GENERAL SERVICES ADMINISTRATION
Washington, DC 20405

CIO 2100.1Q
October 16, 2024

GSA ORDER

SUBJECT: GSA Information Technology (IT) Security Policy

1. Purpose. This Chief Information Officer (CIO) Order establishes the General Services Administration (GSA) IT Security Policy.

2. Cancellation. This Order cancels and supersedes CIO 2100.1P, GSA Information Technology (IT) Security Policy, dated January 31, 2024.

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

a. Added references to Office of Management and Budget (OMB) Memorandum M-24-10 and GSA Order CIO 2185.1A in Chapter 1, Section 3;
b. Revised IT Security Controls section to clarify requirements in Chapter 1, Section 10;
c. Added Note regarding Cybersecurity Framework 2.0 in Chapter 1, Section 12, part b;
d. Added Artificial Intelligence section as Chapter 1, Section 15;
e. Added Chief AI Officer role and responsibilities as Chapter 2, Section 7.
f. Added AO responsibility in Chapter 2, Section 11, part t;
g. Updated System Owners responsibility on inventories in Chapter 2, Section 16, part f;
h. Updated for clarity the assessments required in Chapter 3, Section 4, part a.
i. Added RPA guide reference in Chapter 4, Section 1, part a, and requirement in part c;
j. Removed sections on Bring Your Own Device/personal mobile devices (Chapter 4, Section 1, part g(8)(d) and part rr, Section 7 parts r-t; updated Section 7 part q
k. Updated CUI awareness training requirement in Chapter 4, Section 2, part c.
l. Added Chapter 4, Section 4, part k prohibiting uploading of CUI into any AI Tool;
m. Updated Chapter 4, Section 7, part m, on Bluetooth;
n. Updated and consolidated Chapter 4 Section 7, parts q-t into part q, to clarify mobile applications must adhere to CIO-IT Security-12-67; and
o. Revised Chapter 5, Section 3, part c and l to clarify mobile device monitoring.

4. Applicability.

a. This IT Security Policy applies to all:

(1) GSA Federal employees, contractors, and vendors of GSA, who manage, maintain, operate, or protect GSA systems or data;
(2) IT systems owned and operated by or on the behalf of any of the GSA Service and Staff Offices (SSOs), including Regional Offices; and
(3) GSA or Federal data contained on or processed by IT systems owned and operated by or on the behalf of any of the GSA SSOs, including Regional Offices.

b. Except for Chapter 2, section 21 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. Introduction. The purpose of this Order is to document and set forth GSA's IT Security Policy. This policy facilitates adequate protection of GSA's IT resources by establishing controls required to comply with Federal laws and regulations, Executive Orders, OMB Memoranda, and CISA Cybersecurity Directives.

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. GSA employs management, technical, and operational security controls to achieve the security objectives listed below and manage cybersecurity risk in accordance with (IAW) Executive Order (EO) 13800 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Risk Management Framework. An important component of risk-based management is to integrate technical and non-technical security mechanisms and techniques into a system. 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 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 the other four security

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

f. Resilience. The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

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 necessary to protect CUI (e.g., Personally Identifiable Information [PII], building drawings, proprietary data) and allow GSA IT systems to operate within an acceptable level of residual risk;
- Supporting GSA's objective to ensure 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 laws, orders, directives, regulations, policies, standards, guidelines, and commercial standards:

- 32 Code of Federal Regulations 2002, Controlled Unclassified Information
- Chief Financial Officers (CFO) Act of 1990 (Public Law 101-576)
- CISA Cybersecurity Directives
- Clinger-Cohen Act of 1996 – Divisions D - Federal Acquisition Reform Act (FARA) and Division E – Information Technology Management Reform Act (ITMRA) of the National Defense Authorization Act of 1996 are collectively referred to as the Clinger-Cohen Act
- CSF, Version 1.1, Framework for Improving Critical Infrastructure Cybersecurity
- Cybersecurity Enhancement Act of 2014 (Public Law 113-274)
- EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- EO 14028, Improving the Nation's Cybersecurity
- Federal Information Processing Standard (FIPS) 140-3, Security Requirements for Cryptographic Modules, (Note: Although FIPS 140-3 has been issued, FIPS 140-2 modules will still be accepted for use through September 22, 2026.)
- Federal Financial Management Improvement Act of 1996 (FFMIA) (Public Law

104-208)
- Federal Information Security Modernization Act (FISMA) of 2014 (Public Law 113-283)
- Federal Managers Financial Integrity Act of 1982 (FMFIA) (Public Law 97-255)
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems
- Internet of Things Cybersecurity Improvement Act of 2020 (IoT Act) (Public Law 116-207)
- NIST Special Publications (SPs), GSA implements guidance provided by the NIST 800-series SPs within a year of guide publication, or as directed by the CISO.
- NIST Security Measures for EO-Critical Software Use
  Office of Management and Budget (OMB) Circular A-11, Preparation, Submission and Execution of the Budget
- Office of Personnel Management (OPM) 5 Code of Federal Regulations (CFR) Part 930.301, Subpart C, Information Security Responsibilities for Employees who Manage or Use Federal Information Systems
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB Memoranda, while all memoranda must be complied with, the IT Security Policy has been updated to include requirements from the following memoranda that have been issued since the previous policy:
  - OMB M-23-10, The Registration and Use of .gov Domains in the Federal Government.
  - OMB M-23-13, "No TikTok on Government Devices" Implementation Guidance
  - OMB M-24-10, “Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence”
- Paperwork Reduction Act (PRA) of 1995 (Public Law 104-13)
- PCI DSS (current version), Payment Card Industry Data Security Standard, Public Law No: 113-274.
- Presidential Policy Directive (PPD-21), Critical Infrastructure Security and Resilience.
- Privacy Act of 1974 (5 U.S.C. § 552a)

4. GSA Policies and guidance. This Order provides policies that support the implementation of the following GSA policies and guidance:

- GSAM Part 504.7005, Notification procedures for cyber-supply chain events
- GSA Order ADM 2181.1, Homeland Security Presidential Directive-12, Personal Identity Verification and Credentialing, and Background Investigations for Contractors
- GSA Order ADM 2430.2A, The U.S. General Services Administration Continuity of Operations Mission Essential Functions
- GSA Order ADM 7800.11A, Personal Use of Agency Office Equipment

- GSA Order ADM P 9732.1E, Personnel Security and Suitability Program Handbook
- GSA Order CIO 1820.2, GSA Records Management Program
- GSA Order CIO 1878.3 CHGE 3, Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices
- GSA Order CIO 2101.2, GSA Enterprise Information Technology Management (ITM) Policy
- GSA Order CIO 2103.2, Controlled Unclassified Information (CUI) Policy
- GSA Order CIO 2104.1B CHGE 2, GSA Information Technology (IT) General Rules of Behavior
- GSA Order CIO 2110.4, GSA Enterprise Architecture Policy
- GSA Order CIO 2135.2D, GSA Policy for Information Technology (IT) Capital Planning and Investment Control (CPIC)
- GSA Order CIO 2140.4, Information Technology (IT) Solutions Life Cycle (SLC) Policy
- GSA Order CIO 2160.2B CHGE 4, GSA Electronic Messaging and Related Services GSA Order CIO 2180.2, GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
- GSA Order CIO 2183.1, Enterprise Identity, Credential, and Access Management (ICAM) Policy
- GSA Order CIO 2185.1A, Use of Artificial Intelligence at GSA
- GSA Order CIO 2200.1, GSA Privacy Act Program
- GSA Order CIO 2231.1, GSA Data Release Policy
- GSA Order CIO P 2100.2C, GSA Wireless Local Area Network (LAN)
- Security
- GSA Order CIO P 2165.2 CHGE 1, GSA Telecommunications Policy
- GSA Order CIO 9297.2C CHGE 1, GSA Information Breach Notification Policy
- GSA Order HRM 9751.1A, Maintaining Discipline
- GSA Order OAS 9900.1A, Government Furnished Information Technology (IT) Equipment for Use Outside GSA Agency Worksites
- GSA Order OSC 2106.2A, GSA Social Media Policy
- GSA Order OSC 2140.2A, Management of GSA's Digital Presence
- GSA CIO-IT Security Procedural Guides and Technical Guides and Standards

5. Compliance and Deviations.

a. Compliance is mandatory immediately upon the signing of this Order. All GSA SSOs including Regional Offices, Federal employees, contractors, and other authorized users of GSA's IT resources are required 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 disciplinary actions under GSA personnel policies and/or penalties under criminal and civil statutes.

b. The appropriate Authorizing Official (AO) must approve all deviations from this order and forward a copy of the approval to the 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 Cybersecurity Risk, including a date of resolution to comply.

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

d. In the event of a disruption to normal operations (e.g., a lapse in appropriations) requirements in this directive will be extended until the disruption is resolved. For example, time based requirements (e.g., account disablement, ATO expiration) will have their time extended.

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

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

7. Definitions. For the purposes of this Order 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. Annual Deliverable. An annual deliverable is a quantifiable task, service, or item that must be provided on a yearly basis. An annual deliverable must be delivered or completed by the end of the Federal fiscal year, which begins on October 1st and ends on September 30th of the following year.

c. 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.

d. Authorization. The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency

assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

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

f. Confidentiality. Limiting information access and disclosure and system access to only authorized users, as well as preventing access by, or disclosure to, unauthorized parties.

g. Critical Software. Critical software is defined as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

(1) is designed to run with elevated privilege or manage privileges;
(2) has direct or privileged access to networking or computing resources;
(3) is designed to control access to data or operational technology;
(4) performs a function critical to trust; or,
(5) operates outside of normal trust boundaries with privileged access.

h. Cybersecurity. Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

i. Federal Information System. An information system owned, managed, or operated by an agency, or on behalf of an agency by a contractor, an awardee, or another organization (reference: Draft legislation of the Federal Information Security Modernization Act of 2023).

j. Internet of Things (IoT) Device. Devices that have at least one transducer (sensor or actuator) for interacting directly with the physical world and at least one network interface (e.g., Ethernet, Wi-Fi, Bluetooth) for interfacing with the digital world. (reference: NIST IR 8425).

(1) Contractor system. An information system in GSA's inventory processing or containing GSA or Federal information where the infrastructure and/or applications are wholly operated, administered, managed, and maintained by a contractor on behalf of GSA in non-GSA facilities.
(2) Federal system (i.e., Agency system). An information system in GSA's inventory processing or containing GSA or Federal information where the infrastructure and/or applications are NOT wholly operated, administered, managed, and maintained by a Contractor.

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

l. 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.

m. Major Information System. A system that is part of an investment requiring special management attention as defined in Office of Management and Budget (OMB) guidance and agency policies, or a system that is part of a major acquisition as defined in Part 7 of OMB Circular A-11, Capital Programming Guide, consisting of information resources.

n. Major IT Investment. An investment requiring special management attention as defined in OMB guidance and agency policies or a major acquisition as defined in the OMB Circular A-11, Capital Programming Guide, consisting of information resources.

o. 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).

p. Non-person entity (NPE). An entity with a digital identity that acts in cyberspace but is not a human being. This can include system and service accounts, hardware devices, and software (e.g., robotic process automation, application programming interfaces, etc.).

q. Non-repudiation. Protection against an individual falsely denying having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, and receiving a message.

r. Person. An individual human being with a digital identity, including an individual using an account that is not a uniquely individual account (e.g., a root or administrator account being used by an individual and not an NPE).

s. Personally Identifiable Information. Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

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 Policy and Compliance Division (ISP) at ispcompliance@gsa.gov 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 privacy controls as identified in GSA's Control Tailoring Workbook based on FIPS 199 Level and A&A process and defined in NIST SP 800-53 Revision 5 and GSA Order CIO 1878.3 CHGE 3 .

10. IT Security Controls. All IT systems, including those operated by a contractor on behalf of the Government must achieve an Authorization to Operate (ATO). To achieve an ATO, systems must implement the appropriate set of security and privacy controls defined in NIST SP 800-53 Revision 5 (or subsequent revision based on GSA's implementation guidance for that revision). A system's specified security and privacy controls are determined by:

a. GSA's Control Tailoring Workbook, based on the system's security categorization level IAW FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, and FIPS 200;

b. A GSA determination whether the system contains CUI/PII, such systems must be FIPS 199 Moderate at a minimum;

c. A GSA determination if the system is a High Value Asset (HVA), in which case GSA's HVA Control Overlay as outlined in CIO-IT Security-24-131 must be applied; and

d. The A&A process under which the system is pursuing a GSA ATO per CIO-IT Security-06-30.

11. Contractor Operations.

a. The appropriate security requirements of this Order must be 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 2 and 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 requiring 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 and, for external information systems, in GSA CIO-IT Security-19-101, External Information System Monitoring. 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 and align with the CSF, 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, Common Control Catalog, and GSA CIO-IT Security-18-91, Risk Management Strategy.

b. Chapters 3-7 of this policy are organized into the five core CSF functions of Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). Appendix A details the category and subcategory definitions and unique identifiers. Additional information is available in CSF Version 1.1. Note: The next major revision of this policy will align to CSF 2.0.

13. Cloud Services. No GSA user or SSOs including Regional Offices, shall conduct or acquire any type of pilot involving the use of GSA data or GSA logon credentials 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 based on the processes defined in GSA CIO-IT Security-06-30 or a FedRAMP ATO.

b. GSA users or SSOs may leverage GSA authorized Cloud Service Provider services reviewed by the GSA Security Engineering Division (ISE) and approved by the GSA CISO. Contact SecEng@gsa.gov for the current list of approved services.

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.

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 are subject to the above conditions.

14. Zero Trust. GSA's Zero Trust Strategy Implementation Plan aligns with EO 14028, OMB M-22-09, the ZTA principles of NIST SP 800-207, and CISA's Zero Trust Maturity Model, Version 2.0. It supports the five pillars of: (1) Identity, (2) Devices,(3) Network, (4) Applications and Workloads, and (5) Data and the cross-cutting capabilities of Visibility and Analytics, Automation and Orchestration, and Governance that support the implementation of the pillars. It will be updated as Federal guidance and technological solutions mature regarding zero trust. GSA's organizations and systems are required to align with the plan.

15. Artificial Intelligence. Artificial intelligence (AI) technologies and platforms may only be procured, used, assessed, and monitored at GSA in accordance with GSA Order CIO 2185.1A, "Use of Artificial Intelligence at GSA."

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 "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 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 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 CIO and delegating authority to that individual to ensure compliance with applicable information security requirements;

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

g. Ensuring 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. Risk Executive (Function). The Risk Executive (Function) at GSA is handled by the Enterprise Management Board (EMB), chaired by the Deputy Administrator who is also the Senior Accountable Official for Risk Management (SAORM). For cybersecurity risks, the CISO, AOs, and subject matter experts facilitate the consistent application of risk management across GSA. The CISO coordinates with the CIO, a member of the EMB, to identify cybersecurity risks for consideration by the EMB. As stated in the EMB,

the Risk Executive (Function) manages and monitors key organizational risks, including those associated with enterprise-wide investments by:

a. Providing a forum to identify and discuss cross-cutting strategic, reputational, regulatory, operational, cybersecurity, financial, and other risks;

b. Elevating new or emerging risks and communicating the status of existing risks, including ongoing mitigation efforts;

c. Identifying risk owners and considering mitigation strategies and/or corrective actions;

d. Considering the effect of these efforts on new or ongoing resource allocation decisions;

e. Maintaining and maturing GSA's risk management framework, including its risk tolerance thresholds, risk appetite, and enterprise risk profile;

f. Engaging with other GSA governance groups, as needed, to provide strategic guidance;

g. Assigning action items to GSA Services and Staff Offices (SSOs) and their governance board for review and implementation;

h. Establishing risk management roles and responsibilities;

i. Developing and implementing an organization-wide risk management strategy that guides and informs organizational risk decisions (including how risk is framed, assessed, responded to, and monitored over time;

j. Determining organizational risk based on the aggregated risk from the operation and use of information systems and the respective environments of operation; and

k. Ensuring shared responsibility for supporting organizational missions and business functions using external providers receives the needed visibility and is elevated to appropriate decision-making authorities.

3. GSA 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 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. Ensuring senior agency officials, including CIOs of bureaus or equivalent officials, carry out their information security responsibilities for securing information and information systems supporting operations and assets under their control;

g. Ensuring all personnel are held accountable for complying with the agency-wide information security program, including taking actions when violations are identified IAW GSA Order HRM 9751.1A, Maintaining Discipline.

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

i. 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;

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

k. Coordinating and reporting on Presidential Policy Directive (PPD-22), Critical Infrastructure Security and Resilience critical infrastructure assets;

l. 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;

m. Ensuring Privacy Threshold Assessments (PTAs), System of Records Notices (SORNs), and Privacy Impact Assessment (PIAs) prepared by GSA organizations for security considerations are reviewed;

n. Providing guidance or input for periodic assessments of SSOs including Regional Offices security measures and goals to assure implementation of GSA policy and procedures;

o. Participating as a member of the GSA Full Response Team IAW GSA Order CIO 9297.2C CHGE 1 to determine if a major incident has occurred;

p. Coordinating with the CISO and consulting with the Deputy Administrator, as necessary, regarding cybersecurity risks; and

q. Participating as a member of the EMB and coordinating with the CISO to identify cybersecurity risks for consideration by the EMB.

4. Chief Financial Officer (CFO). The CFO also has statutory security responsibilities under the Chief Financial Officers 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 the 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 and Investment Control (CPIC) 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 CPIC 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 monitoring SSAE 18 reporting submissions.

5. GSA Senior Agency Official for Privacy (SAOP). The SAOP has statutory responsibilities under the Privacy Act of 1974, GSA Order CIO 2200.1, 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 NIST SP 800-53, Revision 5 as appropriate;

b. Designating which privacy controls can be treated as common and hybrid;

c. Reviewing and approving system categorizations for systems collecting, maintaining, or disseminating PII;

d. Overseeing privacy control assessments as part of the Authorization to Operate (ATO) cycle;

e. Reviewing authorization packages for any GSA IT system that collects, maintains, or uses PII to ensure compliance with applicable privacy requirements and to manage privacy risks prior to AOs making risk determination and acceptance decisions;

f. Reviewing and signing the Certification letter for systems that have a SORN and/or PIA;

g. Ensuring 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;

h. Ensuring PTAs, SORNs, and PIAs are conducted for information systems and collections and ensuring annual SAOP reports are submitted to OMB;

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

j. 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

k. Participating as the GSA Full Response Team leader IAW GSA Order CIO 9297.2C CHGE 1 if a major incident involving privacy has occurred.

6. GSA Senior Agency Official (SAO) for CUI. The SAO for CUI is responsible for overseeing GSA's CUI Program. Information security responsibilities include:

a. Ensuring proper handling, marking, protection and destruction of all types of unclassified sensitive information;

b. Ensuring IT system and application owners conduct self-assessments to identify and mitigate potential risks to CUI; and

c. Determining if an incident of CUI misuse warrants an inquiry and reporting to the CUI Executive Agent.

7. Chief AI Officer (CAIO). The CAIO's full responsibilities are identified in CIO Order 2185.1. Responsibilities related to information security include:

a. Establish and update processes to measure, monitor, and evaluate the performance, accessibility, equity, cost, and outcomes of AI applications;

b. Establish, maintain, and chair AI oversight governing bodies;

c. Oversee the development of GSA's AI inventory and other necessary reporting;

d. Issue waivers for individual applications of AI, in coordination with other officials responsible for those AI applications, from elements of Section 5 of OMB M-24-10; and

e. Establish, and maintain over time, criteria for categories of individual applications of AI that do not require disposition through the AI Governance Board or AI Safety Team.

8. 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. Overseeing the development, publishing, and effectiveness of GSA security

d. policies and IT security procedural guides consistent with this policy;

e. Ensuring written agreements assign security-related functions and identify security responsibilities of each SSO including Regional Offices or activity when two or more activities use the same IT;

f. Providing guidance, advice, and assistance to all SSOs including Regional Officers, on IT security issues, the IT Security Program, and security policies;

g. Reporting to agency senior management on policy compliance;

h. 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;

i. Managing the OCISO which implements the GSA IT Security Program;

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

k. Periodically assessing risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems supporting agency operations and assets;

l. Addressing any deficiencies in the information security policies, procedures, and practices of the agency;

m. Ensuring the development and implementation of procedures to detect, report, and respond to security incidents;

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

o. 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;

p. Implementing performance measures to evaluate the effectiveness of technical and non-technical safeguards protecting GSA information and information systems;

q. Periodically assessing SSO (including Regional Offices) security measures and goals to assure implementation of GSA policy and procedures;

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

s. Administering FISMA requirements and coordinating GSA's annual FISMA security program review and Plan of Action and Milestones (POA&M) implementations;

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

u. Participating as the GSA Full Response Team leader, IAW GSA Order CIO 9297.2C CHGE 1 , if a major non-privacy incident has occurred;

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

w. Consulting with the Deputy Administrator, in coordination with the CIO, as necessary, regarding cybersecurity risks;

x. Coordinating with AOs and experts within the OCISO to apply consistent management of cybersecurity risks across GSA;

y. Providing authoritative decisions, or designating personnel to do so, in support of DevSecOps teams as specified in GSA CIO-IT Security-19-102, DevSecOps OCISO Program, and:

z. Coordinating with the CIO to identify cybersecurity risks for consideration by the EMB.

9. HSSOs. Heads of Services and Staff Offices (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 contractors performing services associated with GSA systems (e.g., system development, maintenance, 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.

10. GSA Chief Privacy Officer (CPO). The CPO is responsible for overseeing GSA's Privacy Program. The CPO's mission 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 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 5, as appropriate;

b. Verifying 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. Reviewing and approving PTAs, SORNs, and PIAs for information systems and collections and coordinating submission of all annual SAOP reports 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 CIO 9297.2C CHGE 1.

11. Authorizing Official (AO). An AO is the Federal Government management official with the responsibility of identifying the level of acceptable risk for an information system, application, or set of common controls and determining whether an acceptable level of risk has been obtained. Final authority to operate or not operate for an information system, application, or a set of common controls 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, application, or set of common controls under their purview based on the acceptability of the implementation of security safeguards in place (risk-management approach);

b. Reviewing and approving all deviations and Acceptance of Risk (AoR) letters based on policies in this Order as described in Chapter 1, Section 5, Compliance and Deviations, of this Order;

c. Ensuring all information systems, applications, or sets of common controls under their purview have a current ATO issued IAW A&A processes defined in GSA CIO-IT Security-06-30 Managing Enterprise Cybersecurity Risk;

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 information systems and applications 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&Ms IAW GSA CIO-IT Security-09-44, Plan of Action and Milestones (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 cybersecurity 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 2200.1, GSA Order CIO 1878.3, and NIST SP 800-53, Revision 5;

j. Reviewing and approving PTAs/PIAs for information systems and applications 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 CIO 9297.2C CHGE 1;

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 information systems and applications 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 information systems and applications by members of the GSA OIG as described in paragraph 22 of this chapter;

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

r. Ensuring information systems and applications handling payment card data meet the security requirements of the PCI DSS; and

s. Coordinating with the CISO and experts within the OCISO regarding the consistent management of cybersecurity risks across GSA.

t. Supporting System Owners, ISSMs, and ISSOs in maintaining accurate inventories as identified in Chapter 3, Section 1, Item a (e.g., systems, hardware, software, HVA).

12. 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. Managing an OCISO Division to implement the GSA IT Security Program and ensuring the organizations under their responsibility meet program goals;

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

e. Advising individuals with IT Security responsibilities on proper system security, security “Best Practices,” and applicable laws and regulations;

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

g. Interfacing with the Technical Standards Committee regarding security;

h. 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., Government Accountability Office (GAO), OIG);

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

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

k. 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;

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

m. Appointing ISSMs and ISSOs in writing for GSA systems;

n. Participating as a member of the GSA Full Response Team (ISE Division Director) as defined in GSA Order 9297.2C CHGE 1 to determine if a major incident has occurred. The ISE Division Director may designate a representative to fulfill this responsibility on a case-by-case basis; and

o. Collaborating with system personnel and others, as required, to collect data and report to OMB, DHS, or other Federal authorities information regarding cybersecurity (e.g., CISA directives, the Cybersecurity Coordination, Assessment, and Response Protocol [C-CAR], critical software).

13. ISSM. The ISSM, who must be a Federal employee, serves as an intermediary between 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. The ISSO Support Division (IST) facilitates integrating IT security in programs and compliance with required security and privacy requirements. The GSA official system inventory repository contains a current list of ISSMs. 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, including the usage of GSA's implementation of its current Governance, Risk, and Compliance (GRC) solution;

d. Reviewing and approving ISSO checklists submitted in GSA's current implementation of its GRC solution and coordinating with ISSOs, as necessary, for systems under their purview;

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

f. 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;

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

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

14. ISSO. The ISSO ensures implementation of adequate system security 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. ISSO Checklists consisting of recurring tasks ISSOs must perform are managed in GSA's implementation of its current GRC solution; ISSOs receive notification to complete checklists when they are generated. A current list of ISSOs is located in the GSA official system inventory repository, GSA EA Analytics and Reporting (available only to those on GSA's network). 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, including the usage of GSA's implementation of its current GRC solution;

d. Completing the recurring activities in ISSO checklists, completing the checklists in GSA's implementation of its current GRC solution and submitting the checklists when completed;

e. Assisting the AO, data owner and Contracting Officer (CO)/Contracting Officer Representative (COR) 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;

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; and

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

15. Privacy Analyst. Privacy Analysts are responsible for ensuring implementation of adequate privacy for a system in order to document, mitigate, and minimize the privacy risks associated with collecting, using, processing, storing, maintaining, and disseminating PII. A Privacy Analyst must be assigned for every information system that contains PII and may have responsibility for more than one system, provided there is no conflict. For their assigned systems, delegated responsibilities may include:

a. Approving system categorizations for systems that contain PII in accordance with FIPS 199 and overseeing proper implementation of privacy controls;

b. Overseeing proper implementation of privacy controls and privacy assessments;

c. Approving the SSPP;

d. Reviewing and signing the Certification letter for systems that have a SORN and/or PIA; and

e. Reviewing PTAs to ensure privacy controls address the risks associated with collecting, using, processing, storing, and disseminating PII. Once a system is identified as having potential privacy implications, the Privacy Analyst determines if a PIA is required.

16. System Owners. System Owners are GSA management officials with responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems. System Owners cannot be ISSOs or ISSMs. 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. Creating and maintaining their system SSPP(s);

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

d. 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;

e. 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;

f. Coordinating with the OCISO, ISSM, and ISSO to maintain accurate inventories as identified in Chapter 3, Section 1, Item a (e.g., systems, hardware, software, HVA);

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

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

i. 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;

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

k. Ensuring 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;

l. 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);

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

n. 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;

o. 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;

p. 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;

q. 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 and Privacy Plan and ensuring that the system is deployed and operated according to the agreed-upon security requirements;

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 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 supports GSA's plan to comply with OMB M-21-31 active and cold data storage time frames;

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;

ee. Participating as a member of the GSA Full Response Team as defined in GSA Order 9297.2C CHGE 1 to determine if a major incident has occurred; and

ff. Managing DevSecOps teams implemented for their systems in collaboration with OCIO-assigned DevSecOps engineer(s).

17. 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 several 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;

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

d. Participating as a member of the GSA Full Response Team as defined in GSA Order CIO 9297.2C CHGE 1 to determine if a major incident has occurred for a system under their purview.

17. 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.

18. 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 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 who 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 and Privacy Awareness course);

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 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 supports GSA's plan to comply with OMB M-21-31 active and cold data storage time frames;

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.

19. 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 information security responsibilities:

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

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

c. Ensuring 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 measurable performance requirements;

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 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.

20. 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 with physical access to devices when needed as part of any incident response effort.

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

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

c. Ensuring adequate protection is maintained on all Government Furnished Equipment (GFE), 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;

d. Accessing systems and data only on a need-to-know, need-to-use, and need-to-share basis;

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

f. Ensuring any sensitive data (e.g., PII, PCI, CUI, authenticators, business 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, are encrypted with GSA-provided encryption;

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

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

22. GSA Office of Inspector General (IG). The GSA OIG 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 information systems:

(1) For the OIG, the point of contact will be the Assistant Inspector General for Auditing (AIGA) or the AIGA's designees. For the SSOs within GSA, the points of contact will be the AO for each information system;

(2) The AIGA will notify the AO of the information system within the AIGA's purview which OIG personnel need to access;

(3) The AO will inform the AIGA of the highest classification level of information on the system and all required security and privacy awareness training required for GSA and/or contractor personnel 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) Regarding 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 14 calendar days after completion of the above steps, the AO will inform the 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.

23. GSA Personnel Security Officer, 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.

24. Office of Human Resources Management (OHRM). The Human Resource Office and Security Office are responsible for designating the risk levels for all occupations in GSA and incorporate the risk level in the position designation(s) for each series and grade.

25. 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 ELP to identify potential security issues as specified in the SSPP.

26. 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 and Privacy 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.

27. OCISO DevSecOps Program (ODP) Security Engineer. ODP Security Engineers are responsible for:

a. Collaborating with the system team on all aspects of system security;

b. Engaging on solution design, planning, and criteria for security requirements;

c. Interpreting security requirements from policies and standards and their applicability to the development project;

d. Integrating security analysis into the change management processes;

e. Collaborating on security code review and compliance impact analysis; and

f. Acting as liaison with the OCISO for decisions and approvals.

CHAPTER 3: POLICY FOR IDENTIFY FUNCTION

This chapter provides security policy statements for the CSF Identify function, which allows GSA to develop an understanding of its systems, assets, data, and capabilities 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 specific policy statements supporting outcomes for the CSF Identify categories and subcategories. Appendix A details specific Identify Category and Subcategory definitions and unique identifiers.

1. Asset Management.

a. System Owners and their teams, ISSMs, and ISSOs must maintain the following inventories in coordination with the OCISO:

(1) An inventory of GSA information systems (including hardware, software, and other data required by Federal or GSA requirements) in GSA's official system inventory repository;
(2) An inventory of the devices/components comprising information systems IAW GSA CIO-IT Security-01-05, Configuration Management (CM);
(3) An inventory of critical software (IAW OMB M-21-30), which must have the security objectives from NIST's Security Measures for EO-Critical Software Use webpage implemented;
(4) A High Value Asset (HVA) inventory IAW BOD 18-02; and
(5) An inventory of information systems and assets that contain cryptanalytically-relevant quantum computer (CRQC)-vulnerable cryptographic systems, including high impact systems, agency HVAs, and any other systems determined to be vulnerable to CRQC-based attacks.

b. Federal Systems on the GSA Enterprise-on premise and in a Federal Managed Cloud environment shall maintain an up-to-date inventory of assets, including using approved Enterprise tools to do so, and leveraging the GSA Enterprise Continuous Diagnostics and Mitigation (CDM) solution.

c. CIO-IT Security-24-125 provides guidance on information exchanges and the types of agreements based on the level and type of data exchanged, the type or method of exchange, and if the exchange is between GSA systems (internal) or between GSA and another entity's systems (external). All communications and data flows and system interconnections, both internal and external, for an information system must be documented in the System Security and Privacy Plan (SSPP). All information exchanges and agreements must be reviewed and certified or updated on the specified timeframe within the agreement (typically annually).

d. All information systems must comply with NIST SP 800-60, Volume 1, Revision 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).

e. 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.

f. All GFE, including PIV cards, must be returned to GSA at the end of a contract and when contract personnel no longer support a contract and as directed by a Contracting Officer.

g. Per OMB M-21-07, all IP-enabled assets within GSA's Federal systems must:

(1) Transition to Internet Protocol Version 6 (IPv6) only environments by the end of FY25.

(2) Be identified as unable to be converted to use IPv6 with a justification and a schedule for replacing or retiring these assets.

h. Per OMB M-23-10, the registration and use of .gov domains in the Federal Government, and GSA and its information systems must use government domains (i.e., .gov or .mil) for all official communications, information, and services, except for third party services operated by non-governmental entities on non-governmental domains that are needed to effectively interact with the public (e.g., social media services, source code collaboration, and vulnerability disclosure reporting systems).

2. Business Environment.

a. GSA's roles within the supply chain are: (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 roles identified in the previous paragraph, 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 PPD-21 GSA, in consultation with the Department of Defense (DOD), DHS, and other departments and agencies as appropriate, shall provide or support government-wide contracts for critical infrastructure systems and ensure such contracts include audit rights for the security and resilience of critical infrastructure.

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

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

f. Integrate and explicitly identify funding for information systems and programs into IT investment and budgeting plans per GSA Order CIO 2135.2D, GSA Policy for IT Capital Planning and Investment Control. 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.

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

h. 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. GSA's 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 PTA and a 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 CIO 1878.3 CHGE 3.

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 CIO 1820.2, GSA Records 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:

(1) Before a system is 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 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. Authorizations can be granted with or without restrictions or limitations. Authorizations with restrictions must identify in the ATO package's Certification and ATO Letters the conditions needing to be resolved and their associated POA&M IDs. Authorizations with conditions (i.e., conditional ATOs) should be issued for a length of time sufficient to allow the conditions to be satisfied. Once the conditions are satisfied, a new unrestricted ATO will be granted for the remainder of the specific A&A process's ATO length.

m. Extension of a system's current ATO for a period not to exceed one year (365 days) may be requested only under one of the following conditions. The system must continue to maintain its complete set of A&A documentation (e.g., System Security and Privacy Plan, Contingency Plan, POA&Ms). All actions to satisfy the following conditions 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;
(7) Completing the system's security assessment has been delayed due to contract issues; or
(8) Complying with Showstopper Controls as listed in CIO-IT Security-06-30.

n. 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 30 days from the date of the ATO expiration to allow mitigation of the High and Very High/Critical vulnerabilities. No more than two extensions may be granted under this condition.

4. Risk Assessment.

a. Every government and contractor IT system operated must undergo a security and privacy control assessment utilizing GSA test cases based on NIST SP 800-53A, Revision 5, Assessing Security and Privacy Controls in Information Systems and Organizations, the GSA A&A process the system is following, and the system's type (e.g., HVAs per CIO-IT Security 24-131). Systems must assess risk per GSA's 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. "Independent" testing means the testers are free from any perceived or actual conflicts of interest regarding the development, operation, or management of the information system(s) targeted by the penetration test.

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. All FIPS 199 High impact information systems and HVAs are required to complete a Red Team exercise as part of their A&A and annually thereafter.

e. The OCISO must identify sources of cyber threat information (e.g., CISA Cybersecurity Directives, US-Computer Emergency Readiness Team [US-CERT] Alerts, etc.) and a process for sharing the information, as appropriate.

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

g. 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.

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

i. 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.

j. The Common Control Catalog (CCC), which documents the enterprise-wide common controls and hybrid controls with an enterprise-wide common portion, must be assessed at least every three years using GSA's security assessment process as defined in CIO-IT Security-06-30. A security assessment report will be produced based on this assessment.

5. Risk Management Strategy.

a. To implement and maintain a risk management process for all information systems, the OCISO is guided by 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.

6. Supply Chain Risk Management.

a. The OCISO Cyber Supply Chain Risk Management (C-SCRM) Program addresses cyber risks both prior to and post contract award for information and computer technology (ICT) products and services. Accordingly, all GSA systems must manage risks to their cyber supply chain IAW:

(1) CIO-IT Security-21-117, OCISO Cyber Supply Chain Risk Management (C-SCRM) Program;
(2) CIO-IT Security-22-120, Supply Chain Risk Management (SR) Controls;
(3) CIO-IT Security-09-48, Security Language for IT Acquisition Efforts; and

(4) NIST SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

b. Cyber Supply Chain events must be reported to the GSA IT Service Desk IAW GSAM Part 504.7005, Notification procedures for cyber-supply chain events.

c. Acquisition professionals must consider potential cyber supply chain risks as part of the acquisition process as follows:

(1) IAW GSAM Part 504.7005.

(2) When applicable, if the original equipment manufacturer (OEM) has a program to authorize both the product's pricing and sale by a third-party vendor, proof of the bidder's authorized standing with the OEM is required prior to any business-award.

d. Systems, their suppliers and third-party suppliers must comply with:

(1) Public Law 115-91, National Defense Authorization Act for Fiscal Year 2018, Section 1634, Prohibition on Use of Products and Services Developed or Provided by Kaspersky Lab, which prohibits the use of any hardware, software, or services developed or provided in whole or in part by— (1) Kaspersky Lab (or any successor entity), (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab, or (3) any entity of which Kaspersky Lab has majority ownership.

(2) Federal Acquisition Regulation (FAR) 52.204-25. It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115-232) the procuring or obtaining or extending or renewing a contract to procure or obtain equipment or services produced or provided by the following organizations unless an exception or waiver is granted per the law or the FAR; (1) Huawei Technologies Company, (2) ZTE Corporation, (3) Hytera Communications Corporation, (4) Hangzhou Hikvision Digital Technology Company, (5) Dahua Technology Company, and any subsidiary or affiliate of these companies.

(3) FAR 52.204-27 which prohibits under Section 102 of the Consolidated Appropriations Act 2023, Public Law 117-328, the presence or use of TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited from being used on any information technology as defined in 40 U.S.C. § 11101(6).

(4) Actions specified in Federal mandates, including but not limited to Federal Laws, Executive Orders, OMB Memoranda, and Cybersecurity Directives when the mandate is applicable to their system or the components therein. System and organizational personnel shall provide data to support compliance with the applicable Federal mandates as requested.

e. Appropriate personnel (e.g., Requiring Official, CO, COR) 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.

f. All information systems must develop anti-counterfeit procedures that include detection of counterfeit hardware or software components consistent with NIST SP 800-53, Revision 5.

g. Internet of Things (IoT) devices cannot be procured unless a review of the contract by the CIO identifies that it complies with NIST SP 800-213 or the CIO grants a waiver under one of the conditions of the IoT Act. Any waivers must include the elements identified in the IoT Act and be sent to the GSA Administrator.

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.

This chapter provides the specific policy statements supporting outcomes for the CSF Protect categories and subcategories. Appendix A details specific Protect category and subcategory definitions and unique identifiers.

1. Identity Management, Authentication and Access Control.

a. The following GSA procedural guides provide specific implementation guidance and/or 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
- GSA CIO-IT Security-19-97: Robotic Process Automation (RPA) Security
- Hardening Guides: Multiple guides for configuring various technologies IAW with GSA required security settings

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

c. Robotic Process Automation (bots) at GSA must be approved, managed, and monitored in accordance with CIO-IT Security-19-97: Robotic Process Automation (RPA) Security.

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

(1) Federal employees on detail to GSA issued a PIV by their assigned Agency.
(2) Employees or contractors expected to be employed for less than 180 days and not issued a PIV.
(3) Any person with a disability prohibiting the use of 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 45 days.

e. Authentication schemes for all systems and users must utilize MFA using two or more types of authentication factors. GSA systems with non-privileged users should integrate with GSA approved centralized authentication services using Security Assertion Markup Language (SAML 2.0) or OpenID Connect. The centralized authentication services will manage the MFA options available to the users to allow for users to have accessible and secure options suited for their affiliation and interaction with the system.

f. New or modernizing applications must have their authentication options evaluated by the ICAM Portfolio, as identified in GSA Order CIO 2183.1.

g. For password-based authentication:

(1) A list of commonly used, expected, or compromised passwords must be maintained and updated within 12 months of the latest available version of the utilized bad and/or compromised password database checking list (e.g., haveibeenpwned.com) and when organizational passwords are suspected to have been compromised directly or indirectly;

(2) User created or updated passwords must be checked to ensure they are not found on the list of commonly used, expected, or compromised passwords;

(3) Passwords must be transmitted only over cryptographically protected channels;

(4) Passwords must be stored using an approved salted key derivation function, preferably using a keyed hash;

(5) Immediate selection of a new password upon account recovery must be required;

(6) User selection of long passwords and passphrases must be allowed, including spaces and all printable characters;

(7) Automated tools must be employed to assist the user in selecting strong password authenticators; and

(8) The following composition and complexity rules must be enforced:

(a) For persons accessing operating systems (workstations and servers), passwords must:

1. Contain a minimum of 16 characters;
2. Have passwords changed when a password is compromised or forgotten; and
3. Not have complexity requirements.

(b) For persons not accessing operating systems (e.g., other applications), passwords must:

1. Contain a minimum of 8 characters;
2. Have passwords changed when a password is compromised or forgotten; and
3. Require a combination of letters, numbers, and special characters if no password checking solution is used; or
4. Have no complexity requirements, if a password checking solution to check a database of known bad passwords is used (e.g., checks for commonly used, expected, or compromised passwords; dictionary words; repetitive or sequential characters such as ‘aaaaaaaa,’ ‘1234abcd,’ ‘1qaz2wsx;’ or context sensitive words such as the username or a derivative).

(c) For non-person entities (NPE), if passwords are required to be used (in lieu of stronger cryptographic means):

1. Contain a minimum of 8 characters and change every 90 days, or contain minimum of 24 characters and change every 365 days;
2. Have passwords changed when a password is compromised or forgotten; and
3. Require a combination of letters, numbers, and special characters.

(d) Passwords for all mobile devices such as GSA approved phones, iPads, and tablets must be a minimum of 6 characters.

h. Protection and handling of passwords

(1) Passwords must not be stored in forms (e.g., Windows dialog boxes, web forms).

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

(3) Password distribution:

(a) Passwords used for authentication (other than default or one-time use 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 channels (e.g., email, text, telephone).
(d) Passwords used for authentication (other than default or one time use passwords) must not be transmitted in clear text.

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

(5) One-time use passwords must expire in two minutes if based on a real-time clock.

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

i. Non-person entities (NPE) must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing accounts. Reviews and validations of all accounts shall be completed consistent with the SSPP to ensure the continued need for system access.

j. Information system user accounts (i.e., persons) must be managed for all systems, including establishing, activating, modifying, reviewing, disabling, and removing user accounts. Reviews and validations of all user accounts shall be completed consistent with the SSPP to ensure the continued need for system access. GSA user account management processes include:

(1) Supervisors, CORs, or account managers coordinating and arranging system access termination for all departing or resigning personnel, including both GSA employees and contractors.
(2) Supervisors, CORs, or account managers initiating account removal, disablement, or permission changes based on a review of information provided by the OCISO (e.g., separation lists, role revisions) for GSA users, including both GSA employees and contractors.
(3) System Owners/account managers verifying that separated GSA users, i.e., users with an ENT account, no longer maintain access to GSA IT systems or resources after 30 days of separation. Verification of non-GSA users' access removal must be performed within the time period specified in the SSPP in NIST control AC-2(3).
(4) ISSOs, ISSMs, and System Owners ensuring processes for removing or modifying access to GSA systems, based on terminations and transfers, are performed IAW procedures specified in GSA CIO-IT Security-03-23.
(5) Supervisors, CORs, or System/Data Owners submitting GSA user access requests and user permission or role changes for account manager approval based on a user's job function and need-to-know.
(6) System Owners/Data Owners, with assistance from the designated ISSO, ensuring 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.
(7) System Owners/Data Owners, with assistance from the designated ISSO, ensuring system access authorizations enforce separation of duties, see Separation of duties.

j. Data or System Owners only grant access to an information system based on a valid need-to-know/need-to-share determined during the account authorization process and the intended system usage.

k. A user account that has been or is expected to be idle for an extensive period of time consistent with account abandonment must be disabled.

l. To securely share files in Google Drive/Google Sites with other government customers and business partners who do not use Google in their workplace, a GSA Affiliated Customer Account (GACA) must be created by the external non-GSA user. GSA employees, contractors, or other users (e.g., detailees, interns) requiring regular/repeated access to the GSA network to conduct business are not permitted to use GACA accounts.

m. 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.

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. Access to rooms, work areas/spaces, and facilities containing agency systems, networks, and data must be limited 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). These records must be reviewed at least annually. 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 the individual verifying the visitor’s credentials.

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. FIPS 199 Moderate and High systems must terminate user sessions regardless of user activity:

(1) After 30 minutes of inactivity.
(2) Thirty days for systems at AAL1.
(3) Twelve hours for systems at AAL2 and AAL3.

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 with the ability to check 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) on the client machine. Machines failing this scan will not be allowed access to the GSA network or any GSA IT resources.
(3) Only properly secured GSA GFE (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 to provide detection of intrusion attempts and protection against unauthorized access.

(1) Only GSA employees and contractor personnel are permitted to use GSA furnished computers, a GSA VPN connection, a Zscaler Private Access connection, or a GSA provided or funded internet connection.

(2) Connections to other networks or computers (split tunneling) are not permitted when connected to the GSA network. However, accessing GSA's network unless approved by GSA's CISO. However, accessing GSA's network via the GSA-provided VPN software over a network is allowed.

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

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. Workstations shall only be operated with assigned user level rights. If elevated privileges on a workstation are required as part of assigned job duties (such as development work), they must be exercised in an admin VDI pool virtual workstation.

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. 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.

cc. 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.

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

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

ff. Separation of duties. The following requirements are required for FIPS 199 Moderate and High systems only.

(1) Any access or permissions clearly violating established separation of duties policies must be coordinated with the designated SSO and ISSM/ISSO to correct or resolve conflicting role assignments.

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

(3) 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. 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.

(4) 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. 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.

(5) Every SSO including Regional Offices, 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 increases the risk of unauthorized modifications to programs being implemented into production systems, introducing vulnerabilities, and negatively impacting the integrity and availability of data generated and stored in the system.

(6) 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 sharing data or passing transactions to identify conflicts with separation of duties policy).

(7) Job descriptions and roles must be documented 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.

(8) Formal procedures must be established to guide personnel in performing their duties, with identification of prohibited actions violating separation of duties.

(9) Duties shall be segregated among users, ensuring 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 requiring 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 requiring 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 exceeding some limit requiring a supervisor's review and approval).

(10) A system leveraging an agile development methodology in a DevSecOps environment must follow separation-of-duties best security practices IAW CIO-IT Security-19-102, DevSecOps Program OCISO.

(11) Proper separation of duties must be ensured for GSA IT system maintenance, management, and development processes.

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

(13) Since critical processes can span separate and distinct applications and systems, all SSOs including Regional Offices 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 spanning multiple IT systems or applications to uncover conflicts not 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).

(14) All SSOs including Regional Offices must establish physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities.

(15) Annual assessments must review the effectiveness of control techniques, with an emphasis on activities unable to 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).

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

hh. 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) Use of the Auth 2.0 Access Scopes listed below is 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 management of user calendars.

(c) Act on Behalf of User. Allows view and modify but not deletion of user email.

(d) Full Data Access. Allows view and management 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, sex, 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 providing access to publicly available information and do not conflict with prohibited access scopes.

ii. 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 OCISO 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 SSO 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.

jj. 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.

kk. 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 smartphone devices, laptop, USB drive) do not require written permission or encryption. Paper "cascade lists," limited to name and home phone number, 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.

ll. System and/or data owners must verify that data extracts containing PII are handled IAW the GSA Rules of Behavior for Handling PII (GSA Order CIO 2180.2). PII must only be disclosed on the basis of a lawful government purpose within GSA and disposed of IAW the applicable records retention schedule.

mm. Non-GFE cannot access the GSA internal wireless network in Regional and Central Office Buildings; they can connect only to the GSA Guest Wireless Network to access the Internet and GSA resources available to the public (www.gsa.gov).

(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.

nn. 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).

oo. All GFE/GSA procured workstations/mobile devices such as phones and tablets, 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.

pp. 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 and Proxy Change Request Process. This includes changes to desktop firewall and intrusion prevention systems.

qq. 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.

rr. All information systems allowing 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 Identity Acceptance Statement IAW NIST SP 800-63-3.

ss. 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.

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

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

vv. 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.

a. All GSA employees and contractors, as appropriate given their role and security responsibilities, must adhere to training requirements in GSA CIO-IT Security-05-29: Security and Privacy Awareness and Role Based Training Program.

b. Failure to comply with annual awareness and specialized IT security training requirements will result in termination of access to the GSA enterprise and applications. AOs can terminate system accounts.

c. All personnel must complete CUI awareness in accordance with GSA CIO Order 2103.2, “Controlled Unclassified Information (CUI) Policy.”

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

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

3. Accessing GSA Resources.

a. GSA enterprise users must read and acknowledge GSA Order CIO 2104.1B CHGE 2, GSA IT General Rules of Behavior, within 90 days of being granted access to the enterprise, and annually thereafter.

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

c. Users have no expectation of privacy on GSA IT systems. All activity on GSA IT systems is subject to monitoring and internal GSA IT systems must display an approved warning banner to all users indicating the system is subject to monitoring. The following warning banner must be based on these instructions:

(1) Paragraph two of the warning banner is only required if the system contains CUI;
(2) Paragraph three is optional but is a best practice.
(3) For publicly accessible sites (i.e., open to the Internet), the sentence “Therefore no expectation of privacy is to be assumed” shall be removed.

**********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.

This system contains Controlled Unclassified Information (CUI). All individuals viewing, reproducing or disposing of this information are required to protect it in accordance with 32 CFR Part 2002 and GSA Order CIO 2103.2 CUI Policy.

For additional information: [contact information or website where users can get help]
****

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

e. Purchased software and upgrades to existing software must be able to run with user level rights. Existing software may be configured to allow for read/write access to a specific folder to allow it to function.

f. 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.

g. 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.

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

i. Local support or Client Engineering will install all approved software.

j. 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. Such tools may, for example, defeat software copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files.

k. GSA provides access to email and social media for Government business. However, users may occasionally make personal use of email and social media involving 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 Communications (OSC) Enterprise Web Management (EWM) group which can monitor and assist with GSA branding and other aspects related to dealing with the public.

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

m. 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 libelous or defamatory material pertaining to GSA, the Federal Government, or any agency employee or official.
(3) Transmitting sexually explicit or offensive material, non-business related large attachments, chain letters, un-authorized mass mailings, or intentionally sending a virus/worm.

n. 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.

o. 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., websites 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), including the user's personal email address(es).

(7) Sending email messages including sensitive information, such as PII, as deemed by the Data Owner, without GSA-provided encryption.

(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.

p. 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).

q. Additional guidance regarding GSA's policy on email is available in the following GSA Orders:

(1) CIO 2160.2B CHGE 4, GSA Electronic Messaging and Related Services,
(2) ADM 7800.11A, Personal Use of Agency Office Equipment,
(3) CIO 2140.4, Information Technology (IT) Solutions Life Cycle (SLC) Policy
(4) CIO P 2165.2 CHGE 1, GSA Telecommunications Policy.
(5) Guidance on social media is available in OSC 2106.2.

r. GFE must not be taken on international travel without prior approval. Users must submit a GSA IT Service Desk ticket and receive approval from GSA IT and their supervisor with a recommendation for approval or disapproval from the OMA Threat Management Office related to country specific threat assessment.

(1) Covered Individuals, as defined in Security Executive Agency Directive (SEAD) 3, must contact OMA prior to any international travel.

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

s. Any GSA employee who must work while overseas (except for OIG employees) 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.

t. If access to the GSA network is needed when traveling outside the United States, use a GSA virtual interface (e.g., Citrix, VDI).

u. Limit WiFi connections to trusted outlets (e.g., business office); do not use public WiFi.

v. If taking a GFE phone, submit an IT Service Desk ticket for International Service. If the phone is connected to WiFi while overseas, it must be wiped upon return.

4. Data Security.

a. All sensitive data (to include PII/CUI and PCI data; authenticators including but not limited to passwords, tokens, keys, certificates, and hashes; and business sensitive data as determined by the AO) must be encrypted everywhere (i.e., at file level, database level, at rest, and in transit). Encryption algorithms and modules must be FIPS 140-3/140-2 validated.

(1) For databases, encryption of the whole database, table, column, or field levels is acceptable, as appropriate. Other methods including but not limited to application encryption or tokenization is also acceptable.

(2) For web services connections, implement end-to-end encryption terminating the connection at the web server; connections terminated at a load balancer shall employ re-encryption techniques to ensure end-to-end encryption.

(3) Internet accessible Websites shall implement HTTPS Only with HTTP Strict Transport Security (HSTS), have no weak ciphers, have no weak protocols, and preload .gov domains.

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

(5) Web sites (internal and public) with authentication functions, must implement Transport Layer Security (TLS) encryption with a FIPS 140-3/140-2 validated encryption module. SSL/TLS implementation must be IAW GSA CIO-IT Security-14-69, SSL/TLS Implementation Guide.

b. Sensitive data shall not be transferred to or accessed from non GSA systems.

c. Authorization to sensitive data must occur at the point of access (Application, API, Database, File)

d. Remote access to sensitive data may occur only via GFE or through an approved GSA virtual interface (i.e., Citrix and/or VDI).

e. PII/CUI stored on network drives and/or in application databases must have proper access controls (i.e., user identification, authentication, and authorization) and shall be made available only to those individuals with a lawful government purpose.

f. The letters CUI and the CUI category shall be used as the banner marking on every page of a GSA-owned CUI basic document IAW the Controlled Unclassified Information (CUI) GSA Marking Manual and the GSA Marking CUI Information page on InSite. Documents marked CUI have limited dissemination and must only be shared in accordance with those markings.

g. Encryption is required If PII/CUI needs to be emailed outside the GSA network. Instructions can be found on the GSA CUI InSite page in the section on Emailing and Mailing CUI. An email will be blocked if Social Security Numbers are attempted to be sent unencrypted.

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. If PII/CUI needs to be sent by courier, printed, or faxed several steps should be taken when sending PII/CUI by courier mark, "signature required" must be included. PII documents must not remain on a printer where unauthorized employees or contractors can access 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/CUI only to those individuals authorized to handle it, create a paper trail, and verify information reached its destination.

j. Data must be protected against unauthorized access, tampering, alteration, loss, and destruction during production, input, output, handling, and storage. Additional guidance may be found in GSA CIO-IT Security-12-63, System and Information Integrity.

k. Data integrity and validation controls must be used on all information systems requiring a high degree of integrity.

l. Data integrity must be protected IAW GSA CIO-IT Security-12-63.

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

n. Systems containing permanent electronic records must be maintained in an electronic format IAW OMB M-23-07.

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

p. GSA provided portable storage devices (e.g., USB flash drives, SD cards, etc.) cannot be used on external systems (e.g., personal computers, other agency systems).

q. Information system media must be physically and securely stored within controlled areas.

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

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

t. 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 of.

u. Controls shall be put in place to monitor or detect changes or updates to systems 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. Contractors shall return all GSA data when they no longer provide GSA contract support and at the end of their contract.

5. 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, DISA STIG guidelines (High Severity/CAT I), Center for Internet Security guidelines (Level 1), or industry best practice guidelines, as deemed appropriate. Any GSA security benchmark published for a particular technology must be referenced to securely configure that technology. GSA security benchmark requirements must be implemented within (180) days of the benchmark's publication. 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 GSA Order CIO 2140.4 as a guide when managing security throughout the system's life cycle.

f. Cloud-based System Owners should use GSA CIO-IT Security-19-102, OCISO DevSecOps Program, to fully integrate security with development and operations teams.

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

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

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

j. Ensure 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.

k. 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.

l. 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.

m. 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.

n. 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.

o. 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.

p. 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.

q. 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.

r. 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.

s. 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.

t. Incident response plans must be developed, revised, and tested 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.

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

v. Background investigation requirements for access to GSA information systems (including contractor operations containing GSA information) shall comply with GSA Order ADM 2181.1, “Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing, and Background Investigations for Contractors.” Temporary contractors (work duration of 15 days or less) requiring access to IT systems (e.g., vendor/contractor summoned for an emergency service call) are not required to have a background investigation and require escort upon entry and while inside a GSA-controlled facility.

w. A favorable initial fitness/suitability determination must be granted, and a Tier 1 or higher background investigation initiated before access to the GSA network or any GSA IT system. There shall be no waivers to this requirement for GSA network and IT system access for GSA employees or contractors.

x. A favorable initial fitness/suitability determination must be granted, and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. 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.

y. A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the GSA network or IT systems is granted. A waiver may be requested to maintain GSA business operations; however, such requests should be used judiciously and not incur unnecessary risks to GSA.

z. If final adjudication of a background investigation is unfavorable, GSA network and IT system access must be revoked, and any GFE, including the GSA PIV card, must be retrieved and returned to OMA.

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

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

6. 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.

7. 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. All systems must, upon request, provide logs to the Secretary of Homeland Security through the Director of CISA and to the FBI, consistent with applicable law and as required by EO 14028, Section 8(e).

c. 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).

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

e. All media containing CUI must be marked IAW the CUI GSA Marking Manual and the GSA Marking CUI Information page on InSite.

f. 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.

g. Protect digital media during transport outside of controlled areas using a certified FIPS 140-3/140-2 encryption module; non-digital media shall follow GSA personnel security procedures.

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

i. 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.

j. Information systems must run with the least amount of system privilege needed to perform a specific function and support system access granted on a need-to-know basis.

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

l. 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.

m. Bluetooth is approved for use on GSA GFE. The following restrictions apply:

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

n. 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).

o. All GSA owned or managed network devices must 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.

p. If GSA systems interconnect, they must connect using a secure methodology providing security commensurate with the acceptable level of risk as defined in the System Security and Privacy Plan and limiting access only to the information needed by the other system IAW GSA CIO-IT Security-01-07 and GSA CIO-IT Security-06-30.

q. GSA CIO-IT Security-12-67 provides GSA's specific information security requirements regarding mobile devices and applications. Per CIO-IT Security-12-67, mobile devices include smartphones and tablets and excludes laptops and basic cell phones. In accordance with CIO-IT Security-12-67:

(1) All mobile applications must follow the approval process described in the guide before being added to any mobile device or being included in a system's boundary.

(2) GSA's Mobile Device Management (MDM) solution must be installed, operating, and managed by GSA on all mobile devices before they connect to any GSA resources.

(3) All mobile applications and devices must be part of a system ATO, or in the case of standalone applications, receive its own ATO.

r. 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 specific policy statements supporting outcomes for the CSF Detect categories and subcategories. Appendix A details specific Detect category and subcategory definitions and unique identifiers.

1. Integration with SecTools and Services. EO 14028 and ensuing mandates and guides require GSA to implement Zero Trust and centralize security visibility and enforcement. To comply with these government-wide requirements OCISO delivers Enterprise Security Shared Services (ES3) including Firewall, Domain Name System (DNS), Application Security, Security Operations Center (SOC), Vulnerability Disclosure Policy (VDP) and Bug Bounty Program, and Vulnerability Scanning. These best-in-class services for risk identification, threat detection, prevention, and monitoring requirements support a “One GSA, One Cyber” strategy. In support of said requirements and strategy:

a. All GSA federal systems connected to the GSA enterprise (on-prem or in the cloud) shall:

(1) Integrate into GSA’s top-level agency SOC, by implementing OCISO audit log shipping mechanisms and related configurations, endpoint security agents, and cloud security tooling.
(2) Integrate with GSA’s enterprise VDP and Bug Bounty Program, Firewall, DNS, Application Security, and Vulnerability scanning services to achieve visibility to better detect and understand threat activity.

b. GSA federal systems not directly connected to the GSA enterprise (on-prem or in the cloud) shall:

(1) Integrate into GSA’s top-level agency SOC, by implementing OCISO audit log shipping mechanisms and related configurations, endpoint security agents, and cloud security tooling.
(2) Integrate with GSA’s enterprise VDP and Bug Bounty Program and enterprise vulnerability scanning services to achieve visibility to better detect and understand threat activity.
(3) Integrate with GSA’s DNS services or as per 6 U.S.C. §663, ensure local DNS recursive resolvers use EINSTEIN 3 Accelerated (E3A) as their primary (or ultimate) upstream DNS resolver.

2. Anomalies and Events.

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

b. 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.

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

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

e. 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.

f. The determination of whether a major incident has occurred (requiring Congressional reporting) will be made by the GSA Full Response Team as defined in GSA Order CIO 9297.2C CHGE 1, Information Breach Notification Policy, 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;
(5) Representative from the Office of General Counsel;
(6) Representatives from the OSC and the Office of Congressional and Intergovernmental Affairs, for awareness and coordination purposes only, and
(7) Security Engineering Division Director or representative.

g. GSA systems and the GSA Incident Response Team will adhere to Federal Laws and requirements associated with responding to cybersecurity vulnerabilities and incidents and GSA guidance as documented in GSA CIO-IT Security-01-02.

3. Security Continuous Monitoring.

a. OCISO will implement continuous monitoring of systems using Continuous Diagnostics and Mitigation 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 in GSA CIO-IT Security-12-66 and GSA CIO-IT Security-12-67.

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 the information system, overwrite the 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. Only authorized personnel are permitted access to rooms, work areas/spaces, and facilities containing agency systems, networks, and data. A list of current authorized personnel shall be maintained and reviewed annually to verify the need for continued access and authorization credentials.

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

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

j. 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 embedded or integrated into third-party technology, is expressly prohibited.

k. 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.

l. GSA monitors mobile devices using MDM policies and rules of behavior as outlined in GSA CIO-IT Security-12-67.

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

n. 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 5 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 SSPP.

o. Contractor Information systems must follow the monitoring requirements IAW External Information System Monitoring GSA CIO-IT 19-101.

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

q. GSA SSOs shall scan for unauthorized wireless access points quarterly and take appropriate action if such an access point is discovered.

r. 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.

s. ISSO checklists in GSA's implementation of its current GRC solution will be completed by ISSOs and monitored by ISSMs to track the completion of recurring security tasks.

4. Detection Processes.

a. Systems must comply with Federal and GSA detection and monitoring requirements as specified in NIST SP 800-53, Revision 5 and IAW GSA CIO-IT Security-01-08.

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

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

d. 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

This chapter provides security policy statements for the Respond function of the CSF. 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 specific policy statements supporting outcomes for the CSF Respond categories and subcategories. 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. Users must immediately report the following to the GSA IT Service Desk:

(1) Suspected vulnerabilities, security violations, and security incidents to the GSA IT Service Desk.
(2) Lost or stolen portable storage devices; and
(3) Lost or stolen hardware, software, and/or information in physical form.

b. Users must also report:

(1) All losses to the Federal Protective Service via the appropriate Regional Hotline, as directed by the appropriate ISSO or the GSA IT Service Desk.
(2) Any loss occurring outside of Federal facilities to the local police.
(3) Lost PIV cards to the Central or Regional OMA office after reporting to the GSA IT Service Desk.

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

d. 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 CHGE 1.

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

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

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

h. 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. IAW GSA CIO-IT Security-01-02, the GSA Incident Response Team will:

(1) Investigate notifications/alerts from detection systems IAW;
(2) Determine the impact of an incident in coordination with other personnel/organization, as appropriate; and
(3) Perform forensics analysis of incidents/the evidence of incidents, as necessary.

c. IAW GSA CIO-IT Security-01-02, the GSA OCISO will:

(1) With the Incident Response Team, categorize incidents;
(2) Establish a vulnerability management process for identifying vulnerabilities via internal testing/scanning; and
(3) Notify personnel with security responsibilities of vulnerabilities disclosed via SAAs or other external sources.

d. ISSMs and ISSOs must report on the status of the SAAs 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, system vulnerabilities must be:

(1) Remediated or mitigated IAW specified timeframes;
(2) Included in a Plan of Action and Milestones; or
(3) Included in an Acceptance of Risk Letter.

d. Systems must comply with the required actions specified in DHS Cybersecurity Directives. The OCISO Security Operations Division (ISO) collaborates with system personnel regarding directives and reports status to DHS, as required.

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 impaired capabilities or services resulting from 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 specific policy statements supporting outcomes for the CSF Recover categories and subcategories. Appendix A details specific Recover category and subcategory definitions and unique identifiers.

1. Recovery Planning. As part of a system's contingency planning process, recovery plans must be 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 the 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 and repairing GSA's reputation regarding an incident.

b. 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.

Function: Identify
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
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
Function: Protect
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
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
PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations
Function: Detect
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
Function: Respond
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
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
Function: Recover
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