verizon✓

General Services Administration
NS2020 Enterprise Infrastructure Solutions (EIS)

Volume 1: Technical
Attachment A: EIS Information Technology (IT) Risk Management Framework Plan

Solicitation Number: QTA0015THA3003
February 22, 2016

Submitted to:
General Services Administration
Mr. Timothy Horan
FAS EIS Contracting Officer
1800 F St NW
Washington DC 20405-0001

Submitted by:
Verizon
22001 Loudoun County Parkway
Ashburn, VA 20147

Verizon Point of Contact:
Kevin K. Anderson
Sr. Contract Manager
703-886-2647 (Office)
571-271-8456 (Mobile)
kevin.k.anderson@verizon.com

Verizon Bidding Entity:

Verizon Business Network Services Inc. on behalf of MCI Communications Services, Inc. d/b/a Verizon Business Services and any additional Verizon entities providing service to the Government for this project (individually and collectively, "Verizon"). Local services are performed by the Verizon ILEC or CLEC in the jurisdiction where services are provided. International services are performed by the appropriate Verizon operating company in the foreign jurisdiction.

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of—or in connection with—the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to this restriction are contained in sheets marked with the following disclaimer:
"Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal."

TABLE OF CONTENTS

TABLE OF FIGURES

[redacted]

[redacted]

[redacted]

LIST OF TABLES

[redacted]

[redacted]

[redacted]

[redacted]

A. EIS IT RISK MANAGEMENT FRAMEWORK PLAN [L.29(3)(a); C.1.8.7; NIST SP 800-37]

As a leading provider of telecommunications services to the U.S. Government, Verizon has an established, proven record in information security risk management utilizing the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-series guidelines including, but not limited to NIST SP 800-37 Rev. 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Verizon has long recognized the importance of managing information security and system risk and was an early adopter of both the initial NIST SP 800-37 and the subsequent Revision 1 as best practices not just to manage but also to minimize risk. Verizon has successfully worked with the General Services Administration (GSA) on numerous contracts including, but not limited to Managed Trusted Internet Protocol Service (MTIPS), Networx, Washington Interagency Telecommunications System (WITS), and FTS2001. To date, Verizon has been granted numerous Authorizations to Operate (ATOs) based on NIST SP 800-37 Rev. 1. As a service provider, Verizon monitors the risk to many U.S. agencies [redacted]

Verizon has worked closely with these government agencies to implement the processes identified in the NIST Risk Management Framework (RMF). Verizon's significant experience in this area has provided Verizon with a solid understanding of the NIST RMF and agency-specific information security and Assessment and Authorization (A&A) requirements. As discussed in **Section A.2** of this RMF Plan, these agency-specific requirements include: GSA CIO P 2100.1, GSA Information Technology (IT) Security Policy; DoD Instruction 8510.01, Risk Management Framework for DoD Information Technology (IT); Intelligence Community Directive (ICD) 503 Intelligence Community Information Technology Systems Security Risk Management; and Committee on National Security Systems Instruction (CNSSI) No. 1253, Security

Categorization and Control Selection for National Security Systems. This Information Technology (IT) RMF Plan outlines how Verizon will leverage its deep agency-specific RMF experience for the EIS program.

A.1 Purpose and Scope

This RMF Plan describes Verizon's overarching approach to managing applicable risks to information systems and their contents as well as the steps that Verizon will take to integrate security requirements throughout the EIS IT System Development Life Cycle (SDLC) and to obtain and maintain an ATO from the government's authorizing official (AO). This RMF Plan provides the following information:

- Overview of Verizon's organizational information security risk management process;
- Identification of the key information security and information systems risk management standards and guidelines Verizon uses in support of EIS IT;
- Definition of the key roles of the organizations and individuals responsible for defining and implementing the EIS IT RMF;
- Overview of the Verizon EIS IT information system and security architecture that will be implemented using the risk management framework;
- Discussion of the specific implementation activities within the RMF process; and
- Identification of Verizon's key RMF deliverables for the EIS IT offering.

As required by the **EIS RFP Section C.1.8.7.7**, this EIS IT RMF Plan describes Verizon's high-level approach to security compliance for security requirements for services provided under EIS. In accordance with the RFP instructions, this high-level EIS IT RMF Plan has been augmented with service-specific RMF Plans for MTIPS and the EIS Business Systems Solution (BSS). The MTIPS RMF Plan is included in Volume 1: Technical, Attachment B and the BSS RMF Plan can be found in Volume 2: Management, Section 8 of Verizon's EIS proposal.

A.2 Applicable Standards and Guidelines

In providing EIS services, Verizon will comply with government identified federal and agency-specific IT security directives, standards, policies, and reporting requirements, as specified in the respective Task Order (TO). Where applicable, Verizon will comply with FISMA, Department of Defense (DoD), Intelligence Community and agency guidance and directives, including applicable Federal Information Processing Standards (FIPS), NIST SP 800-series guidelines, required government policies, and other applicable laws and regulations for protection and security of government IT.

Table A.2-1 lists key information security management standards and guidelines Verizon references in support of the EIS IT RMF. When discussed in this RMF Plan, the versions of the documents identified in **Table A.2-1** are the applicable reference.

Table A.2-1. Applicable EIS IT RMF Documents

EIS IT Risk Management Framework Plan Applicable Documents
▪ Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C, Section 301. Information Security)
▪ Federal Information Security Modernization Act of 2014 (to amend Chapter 35 of 44 U.S.C.)
▪ Clinger-Cohen Act of 1996 (Formerly known as the Information Technology Management Reform Act of 1996).
▪ Privacy Act of 1974 (5 U.S.C. § 552a)
▪ Homeland Security Presidential Directive 12 (HSPD-12), Policy for Identification for Federal Employees and Contractors, August 27, 2004.
▪ E-Government Act of 2002 (Public Law 107-347)
▪ Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
▪ Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information System, March 2006
▪ Federal Information Processing Standards (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, May 2001
▪ OMB Circular A-130, Management of Federal Information Resources (and Appendix III, Security of Federal Automated Information Resources, Transmittal Memorandum, No. 4, November 28, 2008
▪ OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003
▪ OMB Memorandum M-06-16, Protection of Sensitive Agency Information, June 23, 2006
▪ OMB Memorandum M-05-24, Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors, August 5, 2005
▪ OMB Memorandum M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors, February 3, 2011
▪ OMB Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems, November 18, 2013
▪ OMB Memorandum M-15-01, Guidance on Improving Federal Information Security and Privacy Management Practices, October 3, 2014
▪ NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems, February 2006
▪ NIST SP 800-30, Revision 1, Guide for Conducting Risk Assessments. September 2012
▪ NIST SP 800-34, Revision 1, Contingency Planning Guide for Information Technology Systems. May 2010
▪ NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach, February 2010
▪ NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, March 2011
▪ NIST SP 800-40 Revision 3, Guide to Enterprise Patch Management Technologies, July 2013
▪ NIST SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy, September 2009
▪ NIST SP 800-47, Security Guide for Interconnecting Information Technology System, August 2002
▪ NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013
▪ NIST SP 800-53A, Revision 4, Guide for Assessing the Security Controls in Federal Information Systems: Building Effective Security Assessment Plans, December 2014
▪ NIST SP 800-58, Security Considerations for Voice Over IP Systems, January 2005.
▪ NIST SP 800-60 Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008

EIS IT Risk Management Framework Plan Applicable Documents
▪ NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide, August 2012
▪ NIST SP 800-64, Revision 2, Security Consideration in the System Developments Lifecycle, October 2008
▪ NIST SP 800-70 ,Revision 3, National Checklist Program for IT Products – Guidelines for Checklist Users and Developers
▪ NIST SP 800-88 Revision 1, Guidelines for Media Sanitization, December 2014
▪ NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems, February 2007
▪ NIST SP-800-126, Revision 2, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2, September 2011
▪ NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, August 2011
▪ NIST SP 800-137, Information Security Continuous Monitoring for Federal Information Systems and Organizations, September 2011
▪ NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing, December 2011
▪ NIST SP 800-160, Systems Security Engineering Draft, May 2014
▪ NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2015
▪ NIST SP 800-171, Protecting Controlled Unclassified Information in the Nonfederal Information Systems and Organizations, June 2015
▪ Committee on National Security Systems (CNSS) Policy No. 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions, November 28, 2012
▪ Committee on National Security Systems (CNSS) Policy No. 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems, October 1, 2012
▪ Committee on National Security Systems Instruction No. 1253, Security Categorization and Control Selection for National Security Systems, March 12, 2014
▪ Committee on National Security Systems Instruction (CNSSI) No. 5000, Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony, April 2007
▪ Department of Defense Instruction (DODI) 8500.01 Cybersecurity, March 14, 2014
▪ DODI 8510.01, Risk Management Framework (RMF) for DOD Information Technology (IT), March 12, 2014.
▪ Department of Defense (DOD) Cloud Computing Security Requirements Guide (SRG), December 7, 2014
▪ ICD 503, Intelligence Community Information Technology Systems Security Risk Management, July 21, 2015
▪ ICD 703, Protection of Classified National Intelligence, Including Sensitive Compartmented Information, June 21, 2013
▪ ICD 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information, October 2, 2008
▪ ICD 705, Sensitive Compartmented Information Facilities, May 26, 2010
▪ ICD 731, Supply Chain Risk Management, December 7, 2013
[redacted]
[redacted]
[redacted]

In addition to the standards and guidelines identified in **Table A.2-1**, Verizon will comply with the agency-specific policies, directives, and standards as identified at the TO level. **Table A.2-2** provides a representative sample of these standards and guidelines.

Table A.2-2. Representative Agency-specific Security Documents

EIS IT Risk Management Framework Plan Representative Agency-specific Documents
▪ Department of Veterans Affairs, VA Handbook 6500, Risk Management Framework of VA Information Systems, March 10, 2015
▪ Department of Health and Human Services, HHS Information Security and Privacy Policy (IS2P), 2014
▪ Department of Transportation, DOT Order 1351.37, Departmental Cybersecurity Policy, June 21, 2011
▪ Department of Homeland Security, DHS Sensitive Systems Policy Directive 4300A, Version 9.1, July 17, 2012
▪ Department of the Army, Army Regulation (AR) 25-2, Cybersecurity (Draft), March 2015
▪ Centers for Medicare and Medicare Services (CMS), Acceptable Risk Safeguards (ARS), CMS Minimum

EIS IT Risk Management Framework Plan Representative Agency-specific Documents
Security Requirements (CMSR), Version 2.0, September 20, 2013
▪ Centers for Medicare and Medicare Services (CMS),Risk Management Handbook (RMH), Volume 1, Chapter 1, Risk Management in the eXpidited Life Cycle (XLC), Version 1.0, November 8, 2012September 20, 2013
▪ GSA CIO P 2100.1J, GSA Information Technology (IT) Security Policy , December 22, 2015
▪ GSA Order CIO P 2181.1, GSA HSPD-12 Personal Identity Verification and Credentialing, October 20, 2008
▪ GSA Order CIO 2104.1A, GSA IT General Rules of Behavior, June 5, 2012
▪ GSA Order CIO P 1878.1, GSA Privacy Act Program, September 2, 2014
▪ GSA Order CIO P 1878.2A, Conducting Privacy Impact Assessments (PIAs) in GSA, October 29, 2014
▪ GSA IT Security Procedural Guide CIO-IT Security 01-01, Revision 4, Identification and Authentication, May 30, 2015
▪ GSA IT Security Procedural Guide CIO-IT Security 01-02, Revision 11, Incident Response, October 1, 2015
▪ GSA-IT Security Procedural Guide CIO-IT, Security 01-05, Revision 3, Configuration Management, July 14, 2015
▪ GSA-IT Security Procedural Guide CIO-IT Security 01-07, Revision 3, Access Control, April 1, 2015
▪ GSA-IT Security Procedural Guide CIO-IT Security 01-08, Revision 3, Audit and Accountability (AU) Guide, June 30, 2010
▪ GSA IT Security Procedural Guide CIO-IT Security-05-29, Revision 3, IT Security Training and Awareness Program, November 3, 2015
▪ GSA IT Security Procedural Guide CIO-IT Security-06-29, Revision 2, Contingency Planning, August 16, 2010
▪ GSA IT Security Procedural Guide CIO-IT Security-06-30, Revision 7, Managing Enterprise Risk Security Assessment and Authorization, Planning, and Risk Assessment (CA, PL, & RA), May 31, 2011
▪ GSA IT Security Procedural Guide CIO-IT Security 06-32, Revision 3, Media Protection Guide, April 15, 2012
▪ GSA IT Security Procedural Guide CIO-IT Security 07-35, Revision 2, Web Application Security Guide, June 16, 2008
▪ GSA IT Security Procedural Guide 08-39, FY 2015 IT Security Program Management Implementation Plan, Revision 7, October 30, 2014
▪ GSA IT Security Procedural Guide CIO-IT Security-09-44, Plan of Action and Milestones (POA&M) March 30, 2009
▪ GSA IT Security Procedural Guide CIO-IT Security 10-50, Revision 2, Maintenance Guide, April 20, 2015
▪ GSA IT Security Procedural Guide CIO-IT Security 11-51, Revision 2, Conducting Penetration Test Exercise Guide, December 11, 2014
▪ GSA IT Security Procedural Guide CIO –IT Security 12-63, GSA's System and Information Integrity, March 5, 2012
▪ GSA IT Security Procedural Guide CIO-IT Security 12-64, Physical and Environmental Protection, March 30, 2012
▪ GSA IT Security Procedural Guide CIO-IT Security-12-66, Information Security Continuous Monitoring Strategy, June 24, 2015
▪ GSA IT Security Procedural Guide CIO-IT Security-12-67, Securing Mobile Devices and Applications Guide, May 20, 2014
▪ GSA-IT Security Procedural Guide CIO-IT Security 14-69, SSL/TLS Implementation Guide, December 24, 2014

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

A.3.2.2 [redacted]

[redacted]

[redacted] [redacted]

[redacted].

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

A.3.2.4 [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

A.3.3 Verizon Public Sector Support

Verizon Public Sector is dedicated to supporting the needs of its government customers and has created a security organization to align with those needs. This team augments Verizon security policies with government security requirements, including teams supporting policy, engineering, operations, IT and management created to support security and accountability to the government. Verizon's corporate organizational structure depicted in **Figure A.3.1.1-1** above, implements the NIST tiered risk management approach defined in NIST SP 800-37.

A.3.3.1 Senior Information Security Officer, [redacted]

The Senior Information Security Officer (SISO) executes and maintains risk policies as defined by the [redacted]. The SISO reviews security matters with the [redacted] and takes guidance from the [redacted] as the liaison of the Verizon CSO and CISO. The SISO is outside the Verizon Security Engineering or Security Operations Teams to support separation of responsibility with these teams.

[redacted] has more than 15 years of experience in security program leadership, security engineering, and technology management spanning multiple business units across Verizon. **Table A.3.3.1-1** lists the SISO's responsibilities:

[redacted]

[redacted]
[redacted].

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

A.3.3.8 [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]
- [redacted] - [redacted] - [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]
- [redacted] - [redacted] - [redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]
- [redacted] - [redacted] - [redacted] - [redacted] - [redacted]

A.4 Information System Overview

Verizon's EIS information system will cover support for the proposed services under each of these twelve service areas, as specified in **Section C.1.8.1**. Verizon has categorized the following three service areas as FISMA and FedRAMP-compliant EIS services: Cloud Service, Commercial Satellite Communication Service, and Managed Services.

Verizon understands that EIS services will carry non-sensitive programmatic and administrative traffic, Controlled Unclassified Information (CUI) traffic, and higher levels of sensitive and/or classified traffic. As a proven service provider and solution partner with decades of solid past performance for government, DoD, and the IC, Verizon is committed to delivering the highest level of quality, security, and compliance for services provided under EIS.

As one of the largest commercial telecommunications providers in the world, Verizon has internal systems in place to provide these same service requirements for countless customers, including the federal government. Verizon's commercial Business Support System (BSS) incorporates industry-leading and proven IT platforms fully capable of processing, managing, deploying, and supporting service orders in large volumes and variety for government customers simultaneously across a large number of contracts. Verizon's unique back-end operations and service management capabilities coupled with the ability to secure, scale, and deliver diverse service types efficiently and effectively sets Verizon apart from the competition and continues to be the gold standard in the industry.

[redacted]

[redacted].

[redacted]

[redacted]

[redacted]

[redacted]

A.4.1.2 Verizon BSS Operating Environment

The Verizon BSS is an integral part of service order and service management architecture, helping agencies in fulfilling a multitude of telecommunication service requirements successfully and securely. The Verizon BSS infrastructure was developed using a combination of Verizon-proprietary and industry best practices, guidelines, and standards, powered by the latest and best-of-breed technologies available. [redacted]

[redacted]

[redacted]

[redacted]

A.4.1.3 FISMA-Compliant EIS Services Support Systems Operating Environment

The FISMA-compliant EIS Services Support Systems operating environment will be the fully dedicated operating environment developed for the EIS contract to meet Federal and GSA security and operation requirements and guidelines. These operating environments will be built as an overlay onto the Verizon Security programs to meet the additional FISMA impact level as specified in the security requirements, and in support of the NIST RMF processes. Specifically, EIS services with FISMA and FedRAMP security requirements will be managed and monitored via subsystems within this environment. The FISMA-compliant EIS Service Support operating environment provides two primary functions in managing risk associated with EIS service delivery: (1) secured Interface for GSA (BSS system and personnel); and (2) fortified enclave for interworking with the Verizon BSS.

The individual support systems in the dedicated operating environment will validate and support the applicable government-wide agency-specific IT security directives, standards, policies, and reporting requirements, as well as Security Assessment and Authorization (A&A) activities for the Authority to Operate (ATO) effort. This environment will be governed by FISMA associated guidance and directives, such as Federal Information Processing Standards and NIST SP 800- series guidelines; GSA IT security directives, policies and guidelines; as well as other appropriate government-wide laws and regulations for protection and security of government IT as outlined in **Section A.2**.

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted].

[redacted]

[redacted]

[redacted]

[redacted]

A.5.1.1 Verizon BSS

The Verizon BSS is comprised of many collective sets of technology, tools, processes, and resources that perform order processing, provisioning, service management, notification, billing, and payment processing. Verizon has invested heavily in the development of the BSS to simplify and accelerate the service ordering and enablement processes. The Verizon BSS program has been successfully developed and deployed an innovative next-generation BSS for its customers. The Verizon BSS improves quoting, ordering, provisioning, and simplifies billing, which will reduce the overall time from quote to implementation. The system is designed to provide flow-through automation and data validation to reduce defects and billing errors. The BSS platform has been honored by the TM Forum for contributing to enterprise business transformation. Third-party TM Forum testing has concluded that Verizon's BSS closely conformed to Business Process Framework V.13.5. [redacted]

A.5.1.2 FISMA-Compliant EIS Service Support Systems – Government BSS

The Government BSS provides the functions to meet the BSS component service requirements as identified in **RFP Section G.6.5.4**, namely, Customer Management, Financial Management, Order Management, Inventory Management, Service Management, and Program Management. The Government BSS is a fully dedicated operating environment custom-developed for the EIS contract, with the objective to meet federal government and GSA security and operation requirements and guidelines. This government BSS operating environment will be built in compliance with FISMA Moderate impact level, and in support of the NIST Risk Management Framework processes. The Government BSS and its RMF plan are described in greater detail in the BSS RMF plan deliverable.

[redacted]

[redacted]

[redacted]

- [redacted], [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[Reference: NIST SP 800-37 Rev 1, SP800-39]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

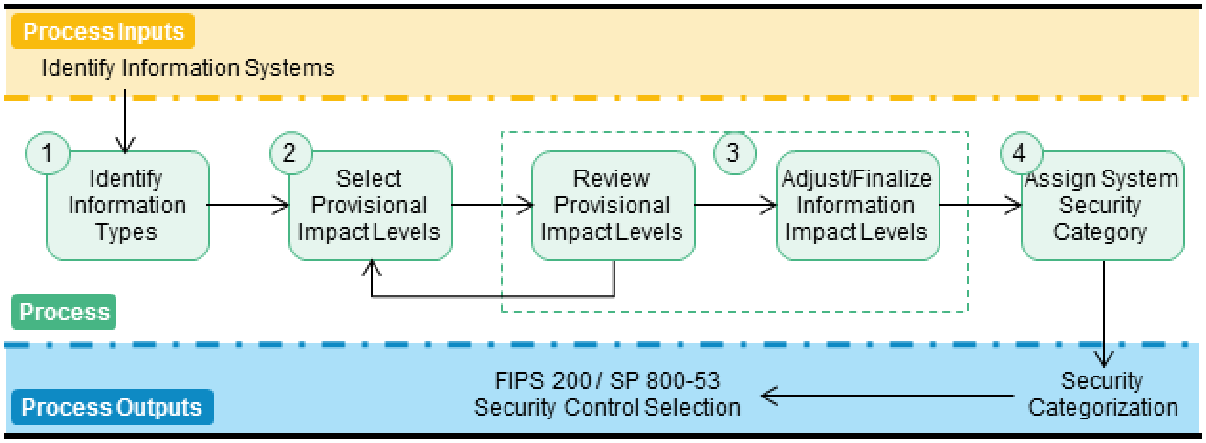
[redacted]

Figure A.6.1-1. CIA Security Objectives (44 U.S.C., Section 3542)

Confidentiality (C)	Integrity (I)	Availability (A)
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. **A loss of confidentiality is the unauthorized disclosure of information.**	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. **A loss of integrity is the unauthorized modification or destruction of information.**	Ensuring timely and reliable access to and use of information. **A loss of availability is the disruption of access to or use of information or an information system.**

Figure A.6.1-2 shows the security categorization process defined in NIST SP 800-60 that Verizon follows. This four-step security categorization process drives the selection of baseline security controls and helps determine the information system's CIA security objectives.

Figure A.6.1-2. Security Categorization Process


Process Inputs
Identify Information Systems
1
Identify Information Types
2
Select Provisional Impact Levels
Review Provisional Impact Levels
3
Adjust/Finalize Information Impact Levels
4
Assign System Security Category
Process
Process Outputs
FIPS 200 / SP 800-53 Security Control Selection
Security Categorization

[Reference: NIST SP800-60 Rev1]

Described and illustrated in **Figure B.6.1-3** below are the three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability).

Figure A.6.1-3. FIPS 199 Categorization Definitions Potential Impact Levels

Low	Moderate	High
The potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security of the United States.	The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security of the United States.	The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security of the United States.

[Ref. NIST SP800-37 Rev1, SP800-39]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

In accordance with **RFP Section C.2.8.4.5.4**, the government is responsible for conducting the Security/Risk Assessment and Penetration Tests. In accordance with Penetration Test Rules of Engagement, Verizon will allow government employees (or customer Agency designated contractors) to conduct security A&A activities to include control reviews in accordance with NIST SP 800-53/NIST SP 800-53A and GSA IT Security Procedural Guide 06-30 (or comparable customer Agency document). Review activities will include operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of government information. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

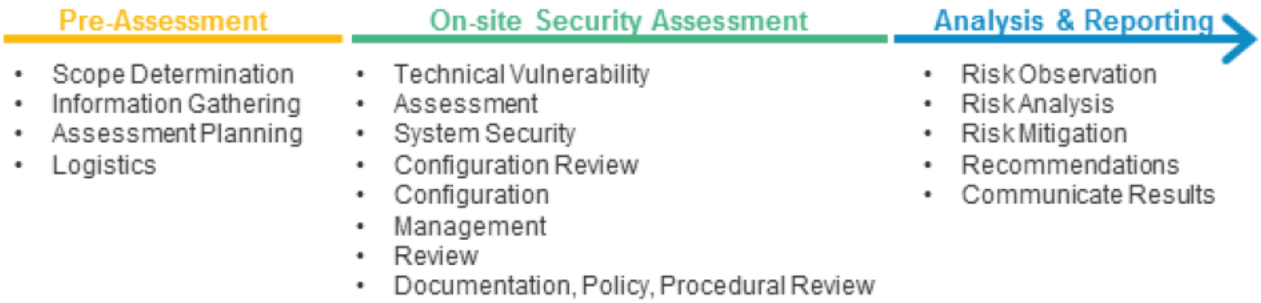
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

[redacted]

[redacted]

[redacted] A high-level overview of the methodology is represented in **Figure A.6.4-1**.

Figure A.6.4-1. Typical IT Security Assessment Methodology. ***[Ref. NIST SP800-37 Rev1, SP800-39]***



[Ref. NIST SP8010-37 Rev. 1, SP00-39]

As illustrated above, a typical security control assessment is conducted in three phases, the Pre-assessment, On-site Security Assessment and the Analysis and Reporting, as described in **Table A.6.4-3**:

Table A.6.4-3. Security Control Assessment Phases.

Security Control Assessment Phases
Phase 1 Pre-Assessment Phase. During the Pre-Assessment phase, the Information System Security Manager and the Security Assessment Team plan necessary details of the IT security assessment. This activity confirms that the scope of the assessment is mutually agreed upon, the assessment schedule and on-site plan is defined, information sharing takes place, and logistical issues are addressed. This phase verifies that the assessment will be carried out in an efficient manner and the goals and objectives of the assessment will be satisfied. Generally, the Pre-Assessment activities begin approximately four weeks in advance of the On-site Security Assessment Phase.
Phase 2 On-Site Security Assessment Phase. The on-site phase of the assessment typically takes a week to complete. During the on-site assessment, the Security Assessment Team reviews key documentation provided by the staff, interviews key personnel, and performs network vulnerability scanning and technical security configuration reviews based on the scope defined during the Pre-Assessment Phase. Scans will be performed as an authenticated user with elevated privileges. The Security Assessment Team also evaluates current practices based on the recommended IT security safeguards described within the NIST and customer Agency Information Security Framework. The Security Assessment Team also evaluates the management, operational, and technical safeguards currently in place in order to determine where risk is present, and meets with stakeholders to discuss any preliminary observations made during the assessment, to answer any questions they may have, and to identify the next steps within the security assessment process.
Phase 3 Analysis and Reporting. Following the conclusion of the on-site assessment activities, the Security Assessment Team performs detailed analysis of the information collected and observations made to develop detailed, actionable risk mitigation recommendations. Observations and recommendations are presented in a prioritized order based on the estimated risk. For each of these vulnerabilities, the report provides recommendations to either eliminate or reduce the risk presented by the vulnerability. Once the on-site assessment has been completed, a draft will be provided to the government in approximately three to four weeks. The government will then have the opportunity to review and comment on the draft. Delivery of the final report should take place approximately two weeks after the comment period is closed.

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted].

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

A.7 Key EIS IT Security Deliverables

As specified in **RFP Section C.1.8.7.4** and **C.1.8.7.5**, Verizon will create, maintain and update EIS IT security A&A documentation as specifically identified within each EIS Task Order (TO). Verizon, in compliance with each agency TO, will provide a valid security A&A when required by the agency, prior to the system being placed in operation, and processing government information.

[redacted].

[redacted]

[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Verizon will maintain and update these key EIS IT security deliverables in accordance with guidance provided by the NIST Special Publications and the Authorizing Official.