In the event funds are not appropriated or otherwise available for this service, the agreement shall terminate without penalty on June 30. After that date, the agreement becomes of no effect and is null and void. However, the Agency agrees to use its best efforts to have the amounts contemplated under the agreement included in its budget. Non-appropriation or non-funding shall not be considered an event of default.
9. **STATUTE OF LIMITATION** - Any clauses limiting the time in which the Agency may bring suit against the Vendor, lessor, individual, or any other party are deleted.
10. **SIMILAR SERVICES** - Any provisions limiting the Agency's right to obtain similar services or equipment in the event of default or non-funding during the term of the agreement are hereby deleted.
11. **FEES OR COSTS** - The Agency recognizes an obligation to pay attorney's fees or costs only when assessed by a court of competent jurisdiction. Any other provision is invalid and considered null and void.
12. **ASSIGNMENT** - Notwithstanding any clause to the contrary, the Agency reserves the right to assign the agreement to another State of West Virginia agency, board or commission upon thirty (30) days written notice to the Vendor and Vendor shall obtain the written consent of Agency prior to assigning the agreement.
13. **LIMITATION OF LIABILITY** - The Agency, as a State entity, cannot agree to assume the potential liability of a Vendor. Accordingly, any provision in the agreement limiting the Vendor's liability for direct damages is hereby deleted. Vendor's liability under the agreement shall not exceed three times the total value of the agreement. Limitations on special, incidental or consequential damages are acceptable. In addition, any limitation is null and void to the extent that it precludes any action for injury to persons or for damages to personal property.
14. **RIGHT TO TERMINATE** - Agency shall have the right to terminate the agreement upon thirty (30) days written notice to Vendor. Agency agrees to pay Vendor for services rendered or goods received prior to the effective date of termination. In such event, Agency will not be entitled to a refund of any software license, subscription or maintenance fees paid.
15. **TERMINATION CHARGES** - Any provision requiring the Agency to pay a fixed amount or liquidated damages upon termination of the agreement is hereby deleted. The Agency may only agree to reimburse a Vendor for actual costs incurred or losses sustained during the current fiscal year due to wrongful termination by the Agency prior to the end of any current agreement term.
16. **RENEWAL** - Any reference to automatic renewal is deleted. The agreement may be renewed only upon mutual written agreement of the parties.
17. **INSURANCE** - Any provision requiring the Agency to purchase insurance for Vendor's property is deleted. The State of West Virginia is insured through the Board of Risk and Insurance Management, and will provide a certificate of property insurance upon request.
18. **RIGHT TO NOTICE** - Any provision for repossession of equipment without notice is hereby deleted. However, the Agency does recognize a right of repossession with notice.
19. **ACCELERATION** - Any reference to acceleration of payments in the event of default or non-funding is hereby deleted.
20. **CONFIDENTIALITY** -Any provision regarding confidentiality of the terms and conditions of the agreement is hereby deleted. State contracts are public records under the West Virginia Freedom of Information Act.
21. **AMENDMENTS** - All amendments, modifications, alterations or changes to the agreement shall be in writing and signed by both parties. No amendment, modification, alteration or change may be made to this addendum without the express written approval of the Purchasing Division and the Attorney General.

ACCEPTED BY:

STATE OF WEST VIRGINIA	**Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services**
Spending Unit: _____	Company Name: _____
Signed: _____	Signed: Marsha K. Harrell
Title: _____	Title: **Marsha K Harrell** Senior Consultant Pricing/Contract Management
Date: _____	Date: 1/21/15

Corporate Policy Statement

Policy No.: CPS–103
Issued: December 6, 2010
Subject: Authority to Approve Transactions

verizon
Telecom and Business

APPENDIX 4
VERIZON BUSINESS
CPS–103 LETTER OF DELEGATION OF AUTHORITY
FORM 101

Within the authority granted to me in CPS–103, "Authority to Approve Transactions," I delegate

Patricia L Myers, Manager, Pricing & Contract Management [redacted]
Marsha K Harrell, Senior Consultant, Pricing & Contract Management [redacted] *and*
Jacqualynn A Whiting, Director, Pricing & Contract Management [redacted]

the authority to perform the following function:

Execute and deliver Verizon Business Customer Contracts and Proposals requiring "wet ink" signatures, including any and all ancillary documents and amendments related thereto, that are duly approved in accordance with then-applicable Verizon Business corporate policies, including the use of stamp bearing facsimile of my signature in accordance with *Security Procedure for Anthony Recine, Vice President, Pricing & Contract Management, Blue Ink Stamp* Policy.

This will be effective beginning on July 1, 2014 and ending on June 30, 2015 or before if rescinded by me.

(Annual delegations must be completed by July 1st of each respective year and may not exceed one year from their effective date. Delegations with a start date other than July 1st should also include an end date of the subsequent June 30 or earlier.)

Distribution:

- The person delegated authority must retain a copy of Form 101 delegation, either electronic or hard copy, for one (1) year after expiration date.
- The person granting the delegation must retain the Form 101 delegation, either electronic or hard copy, for one (1) year after expiration date; send a copy to the delegate, the group Chief Financial Officer, and Corporate Finance Compliance at corporatefinancecompliance@core.verizon.com; and ensure the delegation is entered into the Accounts Payable system when appropriate.

Approved By:

Anthony Recine 5/16/14
Signature Date

Anthony Recine [redacted]
Name VZ ID

VP, Pricing & Contract Management [redacted]

[redacted]
Responsibility Code or Cost Center Code

5/15/14
Delegate's Signature – Jacqualynn A Whiting

Patricia L Myers 5/20/14
Delegate's Signature – Patricia L Myers

Marsha K. Harrell 5/20/14
Delegate's Signature – Marsha K Harrell