verizon

General Services Administration
NS2020 Enterprise Infrastructure Solutions (EIS)

Volume 1: Technical
Attachment B: Managed Trusted Internet Protocol Service (MTIPS) 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.

TABLE OF CONTENTS

TABLE OF FIGURES

LIST OF TABLES

B. MTIPS Risk Management Framework Plan [L.29(3)(b); C.2.8.4.5.4; NIST SP 800-37]

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 subsequent Rev. 1 as best practices not just to manage but also to minimize risk. Indeed, in its government business, Verizon has successfully worked with the General Services Administration (GSA) on numerous service programs 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,

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 GSA-specific requirements as defined in the GSA CIO P 2100.1 GSA Information Technology (IT) Security Policy and the GSA CIO IT Security Procedures and Technical Guides. Verizon has worked in concert with GSA on the previously mentioned programs to implement the processes identified in GSA CIO-IT Security-06-30, Rev. 7, Managing Enterprise Risk - Security Assessment and Authorization, Planning, and Risk Assessment. This MTIPS RMF Plan outlines how Verizon will leverage its deep agency-specific RMF experience in implementing MTIPS under the EIS program.

B.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 MTIPS System Development Life Cycle (SDLC) and to obtain and maintain an ATO from the GSA 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 the MTIPS;
- Definition of the key roles of the organizations and individuals responsible for defining and implementing the MTIPS RMF;
- Overview of the Verizon MTIPS 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 MTIPS offering.

B.2 Applicable Standards and Guidelines

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

Table B.2-1. Applicable MTIPS RMF Documents

MTIPS 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.)
▪ E-Government Act of 2002 (Public Law 107-347)
▪ Clinger-Cohen Act of 1996 also known as the Information Technology Management Reform Act of 1996
▪ Privacy Act of 1974 (5 U.S.C. § 552a)
▪ Homeland Security Presidential Directive (HSPD-12), Policy for a Common Identification Standard for Federal Employees and Contractors
▪ 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-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-06-16, Protection of Sensitive Agency Information, June 23, 2006

MTIPS Risk Management Framework Plan Applicable Documents
▪ OMB Memorandum M-08-05, Trusted Internet Connections (TIC) Initiative, November 20, 2007
▪ OMB Memorandum M-09-32, Update on the Trusted Internet Connections Initiative, September 2009
▪ 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
▪ 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 800-41 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 800-60 Revision 1, Guide for Mapping Types of Information and Information Systems to Security Categories, August 2008
▪ 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 800-88, Revision 1, Guidelines for Media Sanitization, December 2014
▪ 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 800-160, Draft, System Security Engineering, May 12, 2014
▪ NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2015
▪ GSA CIO P 2100.1I, GSA Information Technology (IT) Security Policy , December 25, 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
▪ Committee on National Security Systems Instruction No. 1253, Security Categorization and Control Selection for National Security Systems, March 12, 2014
▪ [redacted]
▪ [redacted]
▪ [redacted]
Note: If the Verizon policies/procedures/standards are less stringent than the Federal policies/procedures/standards, Verizon will meet the Federal requirements.

[redacted]

B.3.1 Verizon Information Security Governance

Verizon addresses risk at various levels of the organization, with specific emphasis on

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted].

[redacted]

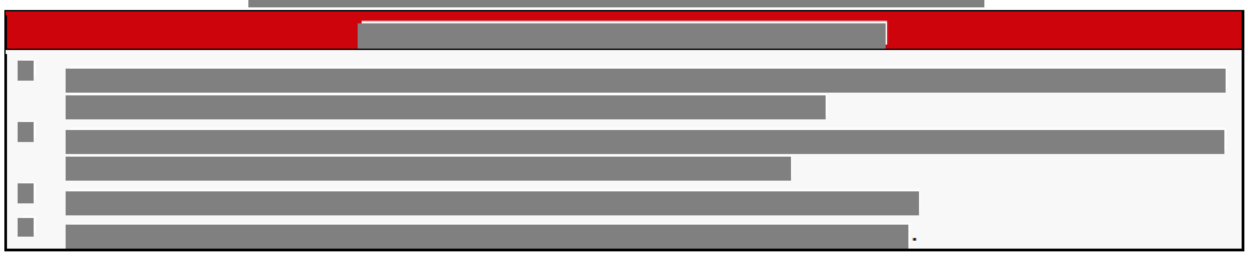
[redacted]

[redacted]

p

[redacted]

[redacted]



[redacted]

[redacted]

ed

[redacted].

[redacted]

[redacted]:

[redacted]

[redacted]

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

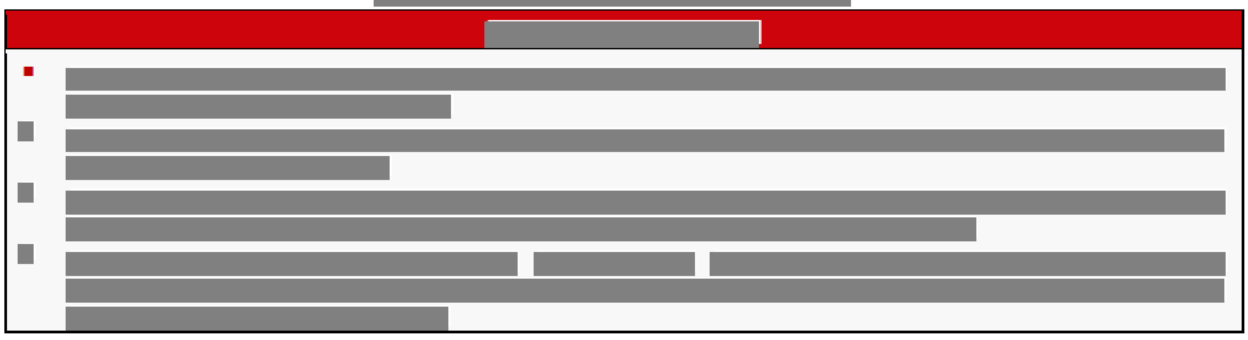
[redacted]

[redacted]

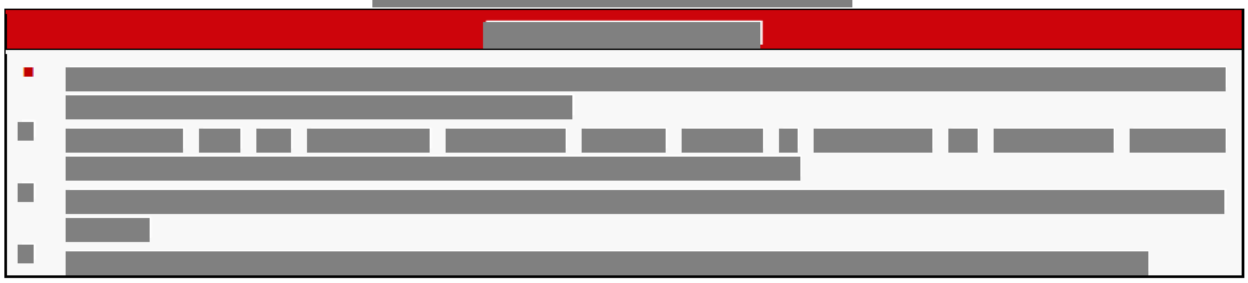
[redacted]

[redacted]

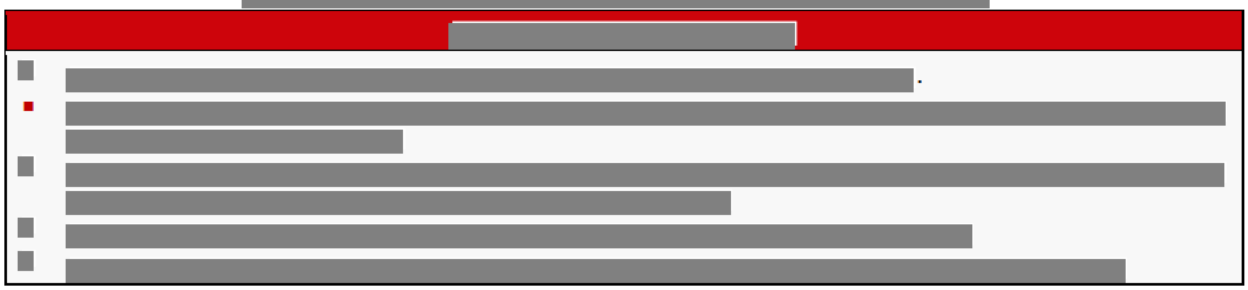
[redacted]



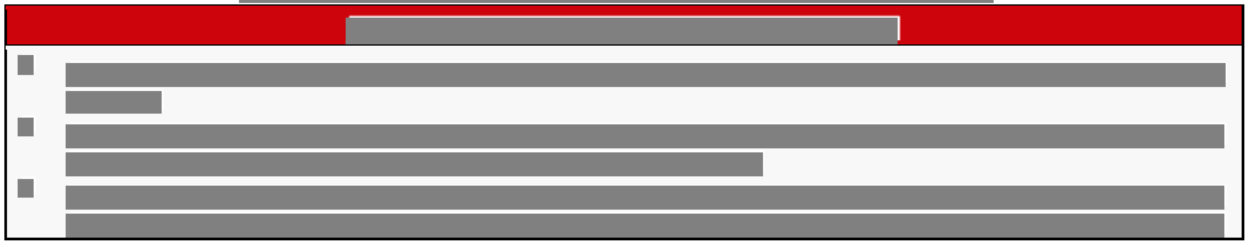
[redacted]

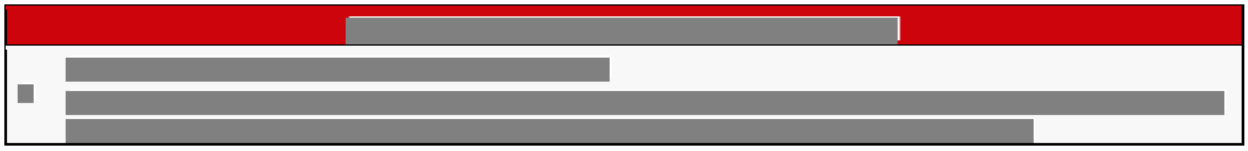


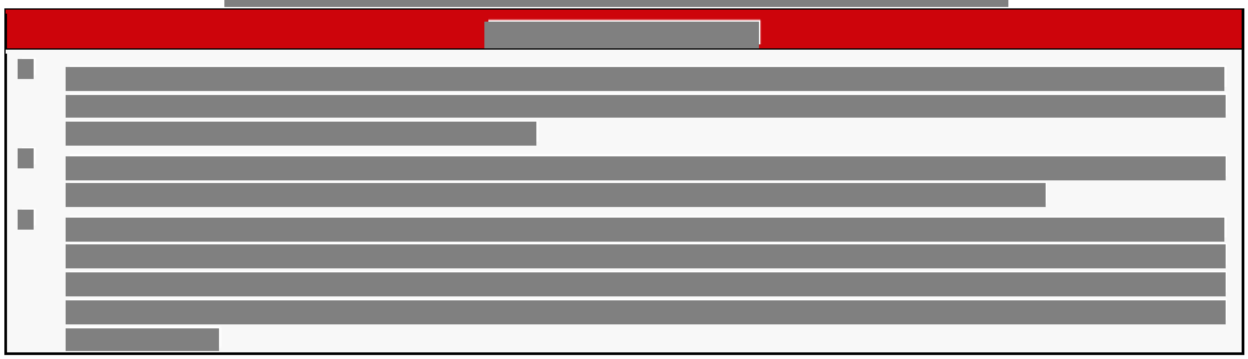
[redacted]

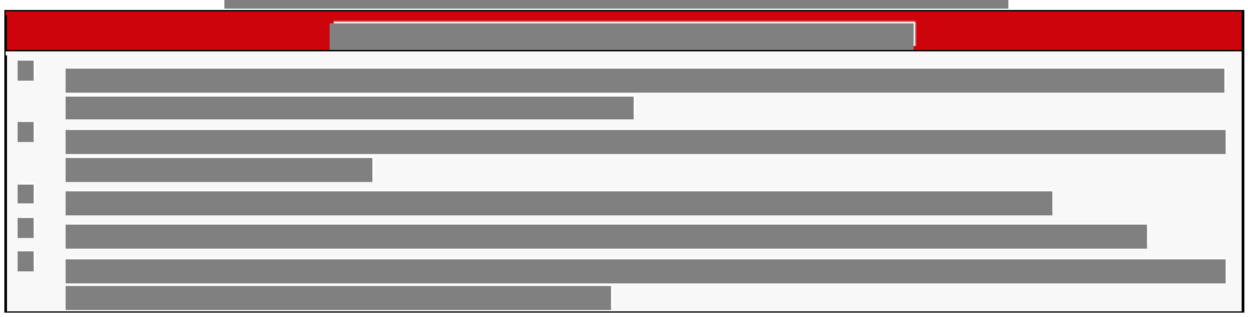


[redacted]









B.4 Information System Overview

The MTIPS program provides Trusted Internet Connections (TIC) – compliant managed security services through the Networx contract vehicle. The objective of the MTIPS is to enable federal government agencies to physically and logically connect to the public Internet and/or other external networks in compliance with OMB's Trusted Internet Connections (TIC) initiative (M-08-05) announced in November 2007. MTIPS facilitates the reduction of the number of Internet connections in government networks and provides standard security services to government users. For government agencies, MTIPS is a bundled solution with the service options to add additional features to enhance the end-to-end service offering.

Verizon MTIPS is a robust offering under the federal Networx Universal program that uses secure IP portals to meet FISMA requirements. The Verizon MTIPS Information System is designed to meet and exceed the MTIPS SOW and associated contract requirements established by the Department of Homeland Security (DHS) TIC 2.0 Reference Architecture. It provides a full suite of core security services such as managed firewalls, intrusion detection and prevention, anti-virus and e-mail scanning services, along with connections to the public Internet that are redundant, highly available and scalable. Verizon's Private IP service, the key building block of MTIPS transport, is a physically separate infrastructure from the public Internet, and securely connects federal agencies to the TIC portals. In addition, Verizon MTIPS is TIC 2.0 compliant and has been incorporated within the MTIPS offering, providing flexibility for agencies to design and add custom features around the basic services.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

verizon

[redacted]

B.6 The Verizon MTIPS RMF Process

For more than 10 years, Verizon has followed the Security Authorization Process (formerly Certification and Accreditation (C&A)) process defined in GSA CIO-IT Security-06-30 Managing Enterprise Risk - Security Assessment and Authorization, Planning, and Risk Assessment. As specified in Rev. 7 of GSA CIO-IT Security-06-30, the Verizon MTIPS RMF process is based on the NIST Risk Management. The Verizon MTIPS RMF process is a documented and repeatable framework that is central to the System Development Life Cycle (SDLC) that will be used for the MTIPS offering.

[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]

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

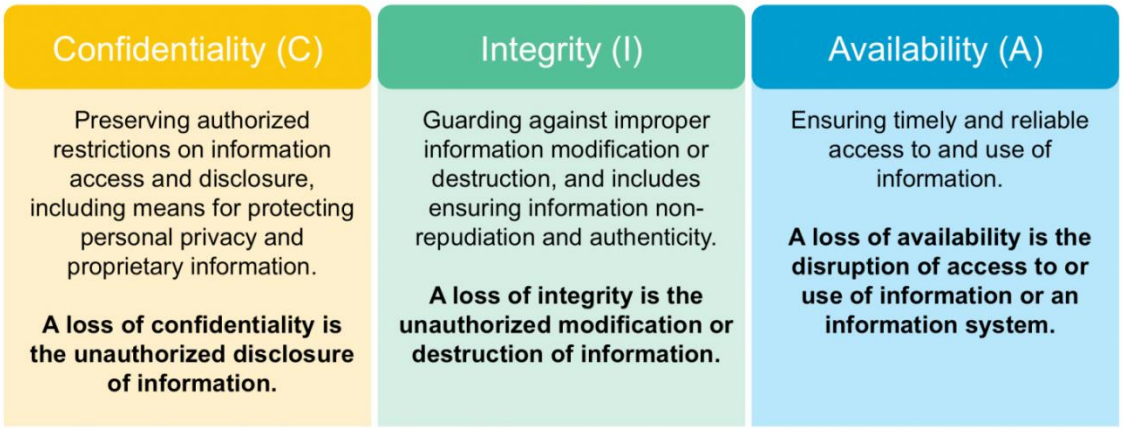
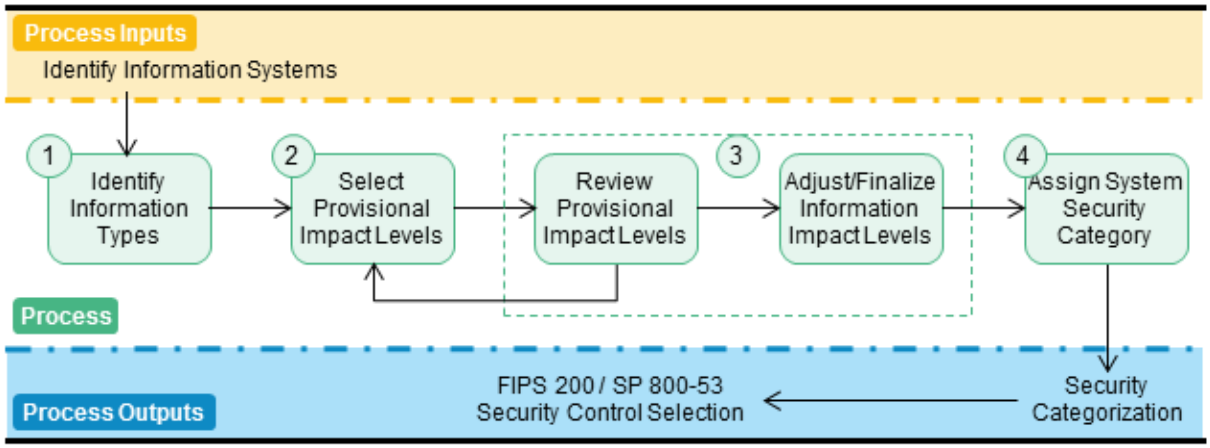


Figure B.6.1-2 shows the security categorization process defined in NIST SP 800-60 that Verizon follows. This four-step security categorization process drives the selection of baseline security controls and helps determine the information system's CIA security objectives.

Figure B.6.1-2. Security Categorization Process



[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). As shown in Figure A.6.1-3, each information type is assigned a potential impact level of Low (L), Moderate (M), or High (H) based on the potential impact of a security breach on organizations and/or individuals.

Figure B.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]

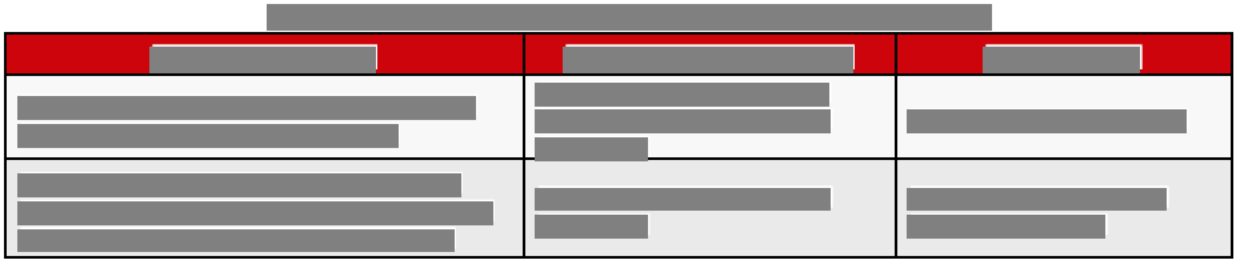
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

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

[redacted]

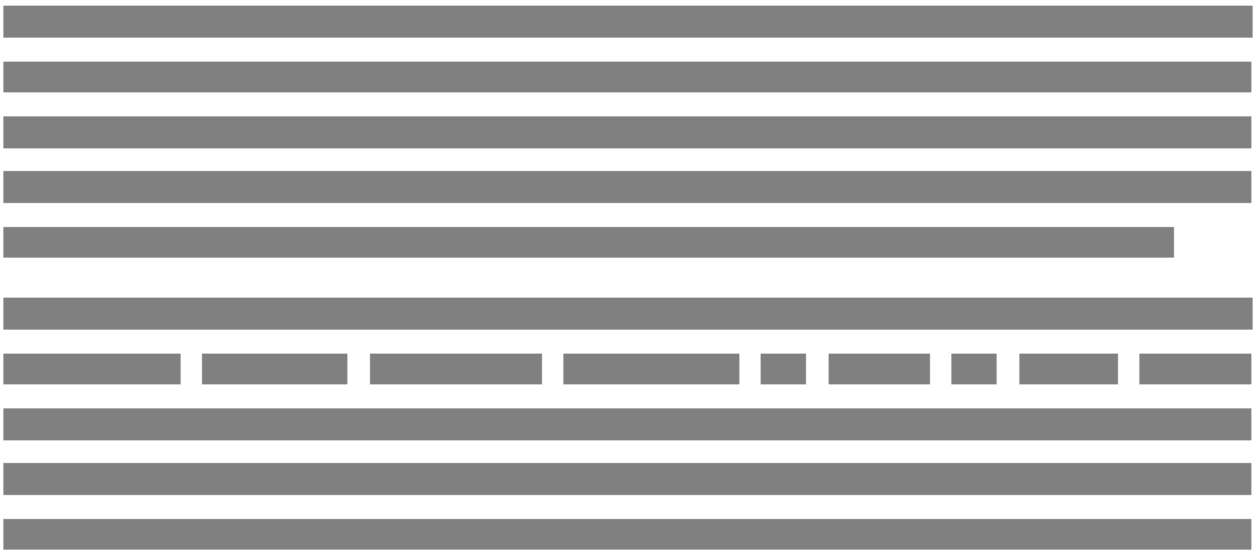


Supporting Tasks	Primary Responsibility	Deliverables

As specified in GSA IT Security Procedural Guide 06-30, **Table B.6.4-2** lists the security assessment requirements will be defined in the Security Assessment Plan and implemented for information systems per its FIPS 199 impact level:

Table B.6.4-2. Security Assessment Requirements.

Security Assessment Requirements
As a High impact information system, MTIPS will be assessed by an independent third party. The use of an independent assessment team reduces the potential for impartiality or conflicts of interest, when verifying the implementation status and effectiveness of the security controls. Verizon will engage with the third party information security organization to support the independent Security Control Assessor's evaluation of the MTIPS environment.
As a High impact information system, Verizon will conduct authenticated vulnerability scanning of servers making up the MTIPS as part of security assessment activities. Verizon currently performs authenticated vulnerability scans on Verizon systems on a recurring basis. Under the EIS program, Verizon will scan MTIPS for vulnerabilities on at least a monthly basis.
As a High impact information system with web servers, Verizon will conduct authenticated vulnerability scans for the Open Web Application Security Project (OWASP) Top Ten Most Critical Web Applications Security Vulnerabilities, using the most current update. Verizon uses the GSA OSAISO recommended WebInspect application for scanning web servers in Verizon IT systems supporting government customers. Verizon will continue to utilize WebInspect to perform vulnerability scans within the MTIPS environment. If necessary, Verizon will perform manual testing and/or verification using the latest versions of the OWASP Testing Guide and/or the GSA IT Security Procedural Guide 07-35 (or comparable customer Agency document). Verizon utilizes Telos Xacta IA Manager suite for IT risk management, which enables Verizon to continuously manage risk and security compliance and automatically manage key elements of the NIST assessment and authorization process. According to Telos, the Xacta IA Manager is deployed at over 24 federal agencies.
As a High impact information system, Verizon currently conducts authenticated database configuration reviews/testing of MTIPS database servers. Verizon currently uses the GSA OSAISO recommended AppDetective application as a tool for scanning databases and will continue to use the AppDetective tool to scan databases within the MTIPS environment.
As a High impact information system, MTIPS must complete independent penetration testing and provide an Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. Verizon will engage with GSA and/or the third party information security organization to support the independent penetration testing of the MTIPS environment.
As High impact information system, Verizon will work with the GSA OSAISO to conduct a code analyses as required by the EIS RFP. Verizon will conduct the code analysis review in accordance with GSA CIO Security Procedural Guide 12-66 using a GSA-recommended code analysis tool, specifically the Fortify Static Code Analyzer package to examine the software for common flaws. The Fortify Static Code Analyzer is used by Verizon to ensure software trustworthiness, reduce costs, increase productivity and implement secure coding best practices. The Static Code Analyzer scans source code, identifies root causes of software security vulnerabilities, correlates and prioritizes results, thus provides line–of–code guidance for closing gaps in software security. Fortify allows Verizon developers to scan code during the development cycle, enabling them to quickly identify and remediate code issues. It ensures that the most serious issues are addressed first, it then correlates and prioritizes results to deliver an accurate, risk and ranked list of issues to be resolved. Verizon designates a dedicated Code Review Team (CRT) from the Verizon Information Technology Infrastructure Management organization, to perform for IT source code review and software security. The results of this analysis will be documented in the GSA-required Code Analysis Report.



[redacted]

[redacted]

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

Figure B.6.4-1. Typical IT Security Assessment Methodology.

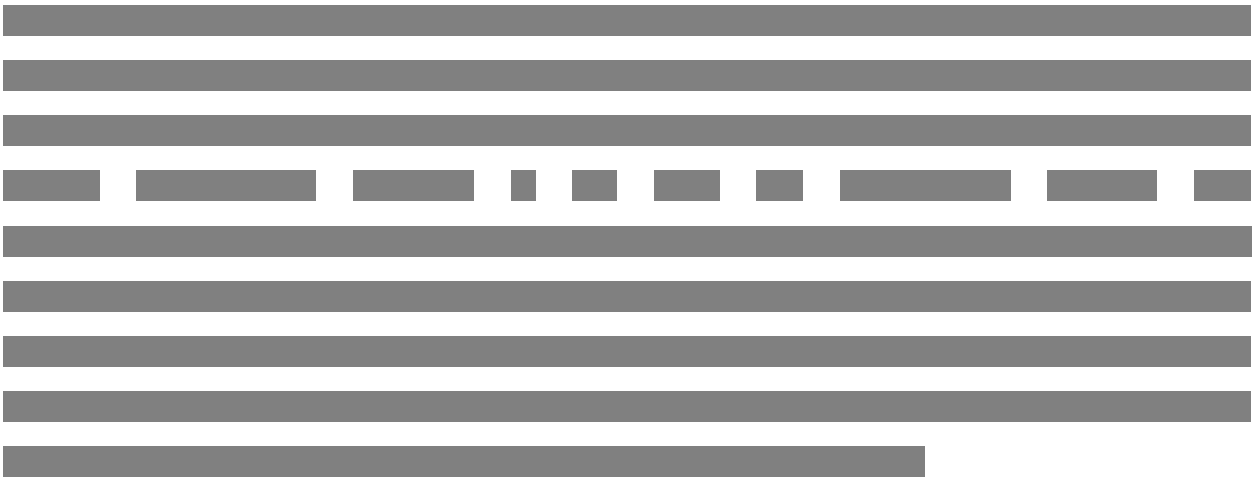
As illustrated in the figure, a typical security control assessment is conducted in three phases, the Pre-assessment, On-site Security Assessment and the Analysis & Reporting:

- **Phase 1 Pre-Assessment Phase:** During the Pre-Assessment phase, the Information System Security Manager and the Security Assessment Team plan the 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-

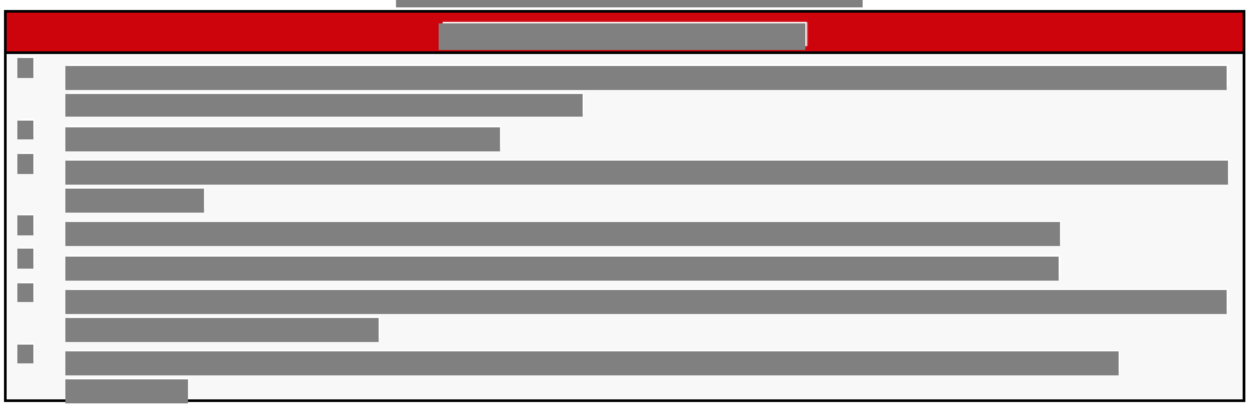
Assessment Phase. Scans will be performed as an authenticated user with elevated privileges.

The Security Assessment Team also evaluates current practices based on the recommended IT security safeguards described within the NIST and GSA 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 GSA in approximately three to four weeks. GSA 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]

d.

[redacted]

B.7 Key MTIPS Security Deliverables

[redacted]

As specified in Section **C.2.8.4.5.4** of the EIS RFP, Verizon will create, maintain and update the required security A&A documentation for the MTIPS offering.

[redacted]