GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2100.1L
January 14, 2019

GSA ORDER

SUBJECT: GSA Information Technology (IT) Security Policy

1. Purpose. This Order issues the General Services Administration's (GSA) IT Security Policy.

2. Cancellation. This Order supersedes GSA Order CIO 2100.1K, GSA Information Technology (IT) Security Policy, dated June 30, 2017.

3. Revisions. This Order provides updates for consistency with Federal requirements and program instruction implementation. Changes include:

a. Removal of Chapter 6: Policy on Privacy Controls. GSA's Privacy Act policy is provided in GSA Order CIO 1878.1, GSA Privacy Act Program;

b. Inclusion of information from new Directives: Executive Order (EO) 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure and NIST's Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1 (i.e., the Cybersecurity Framework [CSF]); and

c. Restructuring Chapters 3 through 7 and Appendix A to align with the CSF core functions of: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover.

4. Applicability.

a. This IT Security Policy applies to all GSA Federal Employees, contractors, and vendors of GSA, who manage, maintain, operate, or protect GSA systems or data, all GSA IT systems, and any GSA data contained on or processed by IT systems owned and operated by or on the behalf of any of the Services or Staff Offices.

b. This policy applies to the Office of Inspector General (OIG) only to the extent that the OIG determines it is consistent with the OIG's independent authority under the IG Act and it does not conflict with other OIG policies or the OIG mission.

c. This policy applies to the Civilian Board of Contract Appeals (CBCA) only to the extent that the CBCA determines it is consistent with the CBCA's independent authority

under the Contract Disputes Act and other authorities and it does not conflict with the CBCA's policies or the CBCA mission.

5. Signature.

/S/_____
DAVID SHIVE
Chief Information Officer
Office of GSA IT

Table of Contents

CHAPTER 1: THE GSA INFORMATION TECHNOLOGY SECURITY PROGRAM 1
1. Introduction 1
2. Objectives 1
3. Federal laws and regulations 2
4. GSA policies 3
5. Compliance and deviations 4
6. Maintenance 4
7. Definitions 5
8. NIST SP (800 Series) and GSA guidance documents 6
9. Privacy Act systems 6
10. IT security controls 6
11. Contractor operations 6
12. Cybersecurity framework 7
13. Cloud services 8

CHAPTER 2: SECURITY ROLES AND RESPONSIBILITIES 9
1. GSA Administrator 9
2. GSA Chief Information Officer (CIO) 9
3. Chief Financial Officer (CFO) 10
4. GSA Senior Agency Official for Privacy (SAOP) 11
5. GSA Chief Information Security Officer (CISO) 12
6. Heads of Services and Staff Offices (HSSOs) 13
7. GSA Chief Privacy Officer (CPO) 14
8. Authorizing Official (AO) 14
9. Office of CISO Division Directors 16
10. Information Systems Security Manager (ISSM) 17
11. Information Systems Security Officer (ISSO) 18
12. System Owners 19
13. Program Managers 22
14. Project Managers 22
15. Data Owners 22
16. Contracting Officer (CO) and CO Representative (COR) 23
17. Custodians 24
18. Authorized users of IT resources 25
19. GSA Inspector General (IG) 25
20. GSA Personnel Security Officer/ Office of Mission Assurance (OMA) 28
21. Office of Human Resources Management (OHRM) 28
22. System/Network Administrators 28
23. Supervisors 29

CHAPTER 3: POLICY FOR IDENTIFY FUNCTION 30
1. Asset management 30
2. Business environment 31

3. Governance 32
4. Risk assessment 33
5. Risk Management Strategy 34
6. Supply Chain Risk Management. 35

CHAPTER 4: POLICY FOR PROTECT FUNCTION 36
1. Identity management, authentication and access control 36
2. Awareness and training. 49
3. Data security 52
4. Information protection processes and procedures 54
5. Maintenance 57
6. Protective technology 57

CHAPTER 5: POLICY FOR DETECT FUNCTION 61
1. Anomalies and events 61
2. Security continuous monitoring 62
3. Detection processes 64

CHAPTER 6: POLICY FOR RESPOND FUNCTION 65
1. Response planning 65
2. Communications 65
3. Analysis 66
4. Mitigation 67
5. Improvements 67

CHAPTER 7: POLICY FOR RECOVER FUNCTION 68
1. Recovery planning 68
2. Improvements 68
3. Communications 68

Appendix A: CSF CATEGORIES/SUBCATEGORIES 69

CHAPTER 1: THE GSA INFORMATION TECHNOLOGY SECURITY PROGRAM

1. Introduction. The purpose of this Order is to document and set forth GSA's IT Security Policy. This IT Security Policy establishes controls required to comply with Federal laws and regulations (including Department of Homeland Security (DHS) Binding Operational Directives), and thus facilitates adequate protection of GSA IT resources.

2. Objectives. IT Security Policy objectives will enable GSA to meet its mission and business objectives by implementing systems with due consideration of IT related risks to GSA, its partners, and customers. The security objectives for system resources are to provide assurance of confidentiality, integrity, availability, and accountability by employing security controls to manage cybersecurity risk IAW Executive Order (EO) 13800 and the Cybersecurity Framework (CSF). An important component of risk-based management is to integrate technical and non-technical security mechanisms into the system to reflect sound risk management practices. All incorporated security mechanisms must be well founded, configured to perform in the most effective manner, and add value to GSA's IT-related investments. This risk based approach will enable the GSA IT Security Program to meet its goals by better securing IT systems, providing management the information necessary to justify IT Security expenditures, and assisting GSA personnel in authorizing IT systems for operation.

GSA IT security objectives include the following:

a. Confidentiality. Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and Controlled Unclassified Information (CUI). Private or confidential information is not disclosed to unauthorized individuals while at rest, during processing, or in transit.

b. Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. Safeguards must ensure information retains its content integrity. Unauthorized personnel must not be able to create, alter, copy, or delete data processed, stored, or handled by the system.

c. Availability. Ensuring timely and reliable access to and use of information. The system works promptly and service is not denied to authorized users. The system must be ready for use by authorized users when needed to perform their duties.

d. Accountability. Accountability must be to the individual level. Only personnel with proper authorization and need-to-know must be allowed access to data processed, handled, or stored on IT system components.

e. Assurance. Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy. This assurance (i.e., confidence that the other four security

objectives have been met), is provided through assessment and monitoring of security mechanisms and controls.

This Order supports GSA's IT Security Program objectives by:

- Identifying roles and assigning responsibilities in support of GSA's IT Security Program;
- Defining comprehensive and integrated security requirements that are necessary to obtain authorization to allow GSA IT systems to operate within an acceptable level of residual risk;
- Supporting GSA's objective to ensure that all outsourced cloud services are from Federal Risk and Authorization Management Program (FedRAMP) authorized (or in the process of obtaining authorization) cloud service providers, and leverage existing authorizations to operate (ATOs) from other agencies to maximize savings; and
- Supporting GSA's objective to ensure that all systems which process, store, or transmit payment card data or purchase/credit card numbers are compliant with the current version of security requirements defined in the Payment Card Industry Data Security Standard (PCI DSS).

3. Federal laws and regulations. This Order provides policies that support the implementation of the following Federal regulations and laws, and GSA directives.

- Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283)
- Clinger-Cohen Act of 1996 also known as the Information Technology Management Reform Act (ITMRA) of 1996
- CFO Act of 1990, Chief Financial Officers Act of 1990
- Paperwork Reduction Act (PRA) of 1995 (Public Law 104-13)
- Federal Financial Management Improvement Act of 1996 (FFMIA)
- Federal Managers Financial Integrity Act of 1982 (FMFIA) (Public Law 97-255)
- Government Paperwork Elimination Act (GPEA) (Public Law 105-277)
- 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
- Homeland Security Presidential Directive (HSPD-7), Critical Infrastructure Identification, Prioritization, and Protection
- OMB Circular A-11, Preparation, Submission and Execution of the Budget
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications
- OMB M-13-13, Open Data Policy -- Managing Information as an Asset
- OMB M-14-03, Enhancing the Security of Federal Information and Information Systems
- OMB M-16-16, 2016 Agency Open Government Plans

- OMB M-16-24, Role and Designation of Senior Agency Officials for Privacy
- OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information
- Public Law No: 113-274, Cybersecurity Enhancement Act of 2014
- PCI DSS, Payment Card Industry Data Security Standard
- Presidential Policy Directive (PPD-21), Critical Infrastructure Security and Resilience
- EO 13556, Controlled Unclassified Information
- EO 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- CSF, Version 1.1, Framework for Improving Critical Infrastructure Cybersecurity
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- NIST SP 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems
- NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems
- NIST SP 800-37, Revision 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach Planning Guide for Federal Information Systems
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- NIST SP 800-63-3, Digital Identity Guidelines
- NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- NIST SP 800-171, Revision 1, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations
- OPM 5 CFR Part 930.301, Subpart C, Information Security Responsibilities for Employees who Manage or Use Federal Information Systems
- Department of Homeland Security Binding Operational Directives

4. GSA policies:

- GSA Order ADM 7800.11A, Personal Use of Agency Office Equipment
- GSA Order ADM P 9732.1, Suitability and Personnel Security
- GSA Order CIO 1878.1, GSA Privacy Act Program
- GSA Order CIO 1878.2A, Conducting Privacy Impact Assessments (PIAs) in GSA
- GSA Order CIO 2100.2B, GSA Wireless Local Area Network (LAN) Security
- GSA Order CIO 2102.1, Information Technology (IT) Integration Policy
- GSA Order CIO 2103.1, Controlled Unclassified Information (CUI) Policy
- GSA Order CIO 2104.1A CHGE 1, GSA Information Technology (IT) General Rules of Behavior

- GSA Order CIO 2110.4, GSA Enterprise Architecture Policy
- GSA Order CIO 2135.2B, GSA Information Technology (IT) Capital Planning and Investment Control
- GSA Order CIO 2140.4, Information Technology (IT) Solutions Life Cycle (SLC) Policy
- GSA Order CIO 2160.2B CHGE 1, GSA Electronic Messaging and Related Services
- GSA Order CIO 9297.1, GSA Data Release Policy
- GSA Order CIO 9297.2C, GSA Information Breach Notification Policy
- GSA Order CIO P 2165.2, GSA Telecommunications Policy
- GSA Order CIO P 2180.1, GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
- GSA Order CIO P 2181.1, Homeland Security Presidential Directive-12 (HSPD-12) Personal Identity Verification and Credentialing
- GSA Order CIO P 2182.2, Mandatory Use of Personal Identity Verification (PIV) Credentials
- GSA Order OAS P 1820.1, GSA Records Management Program
- GSA Order OSC 2106.2, GSA Social Media Policy
- All GSA CIO-IT Security Procedural Guides and Technical Guides and Standards

A current list of Government-wide security guidance provided by the National Institute of Standards and Technology (NIST) is located at https://csrc.nist.gov/publications/sp.

5. Compliance and deviations.

a. Compliance is mandatory immediately upon the signing of this Order. This IT Security Policy requires all GSA Services, Staff Offices, Regions (S/SO/R), Federal employees, contractors, and other authorized users of GSA's IT resources, to comply with the security requirements outlined in this policy. This policy must be properly implemented, enforced, and followed to effectively protect GSA's IT resources and data. Appropriate disciplinary actions must be taken in a timely manner in situations where individuals and/or systems are found non-compliant. Violations of this GSA IT Security Policy may result in penalties under criminal and civil statutes.

b. All deviations from this Order must be approved by the appropriate Authorizing Official (AO) with a copy of the approval forwarded to the GSA Chief Information Security Officer (CISO) in the Office of GSA IT for concurrence. Deviations must be documented using the Acceptance of Risk process defined in GSA CIO-IT Security-06-30, Managing Enterprise Risk, including a date of resolution to comply.

c. Additionally, any exceptions or deviations to GSA IT technical guides and standards shall follow the guidelines defined therein.

6. Maintenance. The GSA Office of the Chief Information Security Officer (OCISO) is required to review this policy at least annually and revise it to:

- Reflect any changes in Federal laws and regulations;
- Satisfy additional business requirements;
- Encompass new technology; and
- Adopt new Government IT standards.

7. Definitions. The following terms are defined as listed.

a. Accountability. The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

b. Assurance. Substantiate with confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. “Adequately met” includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.

c. Availability. Ensuring timely and reliable access to and use of information.

d. Confidentiality. Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and CUI information. The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.

e. Federal information system. 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 (per 40 U.S.C. § 11331).

(1) Contractor system. An information system processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor in non-GSA facilities.

(2) Federal system (i.e., Agency system). An information system processing or containing GSA or Federal information where the infrastructure and/or applications are NOT wholly operated, administered, managed, and maintained by a Contractor.

g. Federal information. Information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

h. Integrity. Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity. The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

i. Major information system. A system that is part of an investment that requires special management attention as defined in Office of Management and Budget (OMB) guidance and agency policies, a "major automated information system" as defined in 10 U.S.C. § 2445, or a system that is part of a major acquisition as defined in Part 7 of OMB Circular A-11, Capital Programming Guide. Major information systems include those information systems with an Exhibit 300 (also referred to as Major Programs) and any Exhibit 53 information systems that are not specifically covered by a major information system's security plan.

j. Major IT investment. An investment within an IT investment portfolio that is designated as major, IAW capital planning guidance issued by the Director of OMB.

k. Minor applications (non-major information systems). Systems/applications that may be coalesced together as subsystems of a single larger, more comprehensive system for the purposes of security authorization. Minor applications/subsystems must be under the same management authority, have the same function or mission objective, the same operating characteristics, and information security needs, and reside in the same general operating environment(s).

8. NIST SP (800 Series) and GSA guidance documents. All policies shall be implemented using the appropriate special publication from NIST and/or GSA procedural guides to the greatest extent possible. Where there is a conflict between NIST guidance and GSA guidance, contact the GSA OCISO for clarification. Where there are no procedural guides, use industry best practices (e.g., Center for Internet Security Benchmarks, Defense Information Systems Agency Benchmarks). Federal Information Processing Standards (FIPS) publication requirements are mandatory for use at GSA.

Deviations from compliance to NIST special publications must be documented and approved in the same manner as described in Chapter 1, Section 5 of this policy.

9. Privacy Act systems. In addition to the security requirements in this Order, systems that contain Privacy Act data or PII must implement the additional privacy controls as defined in NIST SP 800-53, Revision 4, Appendix J: Privacy Control Catalog, GSA Order CPO 1878.1, Privacy Act Program, and GSA Order CIO P 1878.2A.

10. IT security controls. All IT systems, including those operated by a contractor on behalf of the Government, must implement proper security controls according to:

a. Its security categorization level IAW FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, and FIPS 200; and

b. The current version of NIST SP 800-53, Revision 4.

11. Contractor operations.

a. GSA System Program Managers and Contracting Officers shall ensure that the appropriate security requirements of this Order are included in task orders and contracts for all IT systems designed, developed, implemented, and operated by a contractor on behalf of GSA, including but not limited to systems operating in a Cloud Computing environment. In addition, GSA shall ensure that the contract allows GSA or its designated representative (i.e., third-party contractor) to review, monitor, test, and evaluate the proper implementation, operation, and maintenance of the security controls. This requirement includes, but is not limited to: documentation review, server configuration review, vulnerability scanning, code review, physical data center reviews, and operational process reviews and monitoring of Service Organization Control (SOC) 2/Statements on Standards for Attestation Engagements (SSAE) 18 reports.

b. The security controls implemented as part of contracts and task orders must include specific language that requires solutions to align with existing Information Security architecture. Security deliverables must be provided in a timely manner for review and acceptance by GSA. Additional information may be found in GSA CIO-IT Security-09-48, Security and Privacy Requirements for IT Acquisition Efforts. Note: As indicated in Chapter 1, Section 5, GSA has a deviation request process by which a deviation from approved security architecture/standards may be requested.

12. Cybersecurity framework.

a. EO 13800 requires all agencies to use the NIST CSF or any successor document to manage an agency's cybersecurity risk. To support this mandate, GSA has adapted this security policy and its primary procedural guides for managing risk, GSA CIO-IT Security-06-30, GSA CIO-IT Security-18-90, Information Security Program Plan, and GSA CIO-IT Security-18-91, Risk Management Strategy, to align with the CSF. GSA has also started updating its security procedural guides (based on NIST SP 800-53, Revision 4 security control families) to show alignment with the CSF. This process will continue until all guides have been updated. The CSF is organized into five core CSF Functions:

- **Identify (ID):** Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect (PR):** Develop and implement appropriate safeguards to ensure delivery of critical services.
- **Detect (DE):** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond (RS):** Develop and implement appropriate activities to take action regarding a detected cybersecurity event.
- **Recover (RC):** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

b. Chapters 3-7 of this policy are organized into the five core functions. Each chapter is further organized by the CSF's categories and subcategories which divide the

functions into outcomes and activities. Appendix A details the category and subcategory definitions and unique identifiers. Additional information is available in CSF Version 1.1.

13. Cloud services. No GSA user or S/SO/R shall conduct or acquire any type of pilot involving the use of GSA data or logons to a cloud service, platform, application or tool without first consulting with the OCISO's Security Engineering Division (ISE). Such coordination can be made by contacting ISE representatives at SecEng@gsa.gov.

a. No procurement for such products/services shall be completed without coordination through the OCISO and having obtained a valid ATO granted by a GSA AO or a FedRAMP provisional ATO.

b. GSA users or S/SO/Rs may leverage GSA authorized Cloud Service Provider offerings reviewed by the GSA Security Engineering Division (ISE) and approved by the GSA CISO. Allowed CSP offerings are identified in CSP approval memos on the IT Security Procedural Guides page.

c. The use of PII can only be involved in such products/services when the ATO grants such authorization specifically. PII shall never be introduced into any pilot program at any time.

d. Multi-Factor Authentication (MFA) shall be used when implementing any Cloud service, application or tool.

(1) Privileged accounts must use MFA when accessing any Cloud system via a network.

(2) Non-privileged accounts must use MFA when accessing a FIPS 199 Moderate or High Cloud system via a network.

e. Mobile applications that use a Cloud platform for the storage, transmission or processing of GSA data or Federal information under the management or control of GSA is subject to the above conditions.

CHAPTER 2: SECURITY ROLES AND RESPONSIBILITIES

The roles and responsibilities described in the paragraphs below are assigned to the offices and positions identified to ensure effective implementation and management of GSA's IT Security Program. The establishment of a security management structure and assigning of security responsibilities is a requirement of the FISMA.

1. GSA Administrator. The Clinger-Cohen Act of 1996 assigns the responsibility for ensuring "that the information security policies, procedures, and practices of the executive agency are adequate" to the agency head. FISMA provides the following details on agency head responsibilities for information security:

a. Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency, and on information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

b. Ensuring that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the operations of the organization;

c. Ensuring that information security management processes are integrated with agency strategic and operational, and budgetary processes;

d. Ensuring that senior agency officials within the organization are given the necessary authority to secure the information and information systems that support the operations and assets under their control;

e. Designating a Chief Information Officer (CIO) and delegating authority to that individual to ensure compliance with applicable information security requirements;

f. Ensuring that the agency has trained personnel to support compliance with information security policies, processes, standards, and guidelines; and

g. Ensuring that the CIO, in coordination with the other senior agency officials, reports annually to the GSA Deputy Administrator on the effectiveness of the agency information security program, including the progress of remedial actions.

2. GSA Chief Information Officer (CIO). Mandated by the Clinger-Cohen Act of 1996 and FISMA, the GSA CIO has overall responsibility for the GSA IT Security Program and reports to the GSA Deputy Administrator. Information security responsibilities include:

a. Developing and maintaining an agency-wide GSA IT Security Program;

b. Ensuring the agency effectively implements and maintains information security policies and guidelines;

c. Providing guidance, advice, and assistance to the Heads of Services and Staff Offices (HSSOs), and Regional Administrators (RAs) on implementing GSA's IT Security Policy;

d. Providing management processes to enable AOs to implement the components of the IT Security Program for which they are responsible;

e. Ensuring information assurance and the protection of GSA's cyber-based critical infrastructure;

f. Designating a CISO to assist in carrying out the GSA CIO's agency-wide IT security responsibilities;

g. Establishing reporting requirements within GSA to assess GSA's IT security posture, verifying compliance with Federal requirements and approved policies, and identifying agency-wide IT security needs;

h. Conducting independent activities and compliance reviews including oversight of GSA's Assessment and Authorization (A&A) process;

i. Coordinating and reporting on PPD-21 critical infrastructure assets;

j. Reporting annually, in coordination with the other senior agency officials, to the GSA Deputy Administrator on the effectiveness of the agency information security program, including progress of remedial actions;

k. Ensuring Privacy Threshold Analyses (PTAs) and Privacy Impact Assessments (PIAs) prepared by GSA organizations for security considerations are reviewed;

l. Providing guidance or input for periodic assessments of S/SO/R security measures and goals to assure implementation of GSA policy and procedures; and

m. Participating as a member of the GSA Full Response Team IAW GSA Order 9297.2C to determine if a major incident has occurred.

3. Chief Financial Officer (CFO). The CFO also has major statutory security responsibilities under the CFO Act of 1990 and the Clinger-Cohen Act of 1996. Responsibilities include:

a. Developing and maintaining an integrated agency accounting and financial management system, including financial reporting and internal controls, which comply with FMFIA and FFMIA requirements;

b. Complying with such policies and requirements as may be prescribed by the Director of OMB;

c. Complying with applicable accounting principles, standards, and requirements, and internal control standards and any other requirements applicable to such systems;

d. Supporting the GSA IT Capital Planning Process. To achieve satisfactory assurance levels of information security for the financial systems of GSA, close cooperation between the offices of the CFO and the CIO is necessary, including supporting the GSA IT Capital Planning process; and

e. Reporting financial management information to OMB as part of the President's budget to include:

(1) Complying with legislative and OMB-defined responsibilities as they relate to IT capital investments; and

(2) Ensuring the appropriate security requirements of this Order are included in all contracts for IT systems designed, developed, implemented, and operated by a contractor that hosts GSA financial systems. This includes, but is not limited to: documentation review of operational processes and reviews that monitor SSAE 18 reporting submissions.

4. GSA Senior Agency Official for Privacy (SAOP). The SAOP has major statutory responsibilities under the Privacy Act of 1974, GSA Order CIO 1878.1, OMB A-130, and OMB M-16-24. Information security responsibilities include:

a. Ensuring GSA information systems that contain PII address any recommendations of the SAOP as part of the system A&A, including addressing the privacy controls in Appendix J of NIST SP 800-53, Revision 4, as appropriate;

b. Ensuring that GSA data assets go through media protection processes IAW GSA CIO-IT Security-06-32: Media Protection (MP) prior to public release and that applicable Privacy Policies are followed;

c. Ensuring PTAs and PIAs are conducted for electronic information systems and collections and coordinating submission of all GSA Privacy Analysis Worksheets and PIA Summaries to OMB;

d. Developing, implementing, and overseeing personnel security controls for access to PII;

e. Directing the planning and implementation of the GSA Privacy Program to ensure agency personnel, including contractors, receive appropriate privacy awareness training based on their roles and access to privacy data; and

f. Participating as the GSA Full Response Team leader IAW GSA Order 9297.2C if a major incident involving privacy has occurred.

5. GSA Chief Information Security Officer (CISO). FISMA establishes the designation of a Senior Agency Information Security Officer. GSA has assigned that responsibility to the CISO. The CISO is the focal point for all GSA IT security and must ensure the security requirements described in this Order are implemented agency-wide. The CISO reports directly to the CIO as required by FISMA. Responsibilities include:

a. Reporting to the GSA CIO on the implementation and maintenance of the GSA's IT Security Program and Security Policies;

b. Reporting to the GSA CIO on activities and trends that may affect the security of systems and applications assigned to GSA;

c. Implementing and overseeing GSA's IT Security Program by developing and publishing security policies and IT security procedural guides that are consistent with this policy;

d. Ensuring written agreements assign security-related functions and identify security responsibilities of each S/SO/R or activity when two or more activities use the same IT;

e. Providing guidance, advice, and assistance to all S/SO/R on IT security issues, the IT Security Program, and security policies;

f. Reporting to agency senior management on policy compliance;

g. Directing the planning and implementation of the GSA IT Security Awareness Training Program to ensure agency personnel, including contractors, receive appropriate security awareness training based on their roles and access to information and information systems;

h. Managing the CIO Office of the CISO which implements the GSA IT Security Program;

i. Establishing reporting deadlines for IT Security related issues requiring an agency response affecting the GSA IT Security Program;

j. Performing information security duties as the primary duty;

k. Assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems supporting the operations and assets of the agency on a periodic basis;

l. Testing and evaluating the effectiveness of information security policies, procedures, and practices on a periodic basis;

m. Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

n. Ensuring the development and implementation of procedures for detecting, reporting, and responding to security incidents;

o. Ensuring preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of GSA;

p. Supporting the GSA CIO in annual reporting to the GSA Administrator on the effectiveness of the agency information security program, including progress of remedial actions;

q. Developing and implementing IT security performance measures to evaluate the effectiveness of technical and non-technical safeguards used to protect GSA information and information systems;

r. Assessing S/SO/R security measures and goals periodically to assure implementation of GSA policy and procedures;

s. Ensuring the appointment in writing of Information Systems Security Managers (ISSMs) and Information Systems Security Officers (ISSOs) for GSA systems;

t. Administering FISMA requirements and coordinating GSA's annual FISMA security program review and Plan of Action and Milestones (POA&M) implementations;

u. Ensuring IT Acquisitions align with GSA information security requirements;

v. Participating as the GSA Full Response Team leader IAW GSA Order 9297.2C , if a major non-privacy incident has occurred; and

w. Concurring/Non-concurring on ATOs as specified in GSA CIO-IT Security-06-30 and its related A&A procedural guides.

6. Heads of Services and Staff Offices (HSSOs). HSSOs are senior officials or executives within GSA with specific mission or line of business responsibilities. They are responsible for coordinating the efforts of management and technical personnel under their jurisdiction in meeting GSA IT Security requirements. Responsibilities include:

a. Ensuring that contractors performing services associated with GSA systems (such as system development, maintenance, or operation) are subject to GSA security requirements; and

b. Tracking the performance measures and goals established by the CISO and ensuring AOs, ISSMs, and ISSOs support these measures.

7. GSA Chief Privacy Officer (CPO). The CPO is responsible for overseeing GSA's Privacy Program whose mission it is to preserve and enhance privacy protections for all individuals whose personal information is handled by GSA and to encourage transparency of GSA operations involving personal information. The CPO reports to the SAOP. Information security responsibilities include:

a. Confirming that GSA information systems containing PII address any recommendations of the SAOP as part of the system A&A, including addressing the privacy controls in NIST SP 800-53, Revision 4, as appropriate;

b. Verifying that GSA data assets go through media protection processes IAW GSA CIO-IT Security-06-32, prior to public release and that applicable privacy policies are followed;

c. Verifying PTAs and PIAs are conducted for electronic information systems and collections and coordinating submission of all GSA Privacy Analysis Worksheets and PIA Summaries to OMB;

d. Managing the implementation of personnel security controls for access to PII; and

e. Participating as a member of the GSA Full Response Team IAW GSA Order 9297.2C.

8. Authorizing Official (AO). An AO is the Federal Government management official with the responsibility of identifying the level of acceptable risk for an IT system or application and determining whether the acceptable level of risk has been obtained. Final authority to operate or not operate the system rests with the AO. An AO must be assigned to every information system. An AO may have responsibility for more than one system, provided there is no conflict. Responsibilities include:

a. Reviewing and approving security safeguards of information systems and issuing ATO approvals for each information system under their purview based on the acceptability of the security safeguards of the system (risk-management approach);

b. Reviewing and approving all deviations from this Order as described in Chapter 1, Section 5 of this Order.

c. Ensuring all systems under their purview have a current ATO issued IAW A&A processes defined in GSA CIO-IT Security-06-30;

d. Ensuring ATO extensions are issued only based on the conditions identified in Chapter 3, Section 3.l and 3.m;

e. Ensuring vulnerability scans are able to be performed on systems under their purview IAW GSA CIO-IT Security-17-80: Vulnerability Management Process. Vulnerabilities identified from the scans shall be resolved and/or tracked in the systems' POA&M IAW GSA CIO-IT Security-09-44: POA&M and GSA CIO-IT Security-06-30;

f. Providing support to the ISSMs and ISSOs appointed by the GSA CISO for GSA systems under their purview;

g. Ensuring IA is included in management planning, programming budgets, and the IT Capital Planning process;

h. Requiring point(s) of contacts (POCs) within other Federal agencies or outside organizations that manage GSA systems be maintained for systems under their purview. These POCs will be used for notification and coordination of security issues;

i. Ensuring IT systems handling privacy data meet the privacy and security requirements of the Privacy Act and IT information security laws and regulations. This includes GSA Order CIO 1878.1, GSA Order CIO 1878.2A, and NIST SP 800-53, Revision 4;

j. Reviewing and approving PIAs for systems under their purview;

k. Supporting the security measures and goals established by the CISO;

l. Ensuring all incidents involving data breaches which could result in identity theft are coordinated through OCISO and the GSA Full Response Team using the GSA breach notification plan per OMB M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, GSA CIO-IT Security-01-02: Incident Response (IR), and GSA Order 9297.2C;

m. Ensuring contingency plans are developed and tested annually IAW OMB Circular A-130, NIST SP 800-34, Revision 1, Contingency Planning Guide for Federal Information Systems, and GSA CIO-IT Security-06-29: Contingency Planning (CP);

n. Implementing detailed separation of duties policies for IT systems based on the specific processes, roles, permissions, and responsibilities of personnel involved in GSA business operations;

o. Establishing physical and logical access controls to enforce separation of duties policies and alignment with organizational and individual job responsibilities;

p. Ensuring access to systems by members of the GSA OIG as described in paragraph 19 of this chapter;

q. Establishing, where appropriate, system/organization unique rules of behavior for systems under their purview; and

r. Ensuring IT systems handling payment card data meet the security requirements of the PCI DSS.

9. Office of CISO Division Directors. OCISO Directors serve as an intermediary to the AO for ensuring security is implemented. The Directors are the focal point for all IT system security matters for the IT resources under their responsibility. OCISO Directors report to the CISO. Responsibilities include:

a. Monitoring adherence and proper implementation of GSA's IT Security Policy and reporting the results to the CISO;

b. Reviewing and approving A&A documents to be signed by the appropriate business line representatives and concurred by the CISO or appropriate OCISO personnel;

c. Ensuring the security measures and goals established by the CISO are met by the organizations under their responsibility;

d. Ensuring GSA security awareness training requirements for individuals under their responsibility are complied with;

e. Creating security policies that achieve compliance to appropriately address new security requirements;

f. Advising individuals with IT Security responsibilities on proper system security, security "Best Practices," and applicable laws and regulations;

g. Assisting individuals with IT Security responsibilities on security architecture and security engineering principles and practices;

h. Interfacing with the Technical Standards Committee (TSC) with regard to security;

i. Developing, implementing, and tracking the collection of data and reporting of status on POA&Ms, FISMA requirements, and other external or internal requests or requirements (e.g., OIG, Government Accountability Office [GAO]).

j. Coordinating the designation, documentation, and inheritance of common controls with individuals who have IT Security responsibility for information systems;

k. Coordinating the implementation of on-going authorization and continuous monitoring processes with individuals with IT Security responsibility for information systems;

l. Coordinating with System Owners, ISSMs, and ISSOs to maintain an accurate inventory of GSA information systems (including hardware, software, and other data required by Federal or GSA requirements) in the GSA official system inventory repository;

m. Developing and implementing procedures for detecting, reporting, and responding to security incidents.

n. Managing an OCISO Division to implement the GSA IT Security Program; and

o. Appointing ISSMs and ISSOs in writing for GSA systems.

10. Information Systems Security Manager (ISSM). The ISSM serves as an intermediary to the system owner and the OCISO Director responsible for ISSO services. There is at least one ISSM per AO. The ISSM reports to the OCISO IST Director for the systems under their purview. An individual appointed as ISSM for a system cannot also be assigned as the ISSO for the same system. ISSMs must be Federal employees. A current list of ISSMs is located in the GSA official system inventory repository. Responsibilities include:

a. Providing guidance, advice, and assistance to ISSOs on IT security issues, the IT Security Program, and security policies;

b. Verifying annually the list of ISSOs and providing an updated designation letter to the Director for submission to the CISO when changes occur or designations expire;

c. Ensuring A&A support documentation is developed and maintained for the life of the system;

d. Reviewing and coordinating reporting of Security Advisory Alerts (SAA), compliance reviews, security awareness training, incident reports, contingency plan testing, and other IT security program elements;

e. Managing system assessments (including A&A package requirements and PCI DSS Report on Compliance [for IT systems that process, store, or transmit payment card data or purchase/credit card numbers]), and forwarding them to the AO and appropriate OCISO Directors;

f. Forwarding to the applicable OCISO Director, copies of A&A documents to be signed by the appropriate individuals as required in A&A guidance;

g. Supporting the security measures and goals established by the CISO; and

h. Complying with GSA security awareness training requirements for individuals with significant security responsibilities.

11. Information Systems Security Officer (ISSO). The ISSO is responsible for ensuring implementation of adequate system security in order to prevent, detect, and recover from security breaches. An ISSO must be assigned for every information system. An ISSO may have responsibility for more than one system, provided there is no conflict. An individual assigned as the ISSO cannot also be the ISSM or System Owner, for the same system. ISSOs may be Federal employees or contractors. The ISSO must be knowledgeable of the information and processes supported by the system. An ISSO Checklist consolidating recurring tasks ISSOs must perform is available on Google Drive; the checklist is limited to personnel who require access to perform their duties. A current list of ISSOs is located in the GSA official system inventory repository, GSA EA Analytics and Reporting, (GEAR). Responsibilities include:

a. Ensuring the system is operated, used, maintained, and disposed of IAW documented security policies and procedures. Necessary security controls should be in place and operating as intended;

b. Advising System Owners of risks to their systems and obtaining assistance from the ISSM, if necessary, in assessing risk;

c. Assisting system owners in completing and maintaining the appropriate A&A documentation as specified in GSA CIO-IT Security-06-30;

d. Performing the recurring activities as listed in the ISSO Checklist;

e. Assisting the AO, Data Owner and Contracting Officer (CO)/Contracting Officer Technical Representative (COTR) in ensuring users have the required background investigations, the required authorization and need-to-know, and are familiar with internal security practices before access is granted to the system;

f. Promoting information security awareness;

g. Identifying, reporting, and responding to information security incidents in coordination with GSA's incident responders, including beginning protective and corrective measures as directed;

h. Ensuring the user identification and authentication scheme used in the system is administered as intended, including reviewing system role assignments to validate compliance with principles of least privilege;

i. Ensuring media protection procedures are followed IAW GSA CIO-IT Security-06-32;

j. Reviewing audit/log reports for systems integrated with the GSA Enterprise Logging Platform (ELP) for potential security issues;

k. Verifying systems not integrated with the GSA ELP/audit logging tool perform similar reviews to identify potential security issues;

l. Evaluating SAAs and known vulnerabilities to ascertain if additional safeguards are needed, and ensuring systems are patched and securely configured, as appropriate;

m. Supporting the security measures and goals established by the CISO;

n. Complying with GSA security awareness training requirements for individuals with significant security responsibilities;

o. Assisting the AO in achieving PCI DSS implementation and compliance for IT systems that process, store, or transmit payment card data, to include creating and maintaining PCI DSS documentation, and facilitating the self-assessment;

p. Assisting in the identification, implementation, and assessment of a system's security controls, including common controls; and

q. Coordinating with the OCISO to maintain an accurate inventory of GSA information systems (including hardware, software, and other data required by Federal or GSA requirements) in the GSA official system inventory.

12. System Owners. System Owners are management officials within GSA with responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems. System Owners cannot be ISSOs. System Owners represent the interests of the system throughout its lifecycle. Primary responsibility for managing risk should rest with the System Owners. Responsibilities include:

a. Ensuring systems and the data each system processes have necessary security controls in place and are operating as intended and protected IAW GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM;

b. Obtaining the resources necessary to securely implement and manage their respective systems;

c. Consulting with the ISSM and ISSO and receiving the approval of the AO, when selecting the mix of controls, technologies, and procedures that best fit the risk profile of the system;

d. Participating in activities related to the A&A of the system to include security planning, risk assessments, security and incident response testing, configuration management, and contingency planning and testing;

e. Coordinating with the OCISO and the ISSO to maintain an accurate inventory of GSA information systems (including hardware, software, and other data required by Federal or GSA requirements) in the GSA official system inventory;

f. Defining and scheduling software patches, upgrades, and system modifications;

g. Ensuring IT security and privacy requirements are included in IT contracts or contracts including IT;

h. Conducting PTAs on all systems to ascertain whether the system collects information on individuals or when new systems are developed, acquired, or purchased; performing PIAs when applicable;

i. Developing, implementing and maintaining an approved IT contingency plan which includes an acceptable Business Impact Analysis (BIA);

j. Ensuring that information and system categorization has been established for their systems and data IAW FIPS 199, Standards for Security Categorization of Federal Information and Information Systems;

k. Conducting annual reviews and validation of system users' accounts to ensure the continued need for access to a system and verify users' authorizations (rights/privileges);

l. Ensuring security is planned, documented, and integrated into the system development life cycle (SDLC) from the information system's initiation phase to the system's disposal phase;

m. Reviewing the security controls for their systems and networks annually as part of the FISMA self-assessment, when significant changes are made to the system and network, and at least every three years or via continuous monitoring if the system is in GSA's information security continuous monitoring program;

n. Defining, implementing, and enforcing detailed separation of duties by ensuring single individuals do not have control of the entirety of a critical process, roles, permissions, and/or responsibilities;

o. Ensuring physical or environmental security requirements are implemented for facilities and equipment used for processing, transmitting, or storing sensitive information based on the level of risk;

p. Obtaining a written ATO following GSA A&A processes prior to making production systems operational and/or Internet accessible. Developing and maintaining the system security plan and ensuring that the system is deployed and operated according to the agreed-upon security requirements;

q. Ensuring system users and support personnel receive the requisite security awareness training (e.g., instruction in system rules of behavior);

r. Supporting the security measures and goals established by the CISO;

s. Complying with GSA security awareness training requirements for individuals with significant security responsibilities;

t. Integrating and explicitly identifying security funding for information systems and programs into IT investment and budgeting plans;

u. Coordinating with IT security personnel, including the ISSM and ISSO and Data Owners, to ensure implementation of system and data security requirements;

v. Working with the ISSO and ISSM to develop, implement, and manage POA&Ms for their respective systems IAW GSA CIO-IT Security-09-44;

w. Ensuring proper separation of duties for GSA IT system maintenance, management, and development processes;

x. Conducting annual assessments to review the effectiveness of control techniques, with an emphasis on activities that cannot be controlled through logical, physical, or compensating controls;

y. Working with the Data Owner, granting access to the information system based on a valid need-to-know/need-to-share that is determined during the account authorization process and the intended system usage;

z. Working with Data Owners to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities, and archived for a period of not less than 180 days;

aa. Working with Data Owners to audit user activity for indications of fraud, misconduct, or other irregularities;

bb. Working with Data Owners to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity;

cc. Reviewing the security requirements for systems and networks which are in-scope of PCI DSS annually as part of the PCI DSS assessment and when significant changes are made to the system and network;

dd. Working with the OCISO and Data Owners to respond to any information security incidents that impact the system or the data stored within the system; and

ee. Participating as a member of the GSA Full Response Team as defined in GSA Order 9297.2C to determine if a major incident has occurred.

13. Program Managers. Program Managers are management officials within GSA who are responsible for developing, implementing, and/or overseeing multi-year IT initiatives that must be carried out through multiple related projects. A program manager focuses on the strategic goals of GSA. Their role is to manage a number of related projects in a coordinated manner to attain strategic results that could not be achieved at the individual project level. Responsibilities include:

a. Ensuring the appropriate security requirements of this Order are included in task orders and contracts for all IT systems designed, developed, implemented, and operated by a contractor on behalf of the Government;

b. Ensuring cyber risk is adequately managed within the projects under their purview IAW GSA CIO-IT Security-18-90, GSA CIO-IT Security-18-91, and GSA CIO-IT Security-06-30; and

c. Coordinating the projects under their purview to ensure resources are allocated, monitored, and managed to support the required level of security.

14. Project Managers. Project Managers are management officials within GSA who are responsible for managing a project within a larger program. A project manager focuses on managing a team to achieve the goals of the project. Responsibilities include:

a. Ensuring GSA IT security policies and procedural requirements are integrated and cyber risk is adequately managed within projects under their purview IAW GSA CIO-IT Security-18-91 and GSA CIO-IT Security-06-30; and

b. Managing the schedule, resources, and tasks within a project, ensuring security is delivered.

15. Data Owners. The Data Owner/Functional Business Line Manager owns the information but not the system, application, or platform on which the information is stored, transmitted, or processed. Responsibilities include:

a. Determining the security categorization of systems based upon the FIPS 199 levels and ensuring that System Owners are aware of the sensitivity of data to be handled;

b. Coordinating with System Owners, ISSMs, ISSOs, and Custodians to ensure the data is properly stored, maintained, and protected IAW GSA policies, regulations and any additional guidelines established by GSA;

c. Working with the System Owner, with assistance from the ISSO, to ensure system access is restricted to authorized users that have completed required

background investigations, are familiar with internal security practices, and have completed requisite security awareness training programs (e.g., the annual IT Security Awareness Training and Sharing Information in a Collaborative Environment training);

d. Reviewing access authorization listings and determining whether they remain appropriate at least annually;

e. Ensuring protection of GSA's systems and data IAW GSA's IT Security Policy and the GSA Records Management Program;

f. Ensuring that data is not processed on a system with security controls that are not commensurate with the sensitivity of the data;

g. Assisting in identifying and assessing common security controls where the information resides;

h. Ensuring information systems that allow authentication of users for the purpose of conducting Government business electronically complete a Digital Identity Acceptance Statement for digital transactions resulting in an assurance level classification IAW NIST SP 800-63-3, Digital Identity Guidelines;

i. Coordinating with IT security personnel including the ISSM and ISSO and system owners to ensure implementation of system and data security requirements;

j. Working with the System Owner to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities, and archived for a period not less than 180 days;

k. Working with the System Owner to audit user activity for indications of fraud, misconduct, or other irregularities;

l. Working with the System Owner to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity;

m. Identifying the data assets to catalog in GSA’s Enterprise Data Inventory (EDI) and for possible public release; and

n. Working with the OCISO and System Owner to respond to any information security incidents that impact a system or the data stored within a system.

16. Contracting Officer (CO) and CO Representative (COR). The CO/COR function is responsible for managing contracts and overseeing their implementation. Personnel executing this function have the following responsibilities in regards to information security:

a. Collaborating with the CISO or other appropriate official to ensure that the agency's contracting policies adequately address the agency's information security requirements;

b. Coordinating with the CISO or other appropriate official as required ensuring that all agency contracts and procurements are compliant with the agency's information security policy, and include appropriate security contracting language and security requirements in each contract;

c. Ensuring that all personnel with responsibilities in the agency's procurement process are properly trained in information security;

d. Working with the CISO to facilitate the monitoring of contract performance for compliance with the agency's information security policy;

e. Identifying, initiating, and adhering to favorable enter on duty requirements for contractor background investigations in collaboration with the GSA Personnel Security Officer/Office of Mission Assurance (OMA);

f. Ensuring contracts and task orders for ISSM and ISSO services include performance requirements that can be measured;

g. Maintaining the integrity and quality of the proposal evaluation, negotiation, and source selection processes while ensuring that all terms and conditions of the contract are met;

h. Ensuring industry and Government IT providers use Security Content Automation Protocol (SCAP) validated tools with the United States Government Configuration Baseline (USGCB) scanner capability to certify their products operate correctly with USGCB configurations and do not alter USGCB settings; and

i. Ensuring new solicitations for all GSA IT systems include the security contract language from GSA CIO-IT Security-09-48.

17. Custodians. Custodians own the hardware platforms and equipment on which the data is processed. They are the individuals in physical or logical possession of information from Data Owners. Responsibilities include:

a. Coordinating with data owners and system owners to ensure the data is properly stored, maintained, and protected;

b. Providing and administering general controls such as back-up and recovery systems consistent with the policies and standards issued by the Data Owner;

c. Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the AO;

d. Accessing data only on a need-to-know basis as determined by the Data Owner; and

e. Providing the OCISO physical access to devices when needed as part of any incident response effort.

18. Authorized users of IT resources. Authorized users of GSA IT resources, including all Federal employees and contractors, either by direct or indirect connections, are responsible for complying with GSA's IT Security Policy and procedures. Their responsibilities include:

a. Complying with security awareness training and education sessions commensurate with their duties;

b. Reporting any observed or suspected security problems/incidents to the IT Service Desk;

c. Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act requirements, copyright requirements, and procurement-sensitive data;

d. Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password protected screen saver, and removing their PIV card before leaving their workstation;

e. Utilizing assigned privileged access rights (e.g., administrator, power user, database administrator, web site administrator, etc.) to a computer based on need-to-use (i.e., using accounts with those privileges only when the privileges are required to complete an action);

f. Ensuring PII and/or sensitive data stored on any workstations or mobile devices including, but not limited to, laptop computers, notebook computers, external hard drives, USB drives, CD-ROMs/DVDs, and personal digital assistants is encrypted with GSA provided encryption;

g. Ensuring PII and/or sensitive data is only accessed remotely from Government Furnished Equipment (GFE) or through an approved GSA virtual interface (i.e., Citrix and/or VDI). Note: Remote access is permitted unless a system's AO or SAOP explicitly prohibit such access; and

h. Ensuring PII and/or sensitive data is not downloaded or stored on non-GFE.

19. GSA Inspector General (IG). The GSA IG is a statutory office within GSA that, in addition to other responsibilities, works to assess an organization's information security

practices and identifies vulnerabilities and the possible need to modify security measures. The OIG completes this task by:

a. Detecting fraud or instances of waste, abuse, or misuse of an organization's funds;

b. Identifying operational deficiencies within the organization;

c. Performing annual independent FISMA evaluations IAW 44 U.S.C. § 3555(b)(1);

d. Accessing GSA and contractor records. OIG auditors, investigators, inspectors, and attorneys must be provided access to all records, reports, reviews, documents, papers, and materials available to GSA and pertaining to agency programs and activities. When performing reviews of contractor records and proposals, access to information is provided by statute, contract terms, and agreements between the contractor and the Government. To facilitate the process of gaining access to information, auditors, investigators, inspectors, and attorneys carry credentials identifying them as OIG officials. In addition, the following procedures will be followed to allow OIG personnel access to GSA electronic systems:

(1) For the OIG, the point of contact will be the Assistant Inspector General for Auditing (AIGA) or his/her designees. For the S/SOs within GSA, the points of contact will be the AO for each information system;

(2) The AIGA will notify the AO of the electronic system within his or her purview to which OIG personnel need access;

(3) The AO will inform the AIGA what the highest classification level is of information on the system and all security and privacy awareness training that is required of GSA and/or contractor personnel in order to access the system;

(4) The AIGA will designate the OIG personnel who are to be given access and ensure they have appropriate clearance levels;

(5) The AIGA will certify that each OIG person who may have access to the system has completed all security and privacy awareness training required of GSA personnel before access is granted;

(6) The AIGA will annually certify that each OIG person with access to a GSA system has a continuing need for access and has maintained up-to-date training requirements in connection with the system owner's annual review and validation of systems users' accounts;

(7) The AIGA will ensure and state that access is necessary for OIG personnel to accomplish assigned tasks IAW the OIG's organizational mission and functions. The following statement from the AIGA will suffice to establish that access is necessary for

these purposes: “This access is requested to fulfill the OIG’s statutory responsibility to conduct and supervise audits, inspections, and investigations relating to the programs and operations of GSA, and to promote economy, efficiency and effectiveness in the administration of, and to prevent and detect fraud, waste, and abuse in GSA programs and operations;”

(8) With regard to requests for access to Privacy Act systems of records, the AIGA will ensure and certify that the OIG personnel who will be accessing the system have a need for the records in the performance of their duties. The statement shall suffice to establish that access to the system is consistent with the requirements of the Privacy Act;

(9) The AO will work with the system owner to ensure access is granted promptly after the above steps have been completed. If access cannot be granted within fourteen (14) calendar days after completion of the above steps, the AO will inform his/her HSSO and the AIGA and will work with the AIGA to resolve any impediments to OIG access to the system. The CIO, or designee, will assist as requested in resolving any issues;

(10) The system owner will authorize OIG personnel to access GSA-owned information systems from the OIG’s accredited system. When possible under contractual terms, OIG personnel will be authorized access to contractor-owned information systems from the OIG’s accredited system;

(11) To the extent practicable, OIG personnel will not be granted access to other agencies’ owned or controlled records or information about other agencies and their employees that may be maintained in a GSA-controlled system, absent the other agency’s permission;

(12) The OIG will advise the AO immediately if circumstances change such that access is no longer needed; for example, if an individual with access leaves the OIG, or upon conclusion of the investigation/inspection/audit or other OIG purpose for which systems access was provided;

(13) OIG employees will have “read-only” access to all information in the system. OIG personnel will not be able to add to, delete, or modify the data in the system;

(14) Each OIG employee with access will use a unique identifier and password when accessing the system;

(15) Testing in support of an OIG review, whether manual or automated, shall not have an adverse effect on the operational production status of the IT system being reviewed other than the increase in usage/traffic due to additional users;

(16) OIG operational needs may preclude OIG staff from obtaining the required approvals prior to removal of PII from GSA facilities. The following statement from the AIGA will suffice to establish that requirement is necessary for these purposes: “This access is requested to fulfill the OIG’s statutory responsibility to conduct and supervise audits, inspections, and investigations relating to the programs and operations of GSA, and to promote economy, efficiency and effectiveness in the administration of, and to prevent and detect fraud, waste, and abuse in, GSA programs and operations”; and

(17) Should the system be compromised by a reportable incident, and the access of OIG personnel be implicated in the incident, the system owner will promptly notify the IG in writing, and the IG will take appropriate action with respect to the employee(s) responsible.

20. GSA Personnel Security Officer/ Office of Mission Assurance (OMA). The GSA personnel security officer is responsible for the overall implementation and management of personnel security controls across GSA, to include integration with specific information security controls. In consideration of information security, the personnel security officer has responsibility for:

a. Developing, promulgating, implementing, and monitoring GSA personnel security programs;

b. Developing and implementing access agreements, and personnel screening, termination, and transfer procedures; and

c. Ensuring consistent and appropriate sanctions for personnel violating management, operation, or technical information security controls.

21. Office of Human Resources Management (OHRM). The Human Resource Office and Security Office are responsible for:

a. Designating the risk levels for all occupations in GSA and incorporate the risk level in the position designation(s) for each series and grade.

22. System/Network Administrators. System/Network Administrators are responsible for:

a. Ensuring the appropriate security requirements are implemented consistent with GSA IT security policies and hardening guidelines;

b. Implementing system backups and remediation of security vulnerabilities, including patching, updates, configuration changes, etc.;

c. Utilizing privileged access rights (e.g., “administrator,” “root,” etc.) to a computer based on a need-to-use basis (i.e., using accounts with those privileges only when the privileges are required to complete an action);

d. Working with the Custodian/ISSO to ensure appropriate technical security requirements are implemented;

e. Ensuring system/network administrators have separate administrator and user accounts, if applicable (e.g., Microsoft Windows accounts). A normal user account should be used unless administrator rights are required to perform a job function;

f. Identifying and reporting security incidents and assisting the OCISO in resolving the security incident;

g. Utilizing GSA provided MFA to ensure strong authentication; and

h. Performing audit/log reviews for systems not integrated with the GSA Enterprise Logging Platform to identify potential security issues as specified in the system's system security plan (SSP).

23. Supervisors. Supervisors are responsible for:

a. Conducting annual review and validation of staff user accounts to ensure the continued need for access to a system;

b. Conducting annual reviews of staff training records to ensure annual IT Security Awareness Training, and application specific training has been completed for all users. The records shall be forwarded to ISSOs/system owners as part of the annual recertification efforts;

c. Coordinating and arranging system access requests for all new or transferring employees and verifying an individual's need-to-know (authorization);

d. Coordinating and arranging system access termination for all terminating or transferring personnel;

e. Coordinating and arranging system access modifications for personnel; and

f. Documenting job descriptions and roles to accurately reflect the assigned duties, responsibilities, and separation of duties principles. Establishing formal procedures to guide personnel in performing their duties, with identification of prohibited actions.

CHAPTER 3: POLICY FOR IDENTIFY FUNCTION

This chapter provides security policy statements for the Identify function of the CSF. The Identify function allows GSA to develop an understanding of its systems, assets, data, and capabilities in order to manage cybersecurity risk. Use of the activities in the Identify function will enable GSA to prioritize its efforts consistent with its risk management strategy and business needs, by understanding the business context, the resources supporting critical functions, and related cybersecurity risks.

The following paragraphs provide the CSF Identify categories and subcategories and the specific policy statements supporting those outcomes. Appendix A details specific Identify Category and Subcategory definitions and unique identifiers.

1. Asset management.

a. Inventories of physical devices/components of information systems will be maintained IAW GSA CIO-IT Security-01-05, Configuration Management (CM).

b. An accurate inventory of GSA information systems (including hardware, software, and other data required by Federal or GSA requirements) will be maintained in GSA's official system inventory repository.

c. An inventory of information system software platforms and applications IAW GSA CIO-IT Security-01-05.

d. All interconnections between GSA and external entities including off-site contractors or Federal agency/departments must be documented in an Interconnection Security Agreement (ISA) that is approved by the AOs and concurred by the GSA CISO. ISA's must, at a minimum, be reviewed annually. See NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems for detailed information.

e. All communications and data flows, internal and external, for an information system must be documented in a system's SSP.

f. All system interconnections, including connections to external systems, must be documented in a system's SSP.

g. All information systems must comply with NIST SP 800-60, Volume 1, Guide for Mapping Types of Information and Information Systems to Security Categories and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems to determine their security category (i.e., potential impacts for confidentiality, availability and integrity).

h. As part of a system's contingency planning process, resources must be prioritized based on their classification, criticality, and business value. A BIA is required as part of the system's contingency plan.

i. System Owners must ensure adequate personnel are assigned to fulfill those roles and accomplish their responsibilities for systems under their purview.

2. Business environment.

a. GSA's role within the supply chain is: (1) as a consumer of supplies from vendors/providers for its internal systems and use; and (2) as an acquisition agency dedicated to procuring goods and services for the Federal Government, as well as providing acquisition, technical, and project management services to assist agencies in acquiring and deploying information technology and professional services solutions.

b. In both of these roles, requiring activities, working with their COs must ensure supply chain risk management is included in contracts where appropriate, and acquirers must determine whether the acquisition risk is acceptable given their system's environment.

c. Per Presidential Policy Directive (PPD-21), Critical Infrastructure Security and Resilience; GSA, in consultation with the Department of Defense (DOD), Department of Homeland Security (DHS), and other departments and agencies as appropriate, shall provide or support government-wide contracts for critical infrastructure systems and ensure that such contracts include audit rights for the security and resilience of critical infrastructure.

d. GSA COs will coordinate with DHS and other departments and agencies for the acquisition of Government facilities and IT components, ensuring supply chain risks are included in contracts.

e. GSA system contingency plan's BIA should prioritize business missions in relation to the systems supporting the mission objectives and activities.

f. GSA system contingency plan's BIA should identify critical services and any dependencies regarding those services.

g. Integrate and explicitly identify funding for information systems and programs into IT investment and budgeting plans per NIST SP 800-65, Integrating IT Security into the Capital Planning and Investment Control Process and GSA Order CIO 2135.2B. GSA's capital planning and investment control process must be used for the continuous selection, control, and evaluation of IT investments over their life cycles.

h. GSA HSSOs must ensure key personnel have the capacity to perform Mission Essential Functions (MEFs) and Essential Supporting Activities (ESAs) in order to maintain agency resiliency and directly support the public IAW GSA Order OMA 2430.2, The U.S. General Services Administration Continuity of Operations Mission Essential Functions.

i. GSA system contingency plans must address the ability to continue missions under all operating states (e.g., disasters/attacks, recovery, and restoration to normal operations).

3. Governance.

a. This policy, GSA Order CIO 2100.1, outlines GSA's information security policy.

b. HSSOs, System Owners, and others as specified in Chapter 2, must ensure personnel are assigned to fulfill the roles and perform the responsibilities for systems under their purview, including contractor/vendor systems.

c. The primary focus of GSA Order CIO 2100.1 is to provide guidelines that support the implementation of Federal regulations and laws, and the latest versions of the GSA directives referenced in this policy. Chapter 1, Section 3, Federal Laws and Regulations, lists references to legal and regulatory guidance supported by this policy.

d. An entity-wide IT security program must include compliance reviews to determine how well the overall GSA security program meets the agency performance measures.

e. All GSA information systems must complete a Privacy Threshold Analysis (PTA) and a Privacy Impact Assessment (PIA) as part of the A&A process. The PTA/PIA must be reviewed and updated annually or more frequently if there is a significant change to the system's privacy posture. PTAs/PIAs must be prepared IAW GSA Order CPO 1878.1.

f. The OCISO must submit, on behalf of the CIO, an agency-wide FISMA Report to OMB and specified congressional committees annually.

g. The OCISO will generate and store records created or received in the course of performing information security management IAW GSA Order OAS P 1820.1, GSA Record Management Program.

h. AOs must implement a risk management process for all information systems using NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, GSA CIO-IT Security-06-30, and A&A process procedural guides as required.

i. AOs must ensure risk assessments are performed and documented as part of A&A activities IAW GSA CIO-IT Security-06-30 before a system is:

(1) Placed into production;

(2) When significant changes are made to the system;

(3) At least every three (3) years; OR

(4) Via continuous monitoring based on continuous monitoring plans reviewed and accepted by the GSA CISO.

j. The OCISO must conduct compliance reviews to determine if risk is being properly addressed IAW with GSA CIO-IT Security-06-30, GSA CIO-IT Security-18-91, and the GSA CIO-IT Security-18-90.

k. All information systems must be authorized, in writing, before they go into operation. The authorization must be IAW one of the A&A processes in GSA CIO-IT Security-06-30 which requires the system and its risks to be assessed and reported in A&A/ATO packages. The A&A/ATO packages, and therefore system risks, must be updated IAW the system's specific A&A process schedule.

l. Extension of a system's current ATO for a period not to exceed one year (365 days) may only be requested under one of the following conditions. The system must continue to maintain its complete set of A&A documentation (e.g., System Security Plan, Contingency Plan, POA&Ms). All actions to satisfy the conditions below must be completed within the extension period (i.e., no longer than 12 months).

(1) Transitioning to ongoing authorization;

(2) Planning for disposal;

(3) Consolidating into another system for its ATO. The scope of consolidation shall be approved by the OCISO prior to submitting the ATO extension request;

(4) Transitioning into a cloud environment for its ATO. The scope of the transition into the cloud environment shall be approved by the OCISO prior to submitting the ATO extension request;

(5) Re-competing the system's contract;

(6) Completing the upgrade/replacement of major infrastructure components; or

(7) Completing the system's security assessment has been delayed due to contract issues.

m. An information system undergoing a three-year re-authorization having outstanding high or very high/critical vulnerabilities identified during its security assessment, may request a one-time extension for a period not to exceed thirty (30) days from the date of the ATO expiration to allow mitigation of the high and very high/critical vulnerabilities;

4. Risk assessment.

a. Every IT system both government and contractor operated must undergo a security control assessment utilizing GSA test cases based on NIST SP 800-53A, Revision 4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, and the annual requirements provided by the OCISO.

b. All Internet accessible information systems, and all FIPS 199 High impact information systems are required to complete an independent penetration test (or 'pentest') and provide a Penetration Test Report documenting the results of the exercise as part of the A&A package. In addition, these same systems must complete penetration tests annually. The annual penetration tests can be completed internally and do not require an independent assessor.

c. Independent vulnerability testing including penetration testing and system or port scanning conducted by a third-party such as the GAO and other external organizations must be specifically authorized by the AO and supervised by the ISSM.

d. The OCISO must identify sources of cyber threat information and a process for sharing the information, as appropriate.

e. The OCISO must create procedures to share common threats, vulnerabilities, and incident related information with the appropriate organizations.

f. Business impacts must be identified as part of the risk assessment process IAW GSA CIO-IT Security-06-30 and GSA CIO-IT Security-18-91.

g. Threats, vulnerabilities, likelihoods, and impacts must be appropriately identified and considered to assess cybersecurity, supply chain and/or privacy risks IAW GSA CIO-IT Security-06-30 and GSA CIO-IT Security-18-91.

h. All information systems must develop and maintain a POA&M IAW GSA CIO-IT Security-09-44. POA&Ms are the authoritative agency management tool for managing system risk and are used in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in agency programs and systems.

5. Risk Management Strategy.

a. The OCISO implements and maintains a risk management process for all information systems using NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments, GSA CIO-IT Security-06-30, GSA CIO-IT Security-18-90, GSA CIO-IT Security-18-91, and all identified A&A process procedural guides as required.

b. AOs and System Owners must follow the organizational risk tolerance as expressed in GSA CIO-IT Security-18-91.

c. OCISO must update the organizational risk tolerance as expressed in GSA CIO-IT Security-18-91, on a biennial basis based on changes in GSA's risk posture and Federal guidance on any GSA critical infrastructure or sector risks.

6. Supply Chain Risk Management.

a. All FIPS 199 High Impact systems must manage risks to their supply chain IAW NIST SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations.

b. All FIPS 199 High Impact systems must, as part of supply chain risk management, assess the supply chain risk from suppliers and third-party partners.

c. Suppliers and third-party partners must abide by all GSA IT Security Procedural Guides which incorporate supply chain guidance as provided in NIST guidance IAW GSA CIO-IT Security-09-48.

d. Appropriate personnel (e.g., Requiring Official, CO, COTR) must assess a supplier's and third-party partner's supply chain prior to acquisition as part of contract requirements and as necessary thereafter. Assessments may consist of audits, tests, or other forms of evaluation as deemed necessary.

e. All FIPS 199 High impact systems must incorporate Supply Chain Risk Management into response/recovery planning and testing IAW GSA CIO-IT Security-06-29.

CHAPTER 4: POLICY FOR PROTECT FUNCTION

This chapter provides security policy statements for the Protect function of the CSF. The Protect function allows GSA to develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. The activities in the Protect function support the ability to limit or contain the impact of a potential cybersecurity event.

The following paragraphs provide the CSF Protect categories and subcategories and the specific policy statements supporting those outcomes. Appendix A details specific Protect category and subcategory definitions and unique identifiers.

1. Identity management, authentication and access control. GSA guides listed below provide specific implementation guidance and configuration settings/policies for GSA systems and organizations:

- GSA CIO-IT Security-01-01: Identification and Authentication (IA)
- GSA CIO-IT Security-01-07: Access Control (AC)
- GSA CIO-IT Security-03-23: Termination and Transfer
- GSA CIO-IT Security-07-35: Web Application Security
- GSA CIO-IT Security-10-50: Maintenance
- GSA CIO-IT Security-12-67: Securing Mobile Devices and Applications
- Hardening Guides: Multiple guides for configuring various technologies IAW with GSA required security settings

a. All identities and credentials must be managed and administered IAW the procedural guides listed above.

b. All users issued GFE are required to log into the workstation using a GSA issued PIV credential. The following groups of users are exempt from this requirement:

(1) A Federal employee on detail to GSA issued a PIV from the employee's assigned Agency.

(2) Any employee or contractor expected to be employed for less than 180 days and not issued a PIV.

(3) Any person with a disability that does not allow the individual to utilize a PIV card and laptop.

(4) Any user with a PIV that is lost, forgotten at home, or damaged in any way, may contact the IT Service Desk to request a temporary exception to the above requirement, not to exceed forty-five (45) days.

c. Systems with users who are agency business partners or the general public, and who register or log into the system, must accept credentials issued by identity providers who have been certified by federally approved Trust Framework Providers.

d. Information system accounts must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Reviews and validations of all user accounts shall be completed annually to ensure the continued need for system access.

e. Disabling and removal of user accounts supporting account management processes, to include:

(1) Supervisors being responsible for coordinating and arranging system access termination for all departing or resigning personnel, both Federal employees and contractors.

(2) Account removal being initiated by a user's supervisor, COR, or through the review of information provided by the OCISO (e.g., separation lists, role revisions). Data and system owners must verify within 30 days that separated personnel no longer maintain access to GSA IT systems or resources.

(3) Termination and transfer procedures being incorporated into the authorization process for all information systems IAW GSA CIO-IT Security-03-23.

f. Request, including modifications, and approval routing in support of account management processes must ensure:

(1) All access requests require at least one supervisor approval. Access requests submitted directly from a user must not be accepted, regardless of position;

(2) Users complete and send access requests to their supervisor or Contracting Officer Representative (COR), not directly to the data or system owner;

(3) Access requests are routed to the data or system owner by a user's supervisor, COR, ISSO, ISSM, director, or designated official.

g. Authorizations supporting the account management processes must assure:

(1) Supervisors are responsible for coordinating and arranging system access requests for all new or transferring users and for verifying an individual's need-to-know.

(2) Data owners/system owners, with assistance from the designated ISSO, must ensure system access is restricted to authorized users who meet GSA and system access requirements, are familiar with internal security practices, and have completed requisite security and privacy awareness training programs, such as the annual Information Security & Privacy Act training curriculum.

(3) System access authorizations must enforce job function alignment, separation of duties, and be based on the principle of need-to-know. Contractors with system access must utilize a gsa.gov email account to conduct business with GSA.

h. Data or system owners must grant access to the information system based on a valid need-to-know/need-to-share that is determined during the account authorization process and the intended system usage.

i. Orphaned accounts, i.e., a user account that has demonstrated, or is expected to demonstrate, an extensive period of idle time consistent with account abandonment, must be disabled.

j. GSA Affiliated Customer Accounts (GACAs) are a means where any gsa.gov user can share collaboratively in a secure environment with non-GSA users not normally provided a gsa.gov email account. Procedures for setting up a GACA account by an affiliated customer of GSA can be found here: GACA Accounts. GACA accounts are not to be used by GSA employees, contractors or other users (detailees, interns, etc.) requiring regular/repeated access to the GSA network for GSA's Google domain to conduct business. For questions on the proper use of a GACA account or assistance in proper set up, please contact the local IT Manager or Regional ISSO.

k. Annual Privacy Act, Security Training, and application specific training (when required by the application) has been completed for all users.

l. System/network administrators must have separate administrator and user accounts, if applicable (e.g., Microsoft Windows accounts). The administrator privileged account must only be used when administrator rights are required to perform a job function. A normal user account should be used at all other times.

m. Termination and transfer procedures must be followed for all information systems IAW GSA CIO-IT Security-03-23.

n. Physical access to GSA assets must be managed and protected IAW GSA CIO-IT Security-12-64: Physical and Environmental Protection (PE). Facilities management offices may be heavily involved in implementing these controls, especially where controls are associated with multiple systems.

o. Physical and environmental security controls must be commensurate with the level of risk and must be sufficient to safeguard IT resources against possible loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters.

p. GSA servers, routers, and other communication hardware essential for maintaining the operability of GSA systems and their connectivity to the GSA Network, must be placed in an isolated, controlled-access location (i.e., behind locked doors).

q. Limit access to rooms, work areas/spaces, and facilities that contain agency systems, networks, and data to authorized personnel. A list of current personnel with authorized access shall be maintained and reviewed annually to verify the need for continued access and authorization credentials.

r. Visitor access records shall be maintained for facilities containing information systems (except for those areas within the facility officially designated as publicly accessible). Visitor access records include:

(1) Name and organization of the person visiting;
(2) Signature of the visitor;
(3) Form of identification;
(4) Date of access;
(5) Time of entry and departure;
(6) Purpose of visit;
(7) Name and organization of person visited; and
(8) Signature and name of individual verifying the visitor's credentials.

Visitor access records shall be reviewed at least annually.

s. Remote access connections, sessions, and timeout/termination parameters must meet the requirements specified in the procedural guides listed in Section 1 of this Chapter.

t. The following additional requirements apply to connections/sessions.

(1) Remote access connections must be terminated after thirty (30) minutes of inactivity.

(2) Internet accessible application sessions, based on the authentication assurance level (AAL) defined in NIST SPs 800-63-3 and 800-63B, must meet the following requirements.

(a) AAL1. Reauthentication at least once per 30 days during an extended usage session, regardless of user activity. The session will be terminated if this time limit is reached.

(b) AAL2. Reauthentication at least once per 12 hours during an extended usage session, regardless of user activity. Reauthentication after any period of inactivity lasting 30 minutes or longer. The session will be terminated if either of these time limits is reached.

(c) AAL3. Reauthentication at least once per 12 hours during an extended usage session, regardless of user activity. Reauthentication after any period of inactivity lasting 15 minutes or longer. The session will be terminated if either of these time limits is reached.

u. An AO, upon concurrence of the GSA CISO, may grant a deviation to individual requirements specified in the guides only if the system is technically unable to implement the requirement or there is an approved business justification and sufficient

compensating controls have been implemented to reduce the risk to an acceptable level. See Chapter 1, Section 5, Compliance and Deviations.

v. Remote access/endpoint security.

(1) All desktop or laptop computers, including personal devices, connecting remotely to GSA must have anti-virus software running with the latest signature files, a firewall installed and running, and all security patches installed. Failure to have current security signatures or patches may result in loss of access to the GSA network or data.

(2) All computers accessing GSA through a GSA Secure Sockets Layer (SSL) or Internet Protocol Security (IPsec) Virtual Private Network (VPN) must allow an endpoint device that checks for the presence of a client firewall, up-to-date virus protection software and up to date patches. The endpoint device must also verify the absence of malicious software (e.g., Trojans, worms, malware, spyware, etc.) on the client machine. Machines that fail this scan will not be allowed access to the GSA network or any GSA IT resources.

(3) Only GSA GFE that is determined to be properly secured (based on the scans noted above) will be allowed unrestricted remote access to the GSA network.

(4) Personal computers and/or contractor computers will only be allowed access to the Citrix Netscaler and will not have the ability to map local drives (contingent on passing the scans noted above). No PII or other data deemed sensitive by the data owner shall be stored on non-GFE.

(5) In special cases for remote administration and maintenance tasks, contractors will be allowed restricted IPSEC access to specific GSA IP addresses (contingent on passing the scans noted above).

w. Remote access to the GSA domain must be restricted to secure methods using approved identification and authentication methods that provide detection of intrusion attempts and protection against unauthorized access.

(1) Individuals other than GSA employees and contractor personnel are not allowed to use GSA furnished computers, a GSA VPN connection, or a GSA provided or funded internet connection.

(2) Split tunneling is not permitted when connected to the GSA network (no connections to other networks or computers). However, accessing GSA's network via the GSA-provided VPN software over a network is allowed.

(3) When using the GSA IT IPsec VPN, users must connect using only IP and must have the client firewall bound to all network adapters.

(4) Remote access is allowed only with MFA where one of the factors is provided by a device separate from the computer gaining access.

x. The AO or their designee must grant remote access (i.e., external to GSA's network), privileges only to those GSA employees and contractors with a legitimate need for such access as approved.

y. Access permissions and authorizations management must meet the parameter requirements specified in the procedural guides listed in Section 1 of this Chapter.

z. User account privileges must be reviewed across the appropriate Service and Staff Office application portfolio to assess incompatible and non-compliant role assignments (e.g., review of user access assignments across multiple significant systems that share data or pass transactions to identify conflicts with separation of duties policy).

aa. All GSA systems must implement logical access controls to authorize or restrict the activities of users and system personnel to authorized transactions and functions IAW GSA CIO-IT Security-01-07.

bb. The delegation of user roles or permissions for applications, in particular those containing PII and/or other CUI, must be compliant with the principles of least privilege, separation of duties, and need-to-know.

cc. Privileged rights including but not limited to "administrator," "root," and "power user" shall be restricted to authorized employees and contractors as approved by the AO.

dd. Public users must be restricted to using designated public services.

ee. Information systems must enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.

ff. User authorizations must be verified annually for all information systems to determine if they remain appropriate.

gg. Any accesses or permissions that clearly violate established separation of duties policies must be coordinated with the designated S/SO/R ISSO to correct or resolve conflicting role assignments.

hh. Shared user accounts violate the principles of separation of duties and non-repudiation, and must be detected and removed when discovered.

ii. Systems that require users to maintain an active email account must suspend or revoke access for users whose email credentials are no longer valid.

jj. Separation of duties. The following requirements apply to FIPS 199 Moderate and High systems only.

(1) Responsibilities with a security impact must be shared among multiple staff by enforcing the concept of separation of duties, which requires that individuals do not have control of the entirety of a critical process.

(2) Define and implement detailed separation of duties policies for IT systems based on the specific processes, roles, permissions, and responsibilities of personnel involved in departmental business operations.

(3) Every S/SO/R must consider how a separation of duties conflict can arise from shared access to applications and systems. Specifically, application programmers and configuration management personnel should not generally have concurrent access to the development and production environment. Failure to segregate access to source code and production code increase the risk that unauthorized modifications to programs may be implemented into production systems, which could introduce vulnerabilities and negatively impact the integrity and availability of data generated and stored in the system.

(4) Document job descriptions and roles to accurately reflect the assigned duties, responsibilities, and separation of duties principles. By clearly documenting position responsibilities and functions, employees are positioned to better execute their duties IAW policy.

(5) Establish formal procedures to guide personnel in performing their duties, with identification of prohibited actions that would violate separation of duties.

(6) Duties shall be segregated among users so that the following functions shall not generally be performed by a single individual:

(a) Data entry and verification of data. Any data entry or input process that requires a staff member to inspect, review, audit, or test the input to determine that the input meets certain requirements should not permit the same individual to both enter and verify the data. The objective is to eliminate self-certification or verification of data input or entry procedures. Note that this could be an automated or manual process and is not limited to financial transactions.

(b) Data entry and its reconciliation to output. Any data entry or input process that requires reconciliation or matching of transactions to identify discrepancies should not permit the same individual to both enter and reconcile data.

(c) Input of transactions for incompatible processing functions (e.g., input of vendor invoices and purchasing and receiving information).

(d) Data entry and supervisory authorization functions (e.g., authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval).

(7) Ensure proper separation of duties for GSA IT system maintenance, management, and development processes.

(8) Information systems must enforce separation of duties through assigned access authorizations.

(9) Since critical processes can span separate and distinct applications and systems, each S/SO/R will take a macro view of existing roles to define and establish incompatibilities and separation of duties conflicts across an entire business process. This means examining roles that may span multiple IT systems or applications to uncover conflicts that may not be immediately apparent (e.g., an individual has permissions to create and/or modify vendor data in a General Ledger system and the ability to create invoices and purchase orders in an Accounts Payable system).

(10) Every S/SO/R must establish physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities.

(11) Conduct annual assessments to review the effectiveness of control techniques, with an emphasis on activities that cannot be controlled through logical, physical, or compensating controls. The reviews determine whether in-place control techniques are maintaining risks within acceptable levels (e.g., periodic risk assessments).

kk. All GSA workstations and mobile devices shall initiate a session lock after fifteen (15) minutes of inactivity. The session lock shall remain in effect until the user re-establishes access using appropriate identification and authentication.

ll. OAuth 2.0 is an industry standard protocol approved by GSA. It enables a gsa.gov user to grant access to their account or data in Google Apps to a relying party. It is used in a wide variety of services for user authentication. The following policies apply to the use of OAuth 2.0.

(1) GSA IT's OCISO shall monitor and restrict the integration of gsa.gov accounts with OAuth 2.0 to third-party services including but not limited to; websites, Software as a Service (SaaS), mobile applications, and Google Apps Scripts.

(2) OAuth 2.0 Access Scopes are used to limit the authorization granted to the relying service by the gsa.gov user. The Access Scopes listed below present risk to gsa.gov accounts and data and are prohibited unless integrated with websites, mobile apps, and SaaS authorized to operate by GSA and/or included in the GSA IT Standards Profile.

(a) Access inbox and contacts information. Allows view of email messages and settings.

(b) Access personal information. Allows manage of user calendars.

(c) Act on behalf of user. Allows view and modify but not delete user email.

(d) Full data access. Allows view and manage of files and documents in connecting users Google Drive.

(e) Limited access to data and files. Can be varied from access to a single file to allowing the app to view and manage its own configuration data in Google Drive.

(f) Manage devices. Administrator's scope to view and manage mobile devices' metadata.

(g) Manage user activity. Administrator's scope to view users on a domain; manage org units in a domain; view org units in a domain; view and manage provisioning of users in a domain; general domain Application Program Interface (API) operations include managing a domain's language, organization name, max number of users; current number of users.

(h) Other. Miscellaneous permissions. Restrictions are detailed in the system authorization letter.

(i) Payment information. Read Google Wallet credentials from the production environment.

(j) Read-only access to data and files. “Read-only Access” to data and files.

(k) Access location information. Google Map Data API - View Google Maps engine data; Google FIT: Location.

(3) The OAuth 2.0 Access Scopes listed below are authorized for integration with gsa.gov accounts with no restriction.

(a) Basic Info. View an email address; View basic information about an account, including name, public profile URL, photo, gender, birthdate, country, language, and time zone.

(b) Limited access to data and Files. Access Google+ features which are generally public.

(c) Other access scopes similar to those in (a) and (b) above that provide access to publicly available information and do not conflict with prohibited access scopes.

mm. Google Apps Script is a JavaScript cloud scripting language that facilitates the automation of routine tasks across Google Apps and third-party services. All scripts are subject to GSA IT review to verify author; access scope; where the script resides (e.g., internal vs external); type of data accessed; and storage of accessed data.

(1) Internally developed scripts are implicitly allowed but require review by the OCIOS and may be restricted from use pending the results of the OCISO review.

(2) Internally developed scripts shall follow the GSA naming convention. "GSA" immediately followed by an underscore "_" or single dash "-", a 1 to 5 character S/SO official symbol Designation of the script's author, immediately followed by an underscore "_" or single dash "-", and followed by a descriptive script name (e.g., "GSA_IS_Script Name").

(3) Externally developed scripts are prohibited but may be allowed following OCISO review and approval.

nn. Technologies with file-sharing functionality (e.g., peer-to-peer networking software) require review by the OCISO prior to use and may be approved if the file sharing functionality has been limited or disabled.

oo. Contingency Plan/Continuity of Operations Plan contact lists containing only a person's name and home phone number and kept on a password protected electronic device (other Government approved Smart Phone devices, laptop, USB drive) do not require written permission or encryption. Paper "cascade lists" limited to name and home phone number that are maintained for the purpose of emergency employee accountability are permissible with the approval of those individuals listed. All paper and other media must be kept in a locked facility or an otherwise secure location when not in use.

pp. PII stored on network drives and/or in application databases must have proper restricted access controls (i.e., userid/account and password) and shall be made available only to those individuals with a valid need-to-know.

qq. System and/or data owners must verify that data extracts containing PII are handled in accordance with GSA's GSA Rules of Behavior for Handling PII (CIO P 2180.1). PII must only be disclosed on a need-to-know basis within GSA and disposed of in accordance with the applicable records retention schedule.

rr. A GSA Guest Wireless Network has been established in the Regional and Central Office Buildings to allow non-GFE access only to the Internet and GSA resources that are available to the general public (www.gsa.gov). It is intended to be a

service for customers of the agency, as well as vendors performing official business on site.

(1) Guest wireless accounts are not ENT accounts.

(2) Guest wireless traffic will be subject to the same content filtering as traffic on the production network.

ss. All non-GFE/workstations connected to the GSA Wired Network shall only be allowed access to the Internet (i.e., guest network only, no access allowed to the GSA resources).

tt. All GFE/GSA Procured Workstations/Mobile devices such as phones, tablets, etc., should connect to the GSA Wireless Network which requires an ENT account to access, rather than the Guest Wireless Network. Connecting in this manner will provide access to GSA resources as well as the Internet, similar to the GSA Wired Network.

uu. OCISO must approve all requests for access through the GSA Firewall. Firewall change requests must follow the process outlined in GSA CIO-IT Security-06-31: Firewall Change Request. This includes changes to desktop firewall and intrusion prevention systems.

vv. OCISO will block access to all external sites deemed to be a security risk to GSA. Exceptions to this policy must be approved by the CISO.

ww. GSA has implemented a Bring Your Own Device (BYOD) policy in GSA CIO-IT Security-12-67 that allows users with an ENT account to connect a non-GSA procured Wireless device to the GSA Wireless Network to access GSA resources.

xx. All information systems that allow authentication of users for the purpose of conducting government business electronically (accessed via the Internet or via other external non-agency controlled networks, such as partner VPN) complete a Digital Identities Acceptance Statement IAW NIST SP 800-63-3.

yy. Systems with a NIST SP 800-63-3 AAL of 2 or above used by Federal employees or contractors must accept Federal PIV cards and verify them IAW NIST SP 800-63-3 series requirements.

zz. All GSA systems must incorporate a proper user identification and authentication methodology. Refer to the GSA CIO-IT Security-01-01 for additional details.

aaa. User IDs shall be unique to each authorized user.

bbb. Authentication schemes for all systems must utilize MFA using two or more types of identity credentials (e.g., passwords, SAML 2.0 biometrics, tokens, smart

cards, one time passwords) as approved by the AO and IAW the security requirements in the subparagraphs of this paragraph. Systems following the Low Impact SaaS process (GSA CIO-IT Security-16-75) are exempt from this requirement.

(1) Privileged accounts must use MFA when accessing any system via a network.

(2) Non-privileged accounts must use MFA when accessing a FIPS 199 Moderate or High level system via a network.

ccc. An authentication scheme using passwords as a credential must implement the following security requirements:

(1) Password length.

(a) Passwords for accounts used to access operating systems (workstations and servers) must contain a minimum of sixteen (16) characters.

(b) Passwords for systems/other accounts (e.g., service, application) must contain a minimum of eight (8) characters.

(c) Passwords for all mobile devices such as GSA approved smart phones, iPads, and tablets must be a minimum of 6 characters. The six-character password requirement also applies to personal mobile devices accessing GSA data or systems.

(2) Password complexity.

(a) Systems not implementing a password solution rejecting unacceptable passwords, as described below, must require a combination of letters, numbers, and special characters.

(b) Systems implementing a password solution rejecting unacceptable passwords, as described below, do not need to enforce password complexity requirements.

1. The password solution must reject unacceptable passwords (e.g., commonly used, expected, or compromised). For example, the password solution should reject previously breached passwords, dictionary words, repetitive or sequential characters (e.g., ‘aaaaaaaa’, ‘1234abcd’, ‘1qaz2wsx’), context sensitive words, such as the name of the service/website, the username, and derivatives of them.

2. Password solutions must be approved by the CISO and the AO.

(3) Password expiration.

(a) Systems rejecting passwords based on a password solution, as described above, only need to force password changes when a password is compromised or forgotten.

(b) Systems not rejecting passwords based on password solution, as described above, must require passwords to be changed every 90 days and when a password is compromised or forgotten.

(4) Passwords must not be stored in forms (i.e., Windows dialog boxes, web forms, etc.).

(5) All default passwords on network devices, databases, operating systems, etc. must be changed.

(6) Password distribution:

(a) Passwords must never be distributed via regular mail or interoffice mail.

(b) User IDs and passwords must never be distributed together.

(c) User IDs and passwords must be distributed via separate emails or channels (e.g., email, text, telephone).

(d) Passwords used for authentication (other than default or one time use passwords) must not be transmitted in the clear.

(7) Users must be authenticated before resetting or distributing a password.

(8) One time use passwords must expire in:

(a) Two (2) minutes if based on a real-time clock;

(b) Ten (10) minutes if sent by means other than physical mail;

(c) Seven (7) days if sent to a postal address of record;

(d) Twenty-one (21) days if an exception is granted to accommodate an address of record outside the direct reach of the U.S. Postal Service.

(9) Password managers are permitted as long as they are listed on the GSA IT Standards List with a Status of Approved or Exception.

ddd. Authentication methods for applications and systems may use the authentication mechanisms provided by the major information system if deemed appropriate by the AO.

eee. E-commerce and publicly accessible systems must incorporate identification and authentication mechanisms commensurate with their security risks and business needs and may differ from the security requirements set forth by this policy. In such cases the identification and authentication mechanisms must be approved by the AO in writing and concurred by the OCISO.

2. Awareness and training. All GSA and other agency employees, and contractors, as appropriate given their role, must adhere to GSA Order CIO 2100.3C, CIO Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities, and GSA CIO-IT Security-05-29: Security Awareness and Role Based Training Program.

a. All GSA employees and contractors (internal and external) must provide verification that Security Awareness and Privacy Training approved by GSA has been completed within 30 days of notification to complete the training and annually thereafter. An external contractor is defined as someone who has access to GSA information but does not have a GSA email account.

b. Failure to comply with annual awareness and specialized IT security training requirements will result in termination of GSA network account and access to GSA information systems. AOs can terminate system accounts.

c. Obtaining access to GSA resources must constitute acknowledgment that monitoring activities may be conducted.

d. Users have no expectation of privacy on GSA IT systems. All activity on GSA IT systems is subject to monitoring.

e. All GSA IT systems must display an approved warning banner to all users attempting to access GSA's computer systems indicating the system is subject to monitoring.

f. Authorized users must be provided written Rules of Behavior (RoB) IAW GSA Order CIO 2104.1 before being allowed access into any GSA, non-public information system.

g. The user must acknowledge receipt of these rules through a positive action (e.g., acknowledgement of RoB during annual OLU training, signing a form/certificate containing RoB).

h. All internal GSA IT systems must display an approved warning banner to all users attempting to access GSA's computer systems. The warning banner must read as follows:

**********WARNING**********

This is a U.S. General Services Administration Federal Government computer system that is "FOR OFFICIAL USE ONLY." This system is subject to monitoring. Therefore, no expectation of privacy is to be assumed. Individuals found performing unauthorized activities may be subject to disciplinary action including criminal prosecution.

i. For publicly accessible sites (i.e., open to the Internet) the sentence, “Therefore, no expectation of privacy is to be assumed” shall be removed.

j. Users of GSA IT resources must use only software that is properly licensed and registered for GSA use. Users should consult with GSA-IT if there is uncertainty about whether the licensing conforms to Government requirements.

k. All GSA users must abide by software and digital media copyright laws and must not obtain, install, replicate, or use unlicensed software and digital media.

l. Users of GSA IT resources must obtain all software from GSA sources and must not download software from the Internet without prior permission from the appropriate ISSO, as downloading software from the Internet may introduce malicious software such as viruses/worms into the GSA network.

m. Users must not install any software or hardware without approval through the IT Standards process and the Chief Technology Officer (CTO).

n. Users must not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise GSA resources unless authorized by the appropriate ISSO. Examples of such tools include those that defeat software copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files.

o. GSA provides access to email and social media for Government business. However, users may occasionally make personal use of email and social media that involves minimal expense to the Government and does not interfere with Government business. Prior to establishing an official GSA social media presence, users must inform the Office of Strategic Communication’s (OSC) Enterprise Web Management (EWM) group which can monitor and assist with GSA branding and other aspects related to dealing with the public.

p. Users must not use email or social media for any activity or purpose involving classified data.

q. Users must avoid the following prohibited email and social media usages:

(1) Transmitting unsolicited commercial announcements or advertising material, unless approved by management in advance.

(2) Transmitting any material pertaining to GSA, the Federal Government, or any agency employee or official that is libelous or defamatory.

(3) Transmitting sexually explicit or offensive material, non-business related large attachments, chain letters, un-authorized mass mailings, or intentionally sending a virus/worm.

r. Personal use of Government IT systems for Internet access must be kept to a minimum and must not interfere with official system use or access

s. Users must avoid prohibited Internet usages including:

(1) Unauthorized attempts to break into any computer, whether belonging to GSA or another organization.

(2) Browsing sexually explicit, gambling sites, or hate-based web sites (i.e., web sites supporting hate groups or hate speech as their primary purpose).

(3) Using Internet access for personal gain (i.e., making use of GSA resources for commercial purposes or in support of for-profit activities such as running a private business).

(4) Theft of copyrighted or otherwise legally protected material, including copying without permission.

(5) Sending or posting sensitive material such as GSA building plans or financial information outside of the GSA network.

(6) Automatically forwarding email messages from GSA email addresses to any non-Federal email account(s) or address(es).

(7) Sending email messages including sensitive information, such as PII, as deemed by the Data Owner, without GSA provided encryption. Certified encryption modules must be used IAW FIPS 140-2, Security requirements for Cryptographic Modules.

(8) Activities in violation of GSA Ethics Policies, including but not limited to promotional materials, solicitations, partisan political activities in violation of the Hatch Act, financial trading, or any other activity in contravention of Federal Government ethical guidance, policies, or regulations.

t. If PII needs to be emailed outside the GSA network, encryption is required. Instructions can be found on the GSA Privacy Act Program InSite page in the section "Documents for Download." An email will be blocked if Social Security Numbers are sent unencrypted.

u. GSA prohibits an employee or contractor supporting GSA from creating or sending information using a non-official GSA electronic messaging account (i.e., company or personal email account).

v. Additional guidance regarding GSA's policy on email is available in GSA Orders CIO 2160.2B CHGE 1, ADM 7800.11A, CIO 2140.4, and CIO P 2165.2. Guidance on social media is available in GSA Order OSC 2106.2.

w. International travel policy for Portable Electronic Devices (PED). The widespread use of PEDs as stand-alone, networks and remote access devices, present special security concerns not limited to laptops, cell phones, thumb drives, Personal Data Assistants (PDA), tablets, and pagers. Vulnerabilities of these devices while on international travel warrant specific controls to protect the GSA network. GFE must not be taken on international travel without prior approval from the individual's supervisor and OMA.

(1) Individuals with a Top Secret/Sensitive Compartmented Information (TS/SCI), or Secret clearance must contact OMA prior to any international travel.

(2) OMA will provide direction on foreign contact, security precautions, mobile devices, etc.

(3) GSA employees (with the exception of the OIG employees) that hold a National Security clearance, and at the discretion of OMA, shall be issued loaner devices by GSA IT when traveling outside the United States, or any area deemed to have an elevated risk during the period of travel. The loaner devices must be returned to GSA IT immediately upon the employee's return. These loaner devices shall be wiped immediately by GSA IT to ensure no data remains resident on the system(s) issued. Due to technical security controls in place for all mobile devices (encryption and mobile device management (MDM)), personnel in Public Trust positions are not required to follow this provision unless deemed to be required by OMA to provide additional safeguards to data these personnel may access.

3. Data security.

a. All PII and PCI data, and business sensitive data as determined by the AO, and authenticators, including but not limited to passwords, keys, and tokens must be encrypted in storage.

b. Physically control and securely store information system media within controlled areas.

c. All agency data on portable storage devices (e.g., USB flash drives, SD cards, external hard drives), must be encrypted with a FIPS 140-2 certified encryption module.

d. If it is a business requirement to store PII on GSA user workstations or mobile devices including, but not limited to notebook computers, USB drives, CD-ROMs/DVDs, personal digital assistants, PII must be encrypted using a FIPS 140-2 certified encryption module.

e. PII stored on network drives and/or in application databases must have proper access controls (i.e., User ID/password) and shall be made available only to those individuals with a valid need-to-know.

f. Web sites (internal and public) with logon functions, must implement TLS encryption with a FIPS 140-2 validated encryption module. SSL/TLS implementation must be IAW GSA CIO-IT Security-14-69: SSL/TLS Implementation Guide.

g. All sensitive information, such as PII, as deemed by the data owner, which is transmitted outside the GSA firewall, must be encrypted. Certified encryption modules must be used IAW FIPS 140-2, Security requirements for Cryptographic Modules.

h. An employee or contractor shall not physically take PII from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or access remotely (i.e., from locations other than GSA facilities), without written permission from the employee's supervisor, the data owner, and the IT system AO. Approvals shall be filed with the employee's supervisor. This applies to electronic media (e.g., laptops, USB drives), paper, and any other media (e.g., CDs/DVDs) that may contain PII.

i. PII and/or sensitive data may only be accessed remotely from GFE or through an approved GSA virtual interface (i.e., Citrix and/or VDI).

j. If PII needs to be emailed outside the GSA network encryption is required. Instructions can be found on the privacy web page in the section "Documents for Download." An email will be blocked from transmittal if Social Security Numbers are attempted to be sent unencrypted.

k. If PII needs to be sent by courier, printed, or faxed several steps should be taken. When sending PII by courier mark, "signature required" when sending documents. This creates a paper trail in the event items are misplaced or lost. Do not let PII documents sit on a printer where unauthorized employees or contractors can have access to the information. When faxing information, use a secure fax line. If one is not available, contact the office prior to faxing, so they know information is coming, and contact them after transmission to ensure they received it. For each event, the best course of action is to limit access to PII only to those individuals authorized to handle it, create a paper trail, and verify information reached its destination.

l. GSA information system assets must adhere to the guidance provided in GSA CIO-IT Security-01-05, GSA CIO-IT Security-06-32 and GSA CIO-IT Security-12-64 as assets are removed, transferred, or disposed.

m. The availability and usability of GSA equipment and software must be maintained and safeguarded to enable agency objectives to be accomplished.

n. Systems that contain permanent electronic records must be maintained in an electronic format by 12/31/2019.

o. All permanent and temporary email records must be accessible electronically in an electronic format.

p. Data (including relevant and pertinent documentation), must be protected against unauthorized access, tampering, alteration, loss, and destruction during production, input, output, handling, and storage. This protection must include clarification for labeling sensitive security documentation IAW GSA policies. Additional guidance may be found in GSA CIO-IT Security-12-63: System and Information Integrity.

q. When using password generated encryption keys, a password of at least 8 characters with a combination of letters, numbers, and special characters is required.

r. Systems implementing encryption must follow the key management procedures and processes documented in GSA CIO-IT Security-09-43: Key Management.

s. Data integrity and validation controls must be used on all information systems that require a high degree of integrity.

t. Ensure that data integrity is protected IAW GSA CIO-IT Security-12-63.

u. Controls shall be put in place to monitor or detect changes or updates to systems that are outside the parameters of a system's baseline operating characteristics. This includes the ability to monitor resource usage and allocation.

v. The requirements for testing and development environments identified in GSA CIO-IT Security-01-05 must be met.

w. Hardware assets must be inspected upon receipt to ensure their authenticity.

x. After receipt, hardware assets must be protected against unauthorized access, tampering, alteration, loss, and destruction during production, input, output, handling, and storage.

4. Information protection processes and procedures.

a. All information systems must be securely configured IAW with GSA IT technical guides and standards, updated, and patched before being put into operation and while in operation.

b. GSA information systems, including vendor owned/operated systems on behalf of GSA, must configure their systems in agreement with GSA technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate. Where a GSA benchmark exists, it must be used. GSA benchmarks may be exceeded but not lowered.

c. All new technology developments, designs, and implementations shall use industry best practices, Government guidelines, and Government audit findings as they become available.

d. GSA IT Security Policy must be incorporated into each phase of the system development lifecycle, (e.g., initiation, planning, development/acquisition, implementation, operation, and disposal), for all GSA information systems.

e. System owners must use NIST SP 800-64, Revision 2, Security Considerations in the System Development Life Cycle and GSA Order CIO 2140.4 as guides when managing security throughout the system's lifecycle.

f. ISE must approve all Security Architecture designs prior to implementation.

g. Configuration changes must be controlled IAW the security controls and processes described in GSA CIO-IT Security-01-05.

h. Information system backups and testing of those backups must be accomplished IAW GSA CIO-IT Security-06-29.

i. Ensure that all agency systems and networks are located in areas not in danger of water damage due to leakage from building plumbing lines, shut-off valves, and other similar equipment to support meeting federal and local building codes.

j. Install and ensure operability of fire suppression devices, such as fire extinguishers and sprinkler systems, and detection devices, such as smoke and water detectors, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

k. Install and ensure operability of air control devices, such as air-conditioners and humidity controls, in all areas where agency information systems are maintained (this includes server rooms, tape libraries, and data centers) to meet federal and local building codes.

l. The guidance provided in GSA CIO-IT Security-12-64 for a secure physical environment for information systems must be applied. Facilities management offices may be heavily involved in implementing these controls, especially where controls are associated with multiple systems.

m. All GSA data from information system media, both digital and non-digital, must be sanitized IAW methods described in GSA CIO-IT Security-06-32 before disposal or transfer outside of GSA.

n. The OCISO shall update this security policy and IT Security Procedural guides biennially, or more frequently as Federal or GSA guidance or the threats, vulnerabilities, or risks to GSA dictate.

o. HSSOs, for their FISMA reportable systems, shall track the performance measures/goals presented by the OCISO. AOs, system owners, ISSMs, and ISSOs shall support these measures. The CISO shall at least annually assess and report on the performance and goals.

p. All systems must adhere to the A&A processes in GSA CIO-IT Security 06-30, security requirements in this policy, and GSA IT Security Procedural guides. At a minimum, annual reviews and updates, when necessary, are required to reflect changes in Federal or GSA processes and guidance.

q. The OCISO will implement dashboards and reports, as appropriate, to provide stakeholders and management personnel with information on the security status of information systems and assets.

r. Contingency plans must be developed and revised annually, as necessary, for all IT systems IAW GSA CIO-IT Security-06-29. The plans must include recovery procedures, a separate disaster recovery plan may be developed if necessary.

s. Incident response plans must be developed and revised annually, as necessary, for all IT systems IAW GSA CIO-IT Security-01-02. The plans must include incident recovery processes, a separate incident recovery plan may be developed if necessary.

t. Contingency plans must be annually tested IAW GSA CIO-IT Security-06-29.

u. Incident response plans must be annually tested IAW GSA CIO-IT Security-01-02.

v. Background investigation requirements for access to GSA information systems (including contractor operations containing GSA information) shall comply with GSA Order CIO P 2181.1, Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing. Contractors requiring non-routine access to IT systems (contractor summoned for an emergency service call) are not required to have a personnel investigation and are treated as visitors and must be escorted while in a GSA facility.

w. Employees and contractors shall have a favorable initial fitness/suitability determination and be in the process of receiving a Minimum Background Investigation (or comparable investigation) or higher to access PII. The authority and access shall be

determined by the appropriate GSA Supervisor (for GSA employees) or CO (for contract personnel), Data Owner, and the System's AO. Each System's AO, with the request of the GSA Supervisor, Data Owner or CO, shall evaluate the risks associated with each such request.

x. There shall be no waivers to background investigations for IT access for GSA employees or contractors. A favorable initial fitness/suitability determination shall be granted before access to the GSA network or any GSA IT system.

y. Vulnerabilities and weaknesses (system and program level) requiring mitigation must be managed using the processes described in GSA CIO-IT Security-09-44.

z. The OCISO will review POA&Ms quarterly and provide system level and management reports IAW GSA CIO-IT Security-09-44.

5. Maintenance.

a. Maintenance and repair of organizational assets must be performed and recorded with approved tools IAW GSA CIO-IT Security-10-50.

b. Maintenance of agency hardware and software must be restricted to authorized personnel.

c. System administration and patch implementation must be restricted to authorized personnel.

d. Remote or non-local maintenance of organizational assets must be authorized, recorded, and authenticated via MFA IAW GSA CIO-IT Security-10-50.

6. Protective technology.

a. The requirements for security auditing/logging capabilities and their review must be implemented on GSA systems IAW GSA CIO-IT Security-01-08: Audit and Accountability.

b. Auditing of actions regarding PII stored on network drives and/or application databases must be captured (e.g., type of action, date/time, user, source of action, outcome of action).

c. Computer-readable data extracts from databases holding PII must be logged, including creator, date, type of information, and user.

d. Restrict access to information system media (e.g., disk drives, diskettes, internal and external hard drives, and portable devices), including backup media, removable media, and media containing sensitive information to authorized individuals.

e. Protect digital media during transport outside of controlled areas using a certified FIPS 140-2 encryption module; non-digital media shall follow GSA personnel security procedures.

f. Users must secure portable storage devices and removable media using the same policies and procedures as paper documents as prescribed by OHRM policies.

g. Users must protect portable storage devices and removable media in the same manner as a valuable personal item and should not leave them unattended in public places, automobiles, etc.

h. Information systems must operate in such a way that they run with the least amount of system privilege needed to perform a specific function and that system access is granted on a need-to-know basis.

i. Information systems must be configured to the most restrictive mode (e.g., limiting ports, protocols, services, etc.) consistent with operational requirements.

j. Google Chrome Extensions (often developed by third parties) extend Google Chrome and Google Apps functionality. Extensions shall be disabled by default and enabled for business purposes following review and approval by OCISO Security Engineering Division.

k. The installation or use of unauthorized instant messaging (IM) software is prohibited (i.e., must use an approved GSA standard).

l. Bluetooth is approved for use with keyboards, mice and headsets on GSA GFE. The following restrictions apply:

(1) Devices must use the Bluetooth Protocol version 1.2 or later. If the device was manufactured 2005 or later, the version must be confirmed by consulting the device specifications.

(2) If a password/PIN must be chosen for device pairing the user should use a combination of letters and numbers when possible. A four digit pin should not be used unless this has been hard coded by the manufacturer. Users should also use a different passcode/PIN for each separate device pairing.

(3) The computer/device should not be discoverable except as needed for pairing. Discoverable mode (also known as "visible mode" or "pairing mode") is the mode that allows the pairing of two Bluetooth devices. Users must ensure discoverable mode is disabled after pairing is completed.

(a) Bluetooth capabilities must be disabled when they are not in use.

(b) Two devices should not remain connected for more than 23 hours at a time, since the encryption keys can repeat after this.

(c) Encryption should always be enabled for Bluetooth connections (i.e., "Security Mode 1" does not enable encryption, and therefore should never be used).

m. Hacking tools are not to be used on GSA workstations without permission from OCISO, including password crackers, software that bypasses network controls (e.g. Tor), or hacking toolkits (e.g. Kali, Metasploit).

n. All network devices that are either owned, managed, maintain a connection to a GSA facility, and/or handle GSA data shall be strategically positioned behind a GSA firewall to provide analysis/correlation, management structure, and minimize threats presented by external attacks.

o. If GSA systems interconnect, they must connect using a secure methodology that provides security commensurate with the acceptable level of risk as defined in the system security plan and that limits access only to the information needed by the other system IAW GSA CIO-IT Security-01-07 and GSA CIO-IT Security-06-30.

p. GSA users must secure mobile devices, like all enterprise devices, against a variety of threats. This includes handling PII. Included in the definition of 'Mobile devices' are smartphones and tablets. Excluded in the definition of mobile devices are laptops since the security controls for laptops are quite different from smartphones. Also excluded in the definition are basic cell phones due to the limited security options available and their limited threat. GSA has outlined information on mobile devices at: https://sites.google.com/a/gsa.gov/mobileinfo/. GSA CIO-IT Security-12-67 is designated as the GSA policy on mobile devices and applications and provides specific information security requirements.

q. GSA's MDM solution ensures Government issued phones have appropriate security including; encryption, application controls, passwords usage, remote locking, remote wiping, and operating system protection.

r. Users must not connect to GSA resources without complying with the requirements which the Guide describes.

s. GSA CIO-IT Security-12-67 details the steps necessary to use a personally owned mobile device, which include:

(1) GSA will install MDM on the device and enforce control security settings, including password usage, encryption, and inactivity timeout.

(2) GSA will ensure that GSA can wipe the device clean if it is lost or stolen or after repeated unsuccessful attempts at logon.

(3) GSA will not support personally owned mobile devices.

(4) Users must agree to and sign a GSA Personal Device Usage Agreement and the GSA Rules of Behavior for Personally Owned Mobile Devices.

t. Systems shall be implemented per the enterprise architecture principles in GSA Order CIO 2110.4. The principles contained in GSA Order CIO 2110.4 are consistent with OMB Circular A-130 which establishes the framework for architecture to address security controls for components, applications, and systems.

(1) In addition to the principles set forth in GSA Order CIO 2110.4, architecture practices cited in OMB's Federal Segment Architecture Methodology must be used during planning a new system or significant capability enhancement.

(2) GSA OCISO has determined that the implementation of enterprise architecture principles is provided as a common control by the Office of Enterprise Planning and Governance (IDR). For additional details, please refer to GSA CIO-IT Security-18-90.

CHAPTER 5: POLICY FOR DETECT FUNCTION

This chapter provides security policy statements for the Detect function of the CSF. The Detect Function allows GSA to develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable timely discovery of cybersecurity events.

The following paragraphs provide the CSF Detect categories and subcategories and the specific policy statements supporting those outcomes. Appendix A details specific Detect category and subcategory definitions and unique identifiers.

1. Anomalies and events.

a. GSA uses centralized MDM to manage the configuration and security of mobile devices. GSA provisions and activates MDM on each mobile device before issuing Government devices to users.

b. The OCISO ELP will be used to establish a baseline of activity for GSA systems/sensors on the network.

c. The OCISO will regularly review/analyze data provided with the ELP for indications of inappropriate or unusual activity. Suspicious activity or suspected violations must be investigated. Any findings must be reported to appropriate officials IAW GSA CIO-IT Security-01-02.

d. Information systems must produce audit/log records that contain sufficient information to establish what events occurred, the sources of the events, and the outcomes of the events.

e. The OCISO ELP will be used for the collection and correlation from GSA systems/sensors.

f. The GSA Incident Response Team will determine the impact of events (potential incidents and actual incidents) based on Federal and GSA guidance as described in GSA CIO-IT Security-01-02.

g. Personnel making the determination of whether a major incident has occurred (requiring Congressional reporting) will be conducted by the GSA Full Response Team as defined in GSA Order CIO 9297.2C and requires at least the following members:

(1) GSA CIO;

(2) GSA CISO, leads the team for major non-privacy incidents;

(3) Mission or system owners;

(4) SAOP leads the team for major privacy incidents; and

(5) Security Engineering Division Director or representative.

h. The GSA Incident Response Team will adhere to the thresholds established by Federal and GSA guidance as identified in GSA CIO-IT Security-01-02.

2. Security continuous monitoring.

a. OCISO will implement continuous monitoring of systems using Continuous Diagnostics and Mediation (CDM) and other enterprise security tools as described in GSA CIO-IT Security-12-66: Information Security Continuous Monitoring.

b. Intrusion detection/protection systems must be implemented.

c. GSA organizations must define procedures to periodically monitor mobile device security to verify compliance with GSA requirements.

d. Monitoring procedures must include specific steps to be taken and protocol to be applied when reviewing audit/log data.

e. The OCISO must be informed in the event of an audit processing failure and system personnel must take one of the following additional actions: shut down information system, overwrite oldest audit records, or stop generating audit records.

f. Access to physical spaces containing GSA IT assets must be monitored for unauthorized access and suspicious incidents IAW GSA CIO-IT Security-12-64.

g. Limit access to rooms, work areas/spaces, and facilities that contain agency systems, networks, and data to authorized personnel. A list of current personnel with authorized access shall be maintained and reviewed annually to verify the need for continued access and authorization credentials.

h. Visitor access records shall be maintained for facilities containing information systems (except for those areas within the facility officially designated as publicly accessible). Visitor access records include:

(1) Name and organization of the person visiting;
(2) Signature of the visitor;
(3) Form of identification;
(4) Date of access;
(5) Time of entry and departure;
(6) Purpose of visit;
(7) Name and organization of person visited, and
(8) Signature and name of individual verifying the visitor’s credentials.

Visitor access records shall be reviewed at least annually.

i. Personnel activity will be monitored IAW GSA CIO-IT Security-01-08.

j. User activity will be monitored for indications of fraud, misconduct, or other irregularities.

k. All information systems must have up-to-date, agency-authorized virus protection software. Note that the use of Kaspersky Lab virus protection software, to include software that is embedded or integrated into third-party technology, is expressly prohibited.

l. All information systems must implement and enforce a malicious code protection program designed to minimize the risk of introducing malicious code (e.g., viruses, worms, spyware, Trojan horses) into agency systems and networks.

m. GSA monitors mobile device activity for unauthorized code, including mobile code, using MDM policies and rules of behavior as outlined at: https://sites.google.com/a/gsa.gov/mobileinfo/.

n. AOs and OCISO will ensure external service providers are connected via the TIC, permitting monitoring and detection of events.

o. External service provider personnel who connect remotely to the GSA network must do so as described in Chapter 4 Section 1, v., regarding remote access and endpoint security, and must permit monitoring and detection of events.

p. For contractors and outsourced operations, implement appropriate safeguards to monitor GSA information and information systems for unauthorized access throughout all phases of a contract. Review contracts to ensure information security is appropriately addressed in the contracting language. GSA CIO-IT Security-09-48 establishes the language for GSA IT acquisitions contracts. All applicable NIST SP 800-53, Revision 4 controls should be put on contract (and a reasonable subset continuously monitored using guidance provided by the OCISO) for all contractor and outsourced operations. Given that the GSA IT security program is risk-based, the system owner/program manager and ISSO can make risk-based decisions on tailoring the system's baseline security controls and then obtain concurrence from the AO and the CISO. Any controls tailored out of the baseline must have the rationale for the decision documented in the system's SSP.

q. Monitoring will be performed as described IAW GSA CIO-IT Security-01-08.

r. GSA S/SO/Rs shall scan for unauthorized wireless access points quarterly and take appropriate action if such an access point is discovered.

s. Systems will be scanned for vulnerabilities of operating systems and web applications periodically IAW GSA CIO-IT Security-17-80. Vulnerabilities identified must be remediated IAW GSA CIO-IT Security-06-30.

3. Detection processes.

a. The OCISO must define the roles and responsibilities for detection personnel to ensure they understand and perform their assigned actions.

b. Systems must comply with Federal and GSA detection and monitoring requirements as specified in NIST SP 800-53, Revision 4 and IAW GSA CIO-IT Security-01-08.

c. OCISO detection personnel must ensure detected event information is communicated to appropriate personnel.

d. Detection process testing should be included during annual incident response testing.

e. The OCISO must review and update detection processes annually or when significant changes occur or problems are encountered with detection activities.

CHAPTER 6: POLICY FOR RESPOND FUNCTION

The Respond Function allows GSA to develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The activities in the Respond Function support the ability to contain the impact of a potential cybersecurity incident.

The following paragraphs provide the CSF Respond categories and subcategories and the specific policy statements supporting those outcomes. Appendix A details specific Respond category and subcategory definitions and unique identifiers.

1. Response planning.

a. All information systems must have their contingency plans and Incident Response Plans tested annually.

b. Lessons learned during contingency plan and incident response plan tests must be incorporated into revised plans.

2. Communications.

a. GSA employees and contractors on the Incident Response Team identified in GSA CIO-IT Security-01-02 are trained on their roles and responsibilities within 60 days of assignment and annually thereafter.

b. Personnel with contingency planning responsibilities must be trained in their contingency roles and responsibilities with respect to the information system annually.

c. Users must immediately report suspected vulnerabilities, security violations, and security incidents to the GSA IT Service Desk.

d. Users must immediately report lost or stolen portable storage devices to the GSA IT Service Desk.

e. All incidents involving the loss or theft of GSA hardware, software, and/or information in physical form must be reported immediately to the GSA IT Service Desk.

(1) Users must also report all losses to the Federal Protective Service (FPS) via the appropriate Regional Hotline, as directed by the appropriate ISSO or the GSA IT Service Desk.

(2) Users must also report any loss that occurs outside of Federal facilities to the local police.

(3) Lost PIV cards must be reported to the Central or Regional OMA office after reporting to the GSA IT Service Desk.

f. GSA Incident Response Teams must report incidents as described in GSA CIO-IT Security-01-02. FISMA requires “major incidents” to be reported to the U.S. Congress within seven days of detection.

g. Data breaches (i.e., loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users with an authorized purpose have access or potential access to PII, whether physical or electronic) shall also follow reporting and response procedures as defined in GSA Order CIO 9297.2C.

h. ISSOs must report any security incidents reported to them to the GSA IT Service Desk and GSA OCISO.

i. Information will be shared by the GSA Incident Response Team, as appropriate, and IAW GSA CIO-IT Security-01-02.

j. Coordination with stakeholders will be conducted by the GSA Incident Response Team, as appropriate, and IAW GSA CIO-IT Security-01-02.

k. Information sharing with external stakeholders will be conducted by the GSA Incident Response Team, as appropriate and in coordination with the GSA CISO, IAW GSA CIO-IT Security-01-02.

3. Analysis.

a. The OCISO will communicate notifications/alerts from detection systems for investigation by GSA’s Incident Response Team via email or the GSA IT Service Desk. Procedures must be documented for responses to detected irregularities.

b. The GSA Incident Response Team will investigate notifications/alerts from detection systems IAW GSA CIO-IT Security-01-02.

c. The GSA Incident Response Team will determine the impact of an incident in coordination with other personnel/organization, as appropriate, during the investigation process defined in GSA CIO-IT Security-01-02.

d. The GSA Incident Response Team will perform forensics analysis of incidents/the evidence of incidents, as necessary, to support investigations as described in GSA CIO-IT Security-01-02.

e. The GSA OCISO and Incident Response Team will categorize incidents IAW GSA CIO-IT Security-01-02.

f. The OCISO will establish a vulnerability management process for identifying vulnerabilities via internal testing/scanning.

g. The OCISO will notify personnel with security responsibilities of vulnerabilities disclosed via security advisory alerts or other external sources.

h. ISSMs and ISSOs must report on the status of security advisory alerts to the Office of the CISO upon request.

4. Mitigation.

a. The GSA Incident Response Team, in coordination with system personnel, will contain incidents IAW GSA CIO-IT Security-01-02.

b. Incidents will be mitigated or remediated based on activities executed by the GSA Incident Response Team and system personnel, as described in GSA CIO-IT Security-01-02 and the system's recovery plan.

c. IAW GSA CIO-IT Security-06-30, newly identified vulnerabilities must be:

(1) Remediated or mitigated IAW specified timeframes;

(2) Included in a Plan of Action & Milestones; or

(3) Included in an Acceptance of Risk Letter.

5. Improvements.

a. Incident response plans must be updated based on lessons learned during incident response or plan testing.

b. Contingency plans must be updated based on lessons learned during responses to disasters, other events invoking the contingency plan or plan testing.

c. Incident response strategies must be reviewed and updated, if necessary, at least annually to address system/organizational changes and problems or issues encountered while responding to incidents or plan testing.

CHAPTER 7: POLICY FOR RECOVER FUNCTION

This chapter provides security policy statements for the Recover Function of the CSF. The Recover Function allows GSA to develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The activities in the Recover Function support timely recovery to normal operations to reduce the impact from a cybersecurity incident.

The following paragraphs provide the CSF Recover categories and subcategories and the specific policy statements supporting those outcomes. Appendix A details specific Recover category and subcategory definitions and unique identifiers.

1. Recovery planning.

a. As part of a system's contingency planning process, recovery plans are exercised as part of a cybersecurity incident response or after the response, as appropriate.

2. Improvements.

a. As part of a system's contingency planning processes, lessons learned from contingency plan tests regarding recovery must be incorporated into a revised contingency plan.

b. As part of system's contingency plan testing and incident responses or incident response plan testing, any lessons learned regarding recovery strategies will be updated in the appropriate plan.

3. Communications.

a. The GSA OCISO will coordinate with the OSC to determine the necessity, appropriate process, and means for managing public information regarding an incident.

b. The GSA OCISO will coordinate with the OSC to determine the necessity, appropriate process, and means for repairing GSA's reputation after an incident.

c. Recovery activities are communicated by the GSA Incident Response Team and system personnel, as appropriate and in coordination with the GSA CISO, IAW GSA CIO-IT Security-01-02 and the system's recovery plan.

APPENDIX A: CSF CATEGORIES/SUBCATEGORIES

The table below provides a listing of CSF categories and subcategories (including unique identifiers) and descriptions from the NIST CSF. Additional information is available in CSF Version 1.1.

Category/Subcategory
Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.
ID.AM-1: Physical devices and systems within the organization are inventoried
ID.AM-2: Software platforms and applications within the organization are inventoried
ID.AM-3: Organizational communication and data flows are mapped
ID.AM-4: External information systems are catalogued
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
ID.BE-1: The organization's role in the supply chain is identified and communicated
ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated
ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated
ID.BE-4: Dependencies and critical functions for delivery of critical services are established
ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.
ID.GV-1: Organizational cybersecurity policy is established and communicated
ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
ID.GV-4: Governance and risk management processes address cybersecurity risks
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
ID.RA-1: Asset vulnerabilities are identified and documented
ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources
ID.RA-3: Threats, both internal and external, are identified and documented
ID.RA-4: Potential business impacts and likelihoods are identified
ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
ID.RA-6: Risk responses are identified and prioritized

Category/Subcategory
Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
ID.RM-1: Risk management processes are established, managed, and agreed to by organizational stakeholders
ID.RM-2: Organizational risk tolerance is determined and clearly expressed
ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.
ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholder
ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process
ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan
ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations
ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers
Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
PR.AC-2: Physical access to assets is managed and protected
PR.AC-3: Remote access is managed
PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties
PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)
PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multifactor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.
PR.AT-1: All users are informed and trained
PR.AT-2: Privileged users understand their roles and responsibilities
PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities
PR.AT-4: Senior executives understand their roles and responsibilities
PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities

Category/Subcategory
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
PR.DS-1: Data-at-rest is protected
PR.DS-2: Data-in-transit is protected
PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
PR.DS-4: Adequate capacity to ensure availability is maintained
PR.DS-5: Protections against data leaks are implemented
PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
PR.DS-7: The development and testing environment(s) are separate from the production environment
PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)
PR.IP-2: A System Development Life Cycle to manage systems is implemented
PR.IP-3: Configuration change control processes are in place
PR.IP-4: Backups of information are conducted, maintained, and tested
PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met
PR.IP-6: Data is destroyed according to policy
PR.IP-7: Protection processes are improved
PR.IP-8: Effectiveness of protection technologies is shared
PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
PR.IP-10: Response and recovery plans are tested
PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
PR.IP-12: A vulnerability management plan is developed and implemented
Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.
PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools
PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
PR.PT-2: Removable media is protected and its use restricted according to policy
PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
PR.PT-4: Communications and control networks are protected

Category/Subcategory
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.
DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
DE.AE-2: Detected events are analyzed to understand attack targets and methods
DE.AE-3: Event data are collected and correlated from multiple sources and sensors
DE.AE-4: Impact of events is determined
DE.AE-5: Incident alert thresholds are established
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
DE.CM-1: The network is monitored to detect potential cybersecurity events
DE.CM-2: The physical environment is monitored to detect potential cybersecurity events
DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events
DE.CM-4: Malicious code is detected
DE.CM-5: Unauthorized mobile code is detected
DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed
DE.CM-8: Vulnerability scans are performed
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
DE.DP-2: Detection activities comply with all applicable requirements
DE.DP-3: Detection processes are tested
DE.DP-4: Event detection information is communicated
DE.DP-5: Detection processes are continuously improved
Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.
RS.RP-1: Response plan is executed during or after an incident
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
RS.CO-1: Personnel know their roles and order of operations when a response is needed
RS.CO-2: Incidents are reported consistent with established criteria
RS.CO-3: Information is shared consistent with response plans
RS.CO-4: Coordination with stakeholders occurs consistent with response plans
RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.
RS.AN-1: Notifications from detection systems are investigated
RS.AN-2: The impact of the incident is understood
RS.AN-3: Forensics are performed
RS.AN-4: Incidents are categorized consistent with response plans

Category/Subcategory
RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.
RS.MI-1: Incidents are contained
RS.MI-2: Incidents are mitigated
RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks
Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.
RS.IM-1: Response plans incorporate lessons learned
RS.IM-2: Response strategies are updated
Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.
RC.RP-1: Recovery plan is executed during or after a cybersecurity incident
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
RC.IM-1: Recovery plans incorporate lessons learned
RC.IM-2: Recovery strategies are updated
Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g., coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).
RC.CO-1: Public relations are managed
RC.CO-2: Reputation is repaired after an incident
RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams