U.S. General Service Administration (GSA)

GSA Order: GSA Information Technology (IT) Security Policy
CIO 2100.1R
Office of the Chief Information Officer
ispcompliance@gsa.gov

Purpose:

This Order sets forth the General Services Administration's (GSA) IT Security Policy and establishes the GSA's risk-based management approach of employing management, technical, and operational controls to achieve GSA's security objectives to comply with Federal laws and regulations, Executive Orders, Office of Management and Budget (OMB) Memoranda, and Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Directives.

Background:

Public Law 113-283, "Federal Information Security Modernization Act of 2014 (FISMA)" and OMB Circular A-130, "Managing Information as a Strategic Resource" require each agency to establish an information security program, including policies and procedures that provide security for the information and information systems supporting the agency's operations and assets. This Order and GSA IT's security procedural guides and other security policies provide the procedures and processes to meet those requirements. As required in Executive Order (EO) 13800, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure", the GSA has organized this Order to reflect the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF) 2.0 core functions of Govern (GV), Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). The Govern function is covered within this Order, the other core functions are covered in the GSA Cybersecurity Handbook.

Applicability:

This Order applies to:

1. GSA Federal employees, contractors, and vendors of GSA, who manage, maintain, operate, or protect GSA systems or data;

2. Except for Section 2, paragraph 2.23, 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.

Cancellation:

This Order cancels and supersedes CIO 2100.1Q, GSA Information Technology (IT) Security Policy, dated October 16, 2024.

Summary of Changes:

This Order includes the following updates:

1. Restructured to include a GSA Cybersecurity Handbook and to align to NIST CSF 2.0 functions.
2. Updated format to comply with OAS 1832.1C, "Internal Directives Management."
3. Updated the roles and responsibilities involved in Cybersecurity within the GSA.
4. Revised, consolidated, and clarified many security requirements in both the Policy and the Handbook.
5. Updated the OCISO Divisions based on FY26 GSA IT reorganization.

Roles and Responsibilities:

The roles and responsibilities responsible for executing this Order are provided in Section 2.

Signature:

/S/ 6/16/2026

DAVID SHIVE
Chief Information Officer
Office of GSA IT

Date

Table of Contents

1. General Services Administration (GSA) Information Security Program

The Federal Information Security Modernization Act (FISMA) of 2014 establishes the requirement for agencies to develop and maintain an agency-wide information security program. This Order, the additional information provided in the GSA Cybersecurity Handbook, and processes and procedures identified in GSA's Procedural and Technical guides establish the GSA information security program.

1.1 Introduction

The purpose of this Order is to document and set forth GSA's Information Technology (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.

1.2 Objectives

The GSA's security objectives are paramount to achieving its mission and business goals. These objectives ensure the robust protection of GSA's systems, data, partners, and customers by proactively managing IT-related risks. GSA implements a comprehensive framework of management, technical, and operational security controls, aligning its cybersecurity risk management practices in accordance with (IAW) Executive Order (EO) 13800 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) and Risk Management Framework.

Security mechanisms must be well founded, configured to perform in the most effective manner, and add value to GSA's IT-related investments. Using a risk-based approach will enable the GSA to meet its IT security goals by better securing IT systems; providing management the information necessary to justify IT Security expenditures; and assisting the GSA in authorizing IT systems for operation. The GSA 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, including ensuring 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 systems and information. The system works promptly, and service is not denied to

authorized users. The system must be ready for use by authorized users to perform their duties.

d. Accountability. Accountability must be at 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 a system accurately mediates and enforces the security policy. This assurance (i.e., confidence the other security objectives have been met), is established 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 disruption. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

1.3 Federal Laws and Regulations

This Order supports 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
- 44 U.S.C. § 3555(b)(1), Annual Independent Evaluation
- 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
- NIST Cybersecurity Framework (CSF) 2.0
- EO 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- EO 14028, Improving the Nation's Cybersecurity
- Federal Information Processing Standards (FIPS) Publication (PUB) 140-3, Security Requirements for Cryptographic Modules, (Note: Although FIPS PUB 140-3 has been issued, FIPS PUB 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 PUB 199, Standards for Security Categorization of Federal Information and Information Systems
- FIPS PUB 200, Minimum Security Requirements for Federal Information and

Information Systems
- Internet of Things Cybersecurity Improvement Act of 2020 (IoT Act) (Public Law 116-207)
- Inspector General Act of 1978, (Public Law 95-452)
- NIST Special Publications (SPs), GSA implements guidance provided by the NIST 800-series SPs within a year of 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
- OMB Circular A-130, Managing Information as a Strategic Resource
- OMB Memoranda (pre-M-25-10, post-M-25-09), currently in force memoranda must be complied with based on their purpose and scope
- PCI DSS (current version), Payment Card Industry Data Security Standard
- Presidential Policy Directive (PPD-21), Critical Infrastructure Security and Resilience
- Privacy Act of 1974 (5 U.S.C. § 552a)

1.4 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 2181.1A, 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 5400.1A, Meetings with Representatives of Foreign Governments or Foreign Industry, Foreign Travel, and Foreign Contact
- GSA Order ADM 7800.11A, Personal Use of Agency Office Equipment
- GSA Order ADM 9732.1E, Personnel Security and Suitability Program Handbook
- GSA Order CIO 1820.2A, 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 2103.2, Controlled Unclassified Information (CUI) Policy
- GSA Order CIO 2104.1C, GSA Information Technology (IT) General Rules of Behavior
- GSA Order CIO 2101.3, GSA Integrated Information Technology Management
- GSA Order CIO 2135.2D, GSA Policy for Information Technology (IT) Capital Planning and Investment Control (CPIC)
- GSA Order CIO 2160.2B CHGE 4, GSA Electronic Messaging and Related Services
- GSA Order CIO 2165.2C, CHGE 1, GSA Telecommunications Policy

- 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 2185.1C, Accelerating Responsible Use of Artificial Intelligence at GSA
- GSA Order CIO 2200.1, GSA Privacy Act Program
- GSA Order CIO 9297.2C CHGE 1, GSA Information Breach Notification Policy
- GSA Order HRM 9751.1A, Maintaining Discipline
- GSA Order OSC 2106.2A, GSA Social Media Policy
- GSA CIO-IT Security Procedural Guides and Technical Guides and Standards

1.5 Compliance and Deviations

a. Compliance is mandatory immediately upon the signing of this Order. All GSA Service and Staff Offices (SSOs), 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 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. 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, Authorization to Operate [ATO] expiration) will have their time extended.

c. Deviations, exceptions, or other conditions not following GSA IT Security policies and standards must be submitted using the Office of the Chief Information Security Officer (OCISO's) Security Deviation Request Form. Deviations and exceptions are managed and tracked using Plan of Action & Milestones (POA&Ms), Acceptance of Risk (AOR) Letters, and Memoranda for Record (MFRs) as defined in GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk.

   (1) System specific policy exceptions upon approval, must be documented in the System's Security Plan (SSP).

   (2) Configuration deviations must follow the instructions for requesting deviations as defined in GSA's IT Security Technical and Standards guides.

1.6 Definitions

For the purposes of this Order the following terms are defined as listed. Additional definitions are provided in the GSA Cybersecurity Handbook, as appropriate.

a. Federal Information System. An information system used or operated by an agency or by a contractor of an agency or by another organization on behalf of an agency.

b. GSA System Designations. For FISMA reporting purposes, GSA designates Federal Information Systems based on the definitions below.

(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.

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

d. Personally Identifiable Information (PII). 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.

1.7 Conflicts

All systems and personnel as identified in Applicability must adhere to NIST SPs , Federal Information Processing Standards Publication (FIPS PUB), and 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 (ISA) at ispcompliance@gsa.gov for clarification.

1.8 GSA System ATOs

All GSA systems must achieve an ATO before being placed into production. 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) based on an Assessment and Authorization (A&A) process defined in GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk.

1.9 Contractor Operations

The appropriate security requirements of this Order must be included in task orders and contracts for all systems designed, developed, implemented, maintained, and operated by a contractor on behalf of GSA, including but not limited to systems operating in a Cloud Computing environment. Note: As indicated Section 1.5, GSA has a deviation

request process by which a deviation from approved security architecture/standards may be requested.

1.10 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 credentials to a cloud service, platform, application, or tool without first consulting with the OCISO's Security Operations & Engineering Division (ISB) Division. Such coordination can be made by contacting ISB representatives at SecEng@gsa.gov. PII or other sensitive data cannot be used in any pilot.

a. No procurement for such products/services shall be completed without coordination through the OCISO and having obtained a valid FedRAMP ATO or an ATO granted by a GSA Authorizating Official (AO) based on the processes defined in GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk.

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

1.11 Zero Trust

The GSA's Zero Trust Strategy Implementation Plan aligns with EO 14028, OMB M-22-09, the Zero Trust Architecture (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. The GSA plan 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.

1.12 Integration with SecTools and Services

EO 14028 and ensuing mandates and guides require the 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:

i. 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.

ii. 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.

1.13 Artificial Intelligence

Artificial intelligence (AI) technologies and platforms may only be procured, used, assessed, and monitored at GSA in accordance with GSA Order CIO 2185.1C, "Accelerating Responsible Use of Artificial Intelligence at GSA." Use of AI in GSA production environments must be approved IAW GSA CIO-IT Security-25-140: Artificial Intelligence (AI) Services Integration Security.

1.14 GSA Cybersecurity Handbook

The GSA Cybersecurity Handbook for GSA Order CIO 2100.1R, "GSA IT Security Policy" provides additional information on security requirements designed to supplement this Order.

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. Detailed responsibilities for the roles in this section are provided in the GSA Cybersecurity Handbook and GSA IT Security Procedural guides. Additional roles and responsibilities are included in the Handbook and procedural guides as necessary.

2.1 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 (i.e., GSA Administrator). The FISMA assigns the agency head the responsibility for providing information security protections for systems and information commensurate with the risk to them, and 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 agency.

2.2 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 Chief Information Officer (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.

2.3 Chief Information Officer (CIO)

The Clinger-Cohen Act of 1996 established the role of the CIO and the FISMA established the CIO as having overall responsibility for developing and maintaining an agencywide information security program. The CIO reports to the GSA Deputy Administrator and is responsible for providing guidance, assistance, and support to the Heads of Services and Staff Offices (HSSOs), and Regional Administrators on implementing GSA's IT Security Policy.

2.4 Chief Financial Officer (CFO)

The CFO ensures financial systems comply with statutory requirements, including the Chief Financial Officers Act of 1990, Clinger-Cohen Act of 1996, FMFIA and FFMIA. The CFO, in coordination with the CIO, supports the GSA IT Capital Planning and Investment Control (CPIC) process, complying with legislative and OMB requirements, and ensuring GSA's financial systems comply with Federal and GSA security requirements.

2.5 Senior Agency Official for Privacy (SAOP)

The SAOP oversees GSA's Privacy Program IAW the Privacy Act of 1974, GSA Order CIO 2200.1, "GSA Privacy Act Program," OMB A-130, OMB M-16-24 and the privacy control baseline in NIST SP 800-53. The SAOP ensures privacy risks are addressed in system authorizations, reviews systems handling PII for compliance and approves their Certification Letters and Privacy Impact Assessments (PIAs), directs privacy training, and incident response activities when PII is breached.

2.6 Senior Agency Official (SAO) for CUI

The SAO for CUI is responsible for overseeing GSA's CUI Program. The SAOP is GSA's Senior Agency Official for CUI.

2.7 Chief AI Officer (CAIO)

The CAIO oversees governance and risk management of AI technologies across GSA IAW GSA Order CIO 2185.1C, Federal requirements, and OMB guidance. The CAIO coordinates with AOs, the OCISO, and System Owners to assess risks and integrate AI into GSA's broader cybersecurity and enterprise risk management framework. The CAIO's full responsibilities are identified in GSA Order CIO 2185.1C.

2.8 Chief Data Officer (CDO)

The CDO enables data-driven decision-making in a variety of ways, from providing and leveraging centralized agency analytics capacity to creating tools and platforms that enable self-service across their agencies and for the public. CDOs serve in a central leadership position, with visibility into relevant agency operations, and are positioned high enough to regularly engage with other agency leaders.

2.9 Chief Information Security Officer (CISO)

The FISMA establishes the designation of a Senior Agency Information Security Officer by the CIO. GSA has assigned that responsibility to the CISO. The CISO is responsible for leading GSA's information security program and serves as the senior official accountable for managing cybersecurity risk across the GSA. The CISO reports to the GSA CIO on the implementation and maintenance of GSA's information security program including security policies, procedural and technical guides, and compliance with the security requirements established in this Order.

2.10 Heads of Services and Staff Offices (HSSOs)

HSSOs are senior officials or executives with specific mission or line of business responsibilities. They are responsible for ensuring GSA systems and personnel within their service or staff office comply with GSA security requirements.

2.11 Chief Privacy Officer (CPO)

The CPO is responsible for managing GSA's Privacy Program and administers GSA's compliance with privacy laws and regulations. The CPO, through the Privacy Program, is responsible for preserving and enhancing privacy protections for all individuals whose personal information is handled by GSA and its systems. The CPO reports to the SAOP.

2.12 Authorizing Official (AO)

An AO must be a Federal employee and is the management official with the responsibility of determining if an acceptable level of risk for a system, application, or set of common controls has been achieved. Final authority to operate or not operate an information system, application, or a set of common controls rests with the AO. Each system, application, or set of common controls must have an assigned AO.

2.13 System Owners (SO)

SOs are GSA management officials with responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's systems. System Owners are accountable for systems throughout their lifecycle. System Owners collaborate with ISSOs, ISSMs, and AOs to assess risk, maintain security documentation, and address vulnerabilities. SOs cannot be ISSOs or ISSMs.

2.14 Office of CISO Division Directors

The OCISO Directors serve as an intermediary to the AO for ensuring security is implemented. The OCISO Directors oversee IT system security for assigned resources, manage implementation of the GSA IT Security Program, and guide compliance efforts. The Division Directors report to the CISO. The OCISO Division responsibilities are summarized below.

- Security Risk & Compliance Division (ISA) - Manages enterprise cybersecurity risk and compliance programs including Identity, Credential, and Access Management (ICAM) systems and policies. Develops and implements cyber security policies, conducts FISMA audit activities and compliance oversight, and administers Cyber Supply Chain Risk Management (C-SCRM) program to ensure GSA maintains appropriate security posture and regulatory compliance across all information systems and operations.
- Security Operations & Engineering Division (ISB) - Operates the Security Operations Center (SOC) and provides comprehensive cybersecurity engineering services including application security (AppSec) programs, cyber engineering and architecture design, and Continuous Diagnostics and Mitigation (CDM) implementation. Responsible for real-time security monitoring, threat detection and response, security architecture development, and automated security tools deployment to protect GSA’s information systems and data assets.
- ISSO Support Division (ISC) - Manages technology system authorizations and provides support services for ISSOs and ISSMs. Operates enterprise Governance, Risk, and Compliance (eGRC) platforms and processes to ensure proper security authorization, risk management, and compliance oversight for GSA’s information systems throughout their lifecycle.

2.15 Information System Security Manager (ISSM)

ISSMs must be Federal employees. ISSMs provide coordination between System Owners and OCISO leadership to manage system-level cybersecurity risk. The ISSM supports the integration of IT security into programs and compliance with security and privacy requirements, and oversees system-specific risk management activities. An individual appointed as ISSM for a system cannot also be assigned as the ISSO for the same system. ISSMs report to the ISC Director.

2.16 Information System Security Officer (ISSO)

ISSOs may be Federal employees or contractors. ISSOs support and provide guidance to System Owners and their teams regarding required security controls, assessing risks, and continuous monitoring of their systems. ISSOs coordinate with the OCISO and System Owner to shepherd a system through its authorization process, maintain its security posture, including recurring assessments and managing POA&Ms, through disposal of the system. An ISSO must be assigned for every information system and must be knowledgeable of the information and processes supported by the system. An individual assigned as the ISSO cannot also be the ISSM or System Owner for the same system. ISSOs report to an ISSM.

2.17 Privacy Analyst

Privacy Analysts are responsible for ensuring the implementation of adequate privacy for systems in order to mitigate and minimize the privacy risks associated with collecting, using, processing, storing, maintaining, and disseminating PII. A Privacy Analyst must be assigned to every information system that contains PII and may have responsibility for more than one system.

2.18 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 the 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. Specific responsibilities for this role are delegated by the System Owner.

2.19 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. Specific responsibilities for this role are delegated by the System Owner.

2.20 Data Owners

Data Owners/Functional Business Line Managers own the information but not the system, application, or platform on which the information is stored, transmitted, or processed. Data Owners are responsible for ensuring data is properly stored, maintained, protected, and monitored based on Federal laws and regulations and GSA policies and guidance. Data Owners are responsible for coordinating with System Owners, ISSMs, ISSOs, and Custodians to ensure they are aware of the type and sensitivity of data (e.g., Personally Identifiable Information, Controlled Unclassified Information) in their systems and implement the proper security controls and measures to protect the data.

2.21 Data Steward

Data Stewards maintain the completeness, accuracy, security, and validity of the data within their domain, both at an individual and aggregate level. Data Stewards serve as a functional subject matter expert (SME) and a custodian for one or more of the organization's enterprise data assets.

2.22 Domain Steward

A data governance professional responsible for the operational oversight, quality, and definition of a specific subject area of data. They act as subject matter experts who define data standards, enforce policies, and ensure data integrity across business functions.

2.23 Contracting Officer (CO) and CO Representative (COR)

COs/CORs are responsible for coordinating and collaborating with the CISO and other appropriate officials to ensure all agency contracts and procurements are compliant with the agency's information security and privacy policies. They also must ensure the appropriate security and privacy contracting language is incorporated in each contract. The CO/COR function is responsible for managing contracts and overseeing their implementation. CO/CORs must be Federal employees.

2.24 Custodians

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

2.25 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.

2.26 Office of Inspector General (OIG)

The GSA OIG is an independent statutory office, established by the Inspector General Act of 1978, responsible for performing: independent financial, program, information technology, contract and compliance audits (e.g., FISMA audits); criminal and civil investigations; reviews of proposed legislation and regulations; and other services to senior GSA, Congressional, and law enforcement officials.

2.27 Personnel Security Officer, Office of Mission Assurance (OMA)

The GSA personnel security officer is responsible for the overall implementation and management of personnel security controls across GSA, to include integration with specific information security controls.

2.28 Office of Human Resources Management (OHRM)

The Human Resource Office and Security Office are responsible for designating the risk levels for all positions in the GSA and incorporating the risk level in the position designation(s) for each series and grade.

2.29 System/Network Administrators

System/network administrators are responsible for implementing and maintaining the technical security of GSA systems and networks. These roles work with the custodian/ISSO to ensure appropriate technical security requirements are implemented.

2.30 Supervisors

Supervisors are responsible for managing personnel to ensure security requirements are met and access to systems are compliant with GSA security policies and standards.

2.31 OCISO DevSecOps Program (ODP) Security Engineer

ODP Security Engineers are responsible for the security design, operational security, application security (AppSec), security and compliance impact analysis during change management, and security/compliance automation of systems.

3. Policy for Govern

This section identifies how the GSA's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored in accordance with the CSF 2.0 Govern Function.

3.1 Organizational Context

This section provides an understanding of GSA's mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements regarding cybersecurity risk management.

a. GSA's mission is to deliver the best customer experience and value in real estate, acquisition, and technology services to the government and the American people.

b. The Enterprise Risk and Strategic Initiatives (ERSI) Board is responsible for identifying and addressing complex, interconnected, and distributed risks to mission delivery. It translates enterprise-level strategies into actionable initiatives and the implementation of sound risk management principles across GSA functions and programs.

c. For cybersecurity risks, the CISO, AOs, ISSMs/ISSOs, and other OCISO personnel facilitate the consistent application of cybersecurity risk management across GSA. The processes and procedures for managing cybersecurity risk at the GSA are managed and guided by:

(1) GSA CIO-IT Security-18-91: Risk Management Strategy (RMS);
(2) GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk;
(3) GSA CIO-IT Security-08-39: FYxx IT Security Program Management Implementation Plan (MIP);
(4) GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program; and
(5) GSA's other IT Security Procedural and Technical guides.

d. Internal stakeholders consist of any of the categories of personnel who are identified in the Applicability Section of this policy. Chapter 2, Roles and Responsibilities, contains general expectations for roles with cybersecurity responsibilities with more detailed expectations in the GSA Cybersecurity Handbook and GSA's other IT Security Procedural and Technical guides.

e. External stakeholders consist of personnel from other Agencies and personnel who support those Agencies, contractor staff who do not have a GSA.gov account but support external systems supporting GSA, and the public. Expectations for external personnel are identified in the GSA Cybersecurity Handbook and GSA's other IT Security Procedural and Technical guides, where appropriate.

f. Section 1.3 identifies the laws, orders, directives, regulations, policies, standards, guidelines, and commercial standards that this Order and the GSA Cybersecurity Handbook address. GSA's other IT Security Procedural guides include the laws, orders, directives, regulations, policies, standards, guidelines, and commercial standards requirements appropriate for them.

g. Section 1.4 identifies GSA's policies and guidance (i.e., IT Security Procedural and Technical guides) which cover contractual and privacy/civil liberties requirements. Specifically, GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts provides requirements to be included in contracts.

h. The OCISO manages the preparation of Agency-wide FISMA reports and coordinates their submission to OMB (quarterly) and congressional committees (annually) IAW GSA CIO-IT Security-04-26: Federal Information Security Modernization Act (FISMA) Implementation Process.

i. GSA Order ADM 2430.2A, "The U.S. General Services Administration Continuity of Operations Mission Essential Functions," directs organizations in the U.S. General Services Administration (GSA) on how to provide essential services (e.g., Mission Essential Functions [MEFs] and Essential Supporting Activities [ESAs]) to GSA employees, other Federal Executive Branch Departments and Agencies, and the public in the event of an emergency event.

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

k. The outcomes, capabilities, and services the GSA depends upon are addressed in:

   (1) GSA Order ADM 2430.2A, "The U.S. General Services Administration Continuity of Operations Mission Essential Functions;"
   (2) GSA Order OMA 2430.2B, "GSA National Continuity Plan;" and
   (3) GSA Order OMA 2430.3A, "The U.S. General Services Administration Emergency Management Program."

l. The GSA's High Value Assets have contingency plans addressing how the services and capabilities they provide which the GSA depends upon will be provided during contingency operations.

3.2 Risk Management Strategy

This section identifies how the GSA's cybersecurity risk management strategy supports operational risk decisions and addresses risk tolerance, assumptions, and priorities. Risk management processes are communicated by the publishing of the guides listed to the GSA's internal web pages and the meetings and decisions described in the guides.

a. GSA's Enterprise Risk and Strategic Initiatives (ERSI) Board identifies and monitors agency-wide risks and leads strategic initiatives to mitigate the risks and solve cross-cutting challenges. It is responsible for identifying, vetting, and

prioritizing the most significant enterprise risks to GSA's mission, and coordinating with risk owners on mitigating and resolving those risks.

b. GSA CIO-IT Security-18-91: Risk Management Strategy (RMS), describes GSA's overall framework for managing cybersecurity risk including roles and responsibilities, risk assumptions, risk tolerance, risk response, and communicating and sharing of risk results.

c. The following guides describe risk management at the system and program levels based on A&A processes, monitoring risks using automated tools and manual processes, communicating risks via system reviews and reports, and following standardized methods for determining, prioritizing, and categorizing risks.

(1) GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk;
(2) GSA CIO-IT Security-08-39: FYxx IT Security Program Management Implementation Plan (MIP);
(3) GSA CIO-IT Security-09-44: Plan of Action and Milestones (POA&M); and
(4) GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program.

d. Supply Chain Risk Management at the GSA, including third party risk, is managed via the processes and procedures described in the following guides.

(1) GSA CIO-IT Security-21-117: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program; and
(2) GSA CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls.

3.3 Roles, Responsibilities, and Authorities

This section identifies how the GSA has established roles and responsibilities and the authorities necessary to have accountability, analyze the effectiveness of processes and procedures, and apply improvements based on this analysis regarding cybersecurity risk. The roles and responsibilities are communicated by the publishing of this Order and guides the GSA's internal web pages and designation letters for specific roles as necessary.

a. The roles, responsibilities, and authorities, including leadership, throughout the GSA and the processes and procedures used to manage, communicate, monitor, and improve cybersecurity risk management across the enterprise are defined in:

(1) Section 2 of this Order;
(2) Section 4 of the GSA Cybersecurity Handbook;
(3) GSA's CIO-IT Security Procedural Guides; and
(4) GSA's Technical Guides and Standards

b. Cybersecurity risks, including resources, are considered by the ERSI and EMB and, as necessary, included in the following strategic plans and initiatives:

(1) GSA Order CIO 2135.2D, “GSA Policy for Information Technology (IT) Capital Planning and Investment Control (CPIC),” for capital planning, investment, and evaluation of IT investments over their life cycles.
(2) Human Capital Accountability Planning as described in GSA’s Five-Year Strategic Plan and OHRM’s annual Strategic Initiatives.

c. Per GSA Order CIO 2135.2D, “GSA Policy for IT Capital Planning and Investment Control,” HSSOs, System Owners, and designated Program Managers, and Project Managers must integrate and explicitly identify funding for information systems and programs into IT investment and budgeting plans and evaluate the investments over their lifecycles.

d. Cybersecurity for GSA’s human resources are established as part of personnel position descriptions and their required knowledge, skills, and abilities, personnel security requirements and processes and procedures in:

(1) GSA Order ADM 9732.1E, “Personnel Security and Suitability Program Handbook;”
(2) GSA Order ADM 2181.1A, “Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing, and Background Investigations for Contractors;”
(3) GSA CIO-IT Security-03-23: Termination and Transfer; and
(4) GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC).

3.4 Policy

This section identifies how this Order and GSA’s procedural guides establish security policy, communicate it, and enforce it for the GSA and its systems.

a. The policies and processes for managing cybersecurity risk at the GSA are established, managed, and guided by this Order and enforced through processes within the following guides. The policies and guides are communicated by publishing them on GSA’s internal infrastructure and providing quarterly emails regarding updates.

(1) GSA CIO-IT Security-18-91: Risk Management Strategy (RMS);
(2) GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk;
(3) GSA CIO-IT Security-09-44: Plan of Action and Milestones (POA&M);
(4) GSA CIO-IT Security-08-39: FYxx IT Security Program Management Implementation Plan (MIP);
(5) GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program; and
(6) GSA’s other IT Security Procedural and Technical guides.

b. The GSA Office of the Chief Information Security Officer (OCISO) reviews this Order annually and revises it at least every 3 years to reflect changes in Federal laws and

regulations and requirements, address new threats and missions, and adapt to new technologies.

3.5 Oversight

This section identifies how the GSA's organizational cybersecurity risk management activities and performance are used to inform, improve, and revise its risk management strategy.

a. GSA CIO-IT Security-18-91: Risk Management Strategy (RMS) describes GSA's overall framework for managing cybersecurity risk including activities that provide feedback on managing risk and inform risk management decisions. The following guides describe risk management at the system and program levels including determining, categorizing, prioritizing, monitoring, and communicating risks. GSA's IT Security Procedural Guides are reviewed and updated to adjust for changing conditions as needed, and no longer than every 3 years.

   (1) GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk;
   (2) GSA CIO-IT Security-08-39: IT Security Program Management Implementation Plan (MIP);
   (3) GSA CIO-IT Security-09-44: Plan of Action and Milestones (POA&M); and
   (4) GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program.

b. In addition to the guides identified above, GSA's ERSI Board identifies and monitors agency-wide risks and leads strategic initiatives to mitigate the risks and solve cross-cutting challenges. It also monitors effectiveness of risk mitigation strategies and performance improvement activities to guide adjustments to GSA's overall cybersecurity risk management processes.

c. The OCISO conducts compliance reviews to determine how well risks are managed and performance measures and goals are being met IAW:

   (1) GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk;
   (2) GSA CIO-IT Security-08-39: FYxx IT Security Program Management Implementation Plan (MIP);
   (3) GSA CIO-IT Security-09-44: Plan of Action and Milestones (POA&M);
   (4) GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program; and
   (5) GSA CIO-IT Security-18-91: Risk Management Strategy (RMS).

3.6 Cybersecurity Supply Chain Risk Management

This section identifies how the GSA's C-SCRM processes have been established, and are managed, monitored, and improved in accordance with the CSF 2.0 Govern Function. Additional information is provided on the GSA's internal C-SCRM Policies, Regulations, and Laws web page.

a. The following documents establish the GSA's C-SCRM strategy, program, policy, processes, and define supply chain roles and responsibilities. They are communicated by publishing them to internal and external websites. A quarterly email of updated security documents is distributed when they have been updated.

(1) This Order;
(2) GSA CIO-IT Security-21-117: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program; and
(3) GSA CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls.

b. The following documents identify how C-SCRM is integrated into overall cybersecurity and enterprise risk management and how suppliers are identified and prioritized.

(1) GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC);
(2) GSA CIO-IT Security-21-117: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program; and
(3) GSA CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls.

c. The following documents establish the GSA's roles, responsibilities, and processes for C-SCRM requirements and reducing risks before entering into contracts or relationships with suppliers or third parties.

(1) GSA CIO-IT Security-21-117: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program;
(2) GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisitions; and
(3) General Services Acquisition Manual.

d. The following guides describe the GSA's processes and procedures for assessing, responding to, and monitoring C-SCRM risks through their lifecycle including post contract or agreement. These guides also describe requirements for anti-counterfeit procedures, incident notification, response, and recovery regarding suppliers and third parties.

(1) GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC);
(2) GSA CIO-IT Security-21-117: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program; and
(3) GSA CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls.

Office of the Chief Information Officer GSA Cybersecurity Handbook

for

GSA Order CIO 2100.1R GSA IT Security Policy

June 16, 2026

Table of Contents

1. Introduction

Chief Information Officer (CIO) Order 2100.1R and this companion handbook establish GSA's IT Security Policy for supporting compliance with Federal laws and regulations, Executive Orders, Office of Management and Budget (OMB) Memoranda, and Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Directives. Together they establish requirements for the protection of GSA's IT resources. GSA's Procedural and Technical guides further specify National Institute of Standards and Technology (NIST) controls, requirements, and implementation guidance on securing GSA's systems. The Order and Handbook apply to all GSA systems as defined in Section 1.6 of the Order.

The remainder of this Handbook provides additional definitions, roles and responsibilities, and security requirements for the Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC) functions of NIST CSF 2.0. The Govern (GV) function is addressed in the GSA IT Security Policy.

2. References

References are listed in the GSA IT Security Policy.

3. Definitions

For the purposes of this Handbook 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. 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).

j. 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.

k. 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 OMB Circular A-11, Capital Programming Guide.

l. Major IT Investment. An investment requiring special management attention as defined in OMB guidance and agency policies or a major acquisition as defined as defined in Section 55 of OMB Circular A-11, Capital Programming Guide, including investments designated as high risk by the CIO, involves a Tier 1 High Value Asset, or has a high-visibility profile with agency executive leadership, congressional leadership, and/or the public.

m. Minor Applications (Non-major Information Systems). Systems/applications that may be combined as subsystems of a larger 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, information security needs, and reside in the same general operating environment(s).

n. 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.).

o. 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.

p. 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).

4. Security Roles and Responsibilities

The following sections identify detailed responsibilities for the roles listed. Additional roles and responsibilities are included in individual procedural guides as necessary.

4.1 Administrator

The Federal Information Security Modernization Act (FISMA) of 2014 assigns the Administrator (i.e., agency head) the following specific information security responsibilities:

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.

4.2 Risk Executive (Function)

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 receive the needed visibility and is elevated to appropriate decision-making authorities.

4.3 Chief Information Officer (CIO)

The CIO has the following security responsibilities:

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 SSOs (HSSOs), and Regional Administrators on implementing GSA's IT Security Policy;

d. Providing management processes to enable Authorizing Officials (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 Associate CIOs of SSOs 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 in accordance with (IAW) GSA Order HRM 9751.1B.

h. Designating a Chief Information Security Officer (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-21);

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 Assessments (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, "GSA Information Breach Notification Policy," 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 Enterprise Management Board (EMB) and coordinating with the CISO to identify cybersecurity risks for consideration by the EMB.

4.4 Chief Financial Officer (CFO)

The CFO has the following security responsibilities:

a. Supporting GSA Order CIO 2135.2D, "GSA Policy for Information Technology (IT) Capital Planning and Investment Control (CPIC)." 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;

b. 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 all contracted GSA financial systems. This includes but is not limited to documentation review of operational processes and reviews monitoring Statements on Standards for Attestation Engagements (SSAE) 18 reporting submissions.

c. Ensuring GSA's financial systems have a current Authorization to Operate (ATO).

4.5 Senior Agency Official for Privacy (SAOP)

The SAOP has the following security responsibilities:

a. Ensuring GSA information systems that contain Personally Identifiable Information (PII) address the privacy controls in NIST SP 800-53, Revision 5 as part of the system's A&A, as appropriate;

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

c. Reviewing and approving Certification Letters and PIAs for systems collecting, maintaining, or disseminating PII;

d. Overseeing privacy control assessments as part of the 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. Ensuring PTAs, SORNs, and PIAs are conducted for information systems and collections and ensuring annual SAOP reports are submitted to OMB;

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

h. 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

i. Participating as the GSA Full Response Team leader IAW GSA Order CIO 9297.2C CHGE 1, "GSA Information Breach Notification Policy" if a major incident involving privacy has occurred.

4.6 Senior Agency Official (SAO) for Controlled Unclassified Information (CUI)

The SAO for CUI has the following security responsibilities:

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 National Archives and Records Administration (NARA).

4.7 Chief Artificial Intelligence (AI) Officer (CAIO)

The CAIO's full responsibilities are identified in GSA Order CIO 2185.1C, "Accelerating Responsible Use of Artificial Intelligence at GSA." Responsibilities related to information security include:

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

b. Establishing, maintaining, and chairing AI oversight governing bodies;

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

d. Issuing 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. Establishing, and maintaining over time, criteria for categories of individual applications of AI that do not require disposition through the AI Governance Board or AI Safety Team.

4.8 Chief Data Officer (CDO)

The CDO's responsibilities related to information security include:

a. Managing data at every stage of the data lifecycle by establishing effective procedures, standards, and controls to ensure quality, accuracy, access, and protection of data;

b. Managing data assets of the agency; and

c. Maximizing the use of data in the agency.

4.9 Chief Information Security Officer (CISO)

The CISO has the following security responsibilities:

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

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

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

d. Reporting to agency senior management on policy compliance;

e. 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;

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

g. 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;

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

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

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

k. 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;

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

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

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

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

p. Ensuring IT acquisitions align with GSA information security requirements;

q. Participating as the GSA Full Response Team leader, IAW GSA Order CIO 9297.2C CHGE 1, "GSA Information Breach Notification Policy" if a major non-privacy incident has occurred;

r. Concurring/non-concurring on ATOs as specified in GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk, and its related A&A procedural guides;

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

t. Coordinating with AOs and experts within the Office of the CISO (OCISO) to apply consistent management of cybersecurity risks across GSA;

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

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

4.10 Heads of Services and Staff Offices (HSSOs)

HSSOs have the following security responsibilities:

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.

4.11 Chief Privacy Officer (CPO)

The CPO has the following security responsibilities:

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. Reviewing and approving PTAs, SORNs, and PIAs for information systems and collections and coordinating submission of all annual SAOP reports to OMB;

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

d. Participating as a member of the GSA Full Response Team IAW GSA Order CIO 9297.2C CHGE 1, “GSA Information Breach Notification Policy.”

4.12 Authorizing Official (AO)

The AO has the following security responsibilities:

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, exceptions, or other conditions not adhering to GSA policies and standards as described in Section 5.2.f;

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 Section 5.1.g;

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 must be resolved and/or tracked in the systems' POA&M's IAW GSA CIO-IT Security-09-44: Plan of Action and Milestones (POA&M) and GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk;

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) for systems under their purview be maintained, including systems managed by other Federal agencies or outside organizations for GSA. 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 Privacy Act Program", GSA Order CIO 1878.3A, "Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices" 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, "GSA Information Breach Notification Policy;"

m. Ensuring contingency plans are developed and tested annually IAW OMB Circular A-130, NIST SP 800-34, Revision 1, 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 Office of Inspector General (OIG) as described in Section 4.24;

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 Payment Card Industry Data Security Standard (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 Section 5.1.a (e.g., systems, critical software, High Value Assets [HVA]).

4.13 System Owners (SO)

System Owners have the following security responsibilities:

a. Provides authorization for assigning a group, role, service, or device identifiers (or by an individual with delegated SO area of responsibility).

b. Ensuring systems and the data they process 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;

c. Creating and maintaining System Security Plans (SSPs), ensuring that the system is deployed and operated according to the agreed-upon security requirements; and obtaining a written ATO following GSA A&A processes prior to making production systems operational and/or Internet accessible;

d. Obtaining the resources, including personnel, necessary to securely implement and manage their respective systems;

e. 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;

f. 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;

g. Coordinating with the OCISO, ISSM, and ISSO to maintain accurate inventories as identified in Section 5.1.a (e.g., systems, critical software, HVA);

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

i. Coordinating with Contracting Officers/Contracting Officer Representatives (CO/CORs) to ensure new solicitations for GSA IT systems include the security contract language from GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts;

j. 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;

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

l. Ensuring information and system categorization has been established for their systems and data IAW Federal Information Processing Standard (FIPS) Publication 199 (FIPS Pub 199), “Standards for Security Categorization of Federal Information and Information Systems;”

m. 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 800-63-4, “Digital Identity Guidelines;”

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

o. 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;

p. 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;

q. Defining, implementing, and enforcing detailed separation of duties to ensure

   - single individuals do not have control of the entirety of a critical process, roles, permissions, and/or responsibilities; and
   - proper separation of duties spanning GSA IT system maintenance, management, and development processes;

r. 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;

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

t. Complying with GSA security awareness training requirements for individuals with significant security responsibilities, and identifying if their personnel need additional training and ensuring they complete any assigned training;

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

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

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

x. 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-26-14 active and cold data storage time frames;

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

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

aa. Complying with the security requirements of the PCI DSS for systems and networks which are in-scope of the PCI DSS assessment annually and when significant changes are made to the system and network;

bb. 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;

cc. Participating as a member of the GSA Full Response Team as defined in GSA Order 9297.2C CHGE 1, "GSA Information Breach Notification Policy" to determine if a major incident has occurred; and

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

ee. Ensuring GSA data assets go through media protection processes IAW GSA CIO-IT Security-06-32: Media Protection (MP), prior to reuse or leaving GSA's control.

4.14 Office of CISO Division Directors

The Office of CISO Division Directors have the following security responsibilities:

a. Monitoring adherence and proper implementation of the GSA 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 data collection and reporting the status for 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 ongoing 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 (ISB Division Director) as defined in GSA Order 9297.2C CHGE 1, "GSA Information Breach Notification Policy," to determine if a major incident has occurred. The ISB 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, the Department of Homeland Security (DHS), or other Federal authorities information regarding cybersecurity (e.g., CISA directives, the Cybersecurity Coordination, Assessment, and Response Protocol [C-CAR], critical software).

4.15 Information System Security Manager (ISSM)

Responsibilities of the ISSM include, but are not limited to:

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 the appropriate A&A documentation is developed, processed, and maintained for the life of the system IAW GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk, including the usage of GSA's Governance, Risk, and Compliance (GRC) solution;

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

e. Reviewing and coordinating the reporting of IT security program elements, as required (e.g., alerts, incidents, vulnerabilities, data calls, etc.);

f. Managing system assessments IAW with the system's A&A process and any required third-party audits or assessments (e.g., 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. Coordinating with CO/CORs to ensure new solicitations for GSA IT systems include the security contract language from GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts; and

h. Complying with GSA security awareness training requirements for individuals with significant security responsibilities, and identifying if their personnel need additional training and ensuring they complete any assigned training.

4.16 Information System Security Officer (ISSO)

Responsibilities of the ISSO include, but are not limited to:

a. Ensuring the system is operated, used, maintained, and disposed of IAW documented IT Security policies and procedures;

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: Managing Enterprise Cybersecurity Risk, including the usage of GSA's GRC solution;

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

e. Assisting the AO, data owner, and CO/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. Identifying, reporting, and responding to information security incidents in coordination with GSA's incident responders, including beginning protective and corrective measures as directed;

g. 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 and separation of duties;

h. Verifying systems not integrated with the GSA Enterprise Logging Platform (ELP)/audit logging tool perform audit reviews to identify potential security issues IAW GSA IT Security-01-08: Audit and Accountability (AU);

i. Evaluating cybersecurity alerts, advisories, directives and known vulnerabilities to ascertain if additional safeguards are needed and ensuring systems are patched and securely configured, as appropriate;

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

k. Assisting the System Owner 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;

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

m. 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.

4.17 Privacy Analyst

Privacy Analysts have the following security responsibilities:

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

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

c. Approving the SSP;

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.

4.18 Data Owners

Data Owners (a.k.a. Business Line POC) have the following security responsibilities:

a. Determining the security categorization of systems based upon the FIPS Pub 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 GSA Order CIO 1820.2A, “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. Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of system and data security requirements;

i. 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-26-14 active and cold data storage time frames;

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

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

l. Identifying the data assets to catalog in GSA’s Data Inventory and for possible public release; and

m. 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.

n. Ensuring GSA data assets go through media protection processes IAW GSA CIO-IT Security-06-32: Media Protection (MP), prior to reuse or leaving GSA's control.

4.19 Contracting Officer (CO) and CO Representative (COR)

COs/CORs have the following information security responsibilities:

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

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

c. 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);

d. Ensuring contracts and task orders for ISSM and ISSO services include measurable performance requirements;

e. 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; and

f. Ensuring new solicitations for all GSA IT systems include the security contract language from GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts.

4.20 Custodians

Custodians have the following security responsibilities:

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.

4.21 Authorized Users of IT Resources

Authorized users of IT resources have the following security responsibilities:

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, or locking and removing their Personal Identity Verification (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 Virtual Desktop Infrastructure [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.

4.22 Office of Inspector General (OIG)

In addition to other responsibilities, the OIG 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 with 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.

4.23 Personnel Security Officer, OMA

The Personnel Security Officer has the following information security responsibilities:

a. Developing, promulgating, implementing, and monitoring the 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.

4.24 Office of Human Resources Management (OHRM)

The Human Resource Office is responsible for designating the risk levels for all positions in the GSA and incorporating the risk level in the position designation(s) for each series and grade.

4.25 System/Network Administrators

System/Network administrators have the following security responsibilities:

a. Ensuring the appropriate security requirements are implemented consistently with GSA IT security policies and procedural and technical guides;

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

e. Performing audit/log reviews for systems not integrated with the GSA ELP to identify potential security issues as specified in the SSP.

4.26 Supervisors

Supervisors have the following security responsibilities:

a. Authorizing the assignment of an individual's identifier rests with the supervisor. Supervisors can be authorized government officials, including System Owners and Contracting Officers, who have the authority to approve initial identification.

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

c. 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;

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

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

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

g. 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.

4.27 OCISO DevSecOps Program (ODP) Security Engineer

ODP Security Engineers have the following security responsibilities:

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.

5. Policy for Identify

This section identifies the processes the GSA uses to understand its cybersecurity risks, manage its assets, assess risks to those assets and individuals, and adopt improvements to its cybersecurity management processes, procedures, and actions. These processes allow the GSA to prioritize protection efforts consistent with its mission, business objectives and cybersecurity risk management strategy.

5.1 Asset Management

This section identifies the requirements for maintaining complete and accurate inventories of GSA systems, hardware, software, services, and data.

a. System Owners and their teams, ISSMs, and ISSOs in coordination with the OCISO, must maintain the following inventories, including using approved Enterprise tools for inventory management where possible:

(1) GSA systems in GSA's official system inventory repository using the Agency System Inventory - FISMA Update Request Form and Agency System Inventory - Subsystem Update Request Form;
(2) An inventory of the devices/components comprising systems in their SSP, IAW GSA CIO-IT Security-01-05: Configuration Management (CM), including hardware, software, services, and other data required by Federal or GSA requirements;
(3) 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) HVAs IAW BOD 18-02 and GSA CIO-IT Security-26-148: Managing High Value Assets (HVA); and
(5) An inventory of 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. Data Owners, in collaboration with Data Stewards, must maintain inventories of data and corresponding metadata IAW the GSA Chief Data Officer web page. The GSA Data Inventory web page provides a list of GSA's data inventory, which lists GSA's key data holdings.

c. All communication data flows, system interconnections, and information exchanges, both internal and external, for an information system must be documented in the SSP IAW GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk and GSA CIO-IT Security-24-125: Managing Information Exchange Agreements.

d. All Interconnection Security Agreements (ISAs), Information Exchange Agreements (IEAs), and Memoranda of Agreements (MOAs) between GSA systems or between GSA and another entity's systems must be updated on the specified timeframe within the agreement (typically annually) and maintained IAW GSA CIO-IT Security-24-125: Managing Information Exchange Agreements.

e. A system's assets must be prioritized based on their classification, criticality, and business impact as part of a system's BIA and Contingency Plan. A BIA is required as part of developing a system's contingency plan.

f. System Owners and Data Owners must manage system assets (i.e., hardware, firmware, software), media, services and data, including records, throughout their life cycles, from acquisition and implementation through operations, maintenance, and transfer or disposal IAW:

(1) GSA Order CIO 1820.2A, "GSA Records Management Program"
(2) GSA Order CIO 2101.3, "GSA Integrated Information Technology Management;"
(3) GSA CIO-IT Security-01-05: Configuration Management (CM);
(4) GSA CIO-IT Security-12-64: Physical and Environmental Protection (PE);
(5) GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk;
(6) GSA CIO-IT Security-06-32: Media Protection (MP);
(7) GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts;
(8) GSA CIO-IT Security-19-101: External Information System Monitoring;
(9) CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls
(10) GSA Solutions Life Cycle (SLC) Handbook; and
(11) GSA's Procedural and Technical guides.

g. Assessment and Authorization (A&A)

GSA is in the process of implementing authorization packages for its systems using a GRC tool. As GSA continues its GRC tool implementation, A&A activities and documentation will be incorporated in the GRC tool to take advantage of its automation capabilities. Therefore, actions that occur during the A&A process and the outcome of those actions (e.g., documents) may be accomplished in the GRC tool rather than via a manual process.

(1) All GSA systems must receive authorization to operate (ATO) IAW one of the A&A processes listed in GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk. The system's A&A package must consist of the documents listed in GSA CIO-IT Security-06-30 and the documents must be updated IAW the system's specific A&A process schedule.

(2) ATOs must be received:

- before being placed into production;
- when significant changes are made to the system;
- prior to their current ATO expiring; or
- when accepted into the GSA Ongoing Authorization program.

(3) ATOs may be granted with or without restrictions or conditions. 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' ATO length.

(4) 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 documents as listed in GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk. All actions to satisfy the following conditions must be completed within the extension period (i.e., no longer than 12 months).

(a) Transitioning to ongoing authorization;
(b) Planning for disposal;
(c) Consolidating into another system for its ATO. The scope of consolidation shall be approved by the OCISO prior to submitting the ATO extension request;
(d) 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;
(e) Re-competing the system's contract;
(f) Completing the upgrade/replacement of major infrastructure components;
(g) Completing the system's security assessment has been delayed due to contract issues; or

(h) Complying with Showstopper Controls as listed in CIO-IT Security-06-30.

(5) A system undergoing a three-year re-authorization having outstanding High or Critical/Very High vulnerabilities identified during its security assessment, may request an extension for a period not to exceed 30 days from the date of the ATO expiration to allow mitigation of the High and Critical/Very High vulnerabilities. No more than two extensions may be granted under this condition.

(6) Specific GSA systems, software, applications, services, features, or functions must follow the processes listed in the guides below to receive an Approval to Use (ATU) and maintain the ATU over their lifecycle.

(a) GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk;

(i) Chrome Extensions;
(ii) SaaS Add-ons;
(iii) Google Apps Scripts;
(iv) Google Cloud Platform Services; and
(v) AWS Services.

(b) GSA CIO-IT Security-11-62: Salesforce Platform Security Implementation; and
(c) GSA CIO-IT Security-19-97: Robotic Process Automation (RPA) Security.

h. 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, "IoT Device Cybersecurity Guidance for the Federal Government," 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.

i. All GSA systems which process, store, or transmit payment card data or purchase/credit card numbers must be compliant with the current version of security requirements defined in the PCI DSS IAW GSA CIO-IT Security-26-147: Payment Card Industry (PCI) Data Security Standard (DSS) Compliance Process.

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

k. Per OMB M-23-10, "The Registration and Use of .gov Domains in the Federal Government," 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).

l. 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.

m. The GSA's IT security program is risk-based, the System Owner/program manager and ISSO can make risk-based decisions on tailoring the system's baseline NIST controls and then obtain concurrence from the AO and the CISO. Any controls tailored out of the baseline must have the rationale for the decision documented in the system's SSP.

n. The ISB Division must approve all Security Architecture designs prior to implementation IAW GSA CIO-IT Security-19-95: Security Engineering Architecture Reviews.

o. Systems must be configured to run with the least privilege and in the most restrictive mode (e.g., limiting ports, protocols, services, etc.) necessary to meet its functions and IAW GSA's IT Security Procedural guides and IT Security Technical guides.

p. All mobile devices (i.e., smartphones, tablets) and applications (i.e., developed, deployed, and/or used on GSA-issued GFE) must adhere to the requirements and approval processes defined in GSA CIO-IT Security-12-67: Securing Mobile Applications and Devices before being used.

q. The GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC) must be assessed and authorized as specified in CIO-IT Security-06-30.

r. Contracts for IT systems designed, developed, implemented, and operated by a contractor on behalf of GSA must include specific language:

(1) Allowing 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 SSAE 18 reports.
(2) Requiring solutions to align with existing information security architecture.
(3) Requiring security deliverables to be provided in a timely manner for review and acceptance by GSA.

5.2 Risk Assessment

This section identifies the requirements for managing cybersecurity risks to GSA assets, individuals, and the overall enterprise. The GSA's management of risks includes assessing threats, vulnerabilities, likelihoods, and impacts.

a. System Owners must ensure vulnerabilities are identified, assessed, remediated, and monitored as part of a system's A&A process and continuous monitoring activities IAW:

- GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk and GSA's other A&A process guides;
- GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program;
- GSA CIO-IT Security-09-44: Plan of Action and Milestones; and
- GSA CIO-IT Security-17-80: Vulnerability Management Process.

b. As specified in GSA CIO-IT Security-01-02: Incident Response (IR) the GSA OCISO maintains a threat awareness program that monitors threat intelligence for actionable information and shares this information with relevant system owners, CISA, and other government agencies as needed.

c. IAW GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk and GSA CIO-IT Security-18-91: Risk Management Strategy, GSA CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls, and the GSA Privacy Program Webpage systems must assess cybersecurity, cyber supply chain, and privacy risks by:

(1) Identifying and documenting internal and external threats that may impact organizational operations, assets or individuals through risk assessments and continuous monitoring activities;

(2) Evaluating how threats may exploit vulnerabilities, including determining the likelihood and potential impact of exploitation. These assessments must be based on system conditions, vulnerability data, and threat intelligence, and must be documented in artifacts such as Security Assessment Reports (SARs) and included as part of the assessment and authorization (A&A) process; and

(3) Using the results of the assessments and continuous monitoring activities to determine inherent risk and prioritize risk response actions. Risk mitigation must be prioritized based on likelihood, business impact, cost and compliance.

d. Systems must prioritize, plan, track, and communicate risk responses, including POA&Ms, IAW:

(1) GSA CIO-IT Security 06-30: Managing Enterprise Cybersecurity Risk
(2) GSA CIO-IT Security-12-66: Information Security Continuous Monitoring Strategy (ISCM) & Ongoing Authorization (OA) Program;
(3) GSA CIO-IT Security-17-80: Vulnerability Management Process;
(4) GSA CIO-IT Security-09-44: Plan of Action and Milestones (POA&M);
(5) GSA CIO-IT Security-11-51: Conducting Penetration Test Exercises; and
(6) GSA CIO-IT Security-24-130: Conducting Red Team Exercises.

e. Deviations, exceptions, or other conditions not following GSA IT Security policies and standards must be addressed IAW Section 1.5 of the GSA IT Security Policy.

f. Vulnerabilities reported by external parties through GSA's Vulnerability Disclosure Program (VDP) must be reviewed by the OCISO and coordinated with appropriate system personnel for validation and mitigation. The GSA has established processes for receiving, analyzing, and responding to vulnerabilities from both external and internal managed systems. For contractor-operated systems, vulnerability reporting, POA&M tracking, and remediation activities must be conducted IAW GSA CIO-IT Security-19-101: External Information System Monitoring. Internally identified vulnerabilities, including those discovered through automated scanning, must be managed in accordance with GSA CIO-IT Security-17-80: Vulnerability Management Process.

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

h. The GSA assesses critical suppliers and the authenticity and integrity of hardware and software prior to acquisition IAW the following guides. Additional guidance is available on the C-SCRM Policies, Regulations, and Laws InSite page.

(1) GSA CIO-IT Security-21-117: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program; and
(2) GSA CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls; and
(3) GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC).

i. The GSA assesses critical suppliers and the authenticity and integrity of hardware and software prior to acquisition IAW the following guides. Additional guidance is available on the C-SCRM Policies, Regulations, and Laws InSite page.

(1) GSA CIO-IT Security-21-117: OCISO Cyber Supply Chain Risk Management (C-SCRM) Program; and
(2) GSA CIO-IT Security-22-120: Supply Chain Risk Management (SR) Controls; and

(3) GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC).

5.3 Improvement

This section identifies GSA's requirements for improving cybersecurity risk management processes, procedures, and activities.

a. The results of the following evaluations must be addressed to improve the security of systems, their assets, and their data.

   (1) FISMA and Financial audits, see GSA CIO-IT Security-22-121: Annual FISMA and Financial Statements Audit;
   (2) FISMA Self-assessments, see GSA CIO-IT Security-04-26: FISMA Implementation; and
   (3) GAO audits, see GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk.

b. The results of the following security tests and exercises must be addressed to improve the security of systems, their assets, and their data.

   (1) A&A process Security Control Assessments, see GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk and GSA's other A&A process guides;
   (2) Penetration Tests, see GSA CIO-IT Security-11-51: Conducting Penetration Test Exercises; and
   (3) Red Team Exercises, see GSA CIO-IT Security-24-130: Conducting Red Team Exercises.

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. Improvements from monitoring operational procedures and processes, to include, but not limited to the following processes, must be implemented.

   (1) Continuous monitoring IAW GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program;
   (2) Vulnerability management IAW GSA CIO-IT Security-17-80: Vulnerability Management Process;
   (3) Configuration management IAW GSA CIO-IT Security-01-05: Configuration Management (CM); and
   (4) Supply Chain Risk Management IAW GSA CIO-IT Security 21-117: Cyber Supply Chain Risk Management (C-SCRM) Program.

e. The following plans must be developed as part of the A&A process for systems and uploaded into GSA's GRC tool. The plans must be reviewed annually, tested in accordance with GSA's procedural guides, and updated as necessary based on lessons learned when executing the plans and testing the plan's processes.

   (1) Incident Response Plan;
   (2) Configuration Management Plan (as necessary per FIPS Pub 199 Level and A&A Process); and
   (3) Contingency Plan, including a Business Impact Analysis.

6. Policy for Protect

This section identifies the safeguards the GSA uses to manage cybersecurity risks. Additional details on implementing safeguards and security requirements for protecting GSA systems and data are included in GSA's IT Security Procedural guides and IT Security Technical guides. Adhering to these guides reduces the likelihood of threats exploiting vulnerabilities and the resultant risks across GSA's enterprise environment.

6.1 Identity Management, Authentication, and Access Control

This section identifies GSA's requirements for managing access to physical and logical assets based on the risk of unauthorized access.

a. Systems and SSOs must manage identities and credentials for authorized users, services and hardware IAW the following guides:

   (1) GSA CIO-IT Security-01-01: Identification and Authentication (IA)
   (2) GSA CIO-IT Security-01-07: Access Control (AC)
   (3) GSA CIO-IT Security-03-23: Termination and Transfer
   (4) GSA CIO-IT Security-07-35: Web Application Security
   (5) GSA CIO-IT Security-10-50: Maintenance (MA)
   (6) GSA CIO-IT Security-12-67: Securing Mobile Devices and Applications
   (7) GSA CIO-IT Security-19-97: Robotic Process Automation (RPA) Security
   (8) GSA IT Technical Guides: Multiple guides for configuring various technologies IAW with GSA required security settings.

b. The identities of the GSA's Federal employees and contractors must be proven and bound to credentials IAW the GSA's Office of Mission Assurance IAW GSA Order ADM 9732.1E, "Personnel Security and Suitability Program Handbook," and GSA Order ADM 2181.1A, "Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing, and Background Investigations for Contractors."

c. Systems owners must restrict interactions (i.e., granting, limiting, and denying access) based on users' proven identities and credentials as defined below.

(1) **General Access:** Access to the GSA network or any GSA system requires a favorable initial fitness determination and an initiated Tier 1 (or higher) background investigation. No waivers are permitted.
(2) **PII/CUI Access:** Access to sensitive information (e.g., PII, CUI) requires a favorable initial fitness determination and an initiated Tier 2 (or higher) investigation based on:
    (a) authorization and access determined by a GSA Supervisor, CO, data owner, and system owner; and
    (b) an evaluation of the risks of such access by the system's AO.
(3) **Privileged Access:** Privileged system access requires a completed Tier 2 investigation (or higher). Waivers may be requested to maintain essential business operations. However, these requests should be made judiciously to avoid unnecessary risk to GSA.
(4) **Temporary Contractors:** Contractors working 15 days or less who require system access (e.g., for emergency service calls) are exempt from background investigations but must be escorted at all times.
(5) **Unfavorable Adjudication:** If a background investigation is unfavorable, all system and network access must be revoked, and GFE, including PIV cards, must be returned.

d. System Owners must implement identification and authentication controls, including multi-factor authentication (MFA), IAW GSA CIO-IT Security-01-01: Identification and Authentication (IA) and GSA Order CIO 2183.1, "Enterprise Identity, Credential, and Access Management (ICAM) Policy." New or modernizing applications must have their authentication options evaluated by the ICAM Portfolio.

e. All users issued GFE laptops/workstations are required to log into them 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.

f. System Owners must implement access controls IAW GSA CIO-IT Security-01-07: Access Control (AC), GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC), and the system's SSP for managing user accounts (i.e., persons) and NPEs access to systems, assets, and data wherever access is granted.

g. When GSA Google files must be shared with external users, the GSA user providing access must manage access to the files via GSA Affiliated Customer Accounts (GACAs) or Google (Personal Identification Numbers (PINs) IAW the Google-pin and GACA InSite page.

h. Systems must enforce the most restrictive set of rights/privileges needed by users (or processes acting on behalf of users) for the performance of their functions/tasks IAW GSA CIO-IT Security-01-07: Access Control (AC). Administrators must have separate user level accounts to use when administrative rights are not needed for a task.

i. 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.

j. Remote access to the GSA's resources, including systems, services, applications, and the GSA network, must align to the following requirements.

(1) Remote access must be documented in the SSP and approved as part of the system's ATO.
(2) Remote access must be implemented IAW CIO-IT Security-01-07: Access Control (AC).
(3) Personnel with GSA.gov accounts may access systems remotely as specified on the InSite Telework page.
(4) Only GSA employees and contractor personnel are permitted to use GSA furnished computers, a GSA Virtual Private Network (VPN) or Zscaler Private Access connection, or a GSA provided or funded internet connection.
(5) In special cases for remote administration and maintenance tasks, contractors may be allowed restricted IPsec access to specific GSA IP addresses.

k. Separation of duties. Systems must enforce separation of duties IAW GSA CIO-IT Security-01-07: Access Control (AC) and the following requirements:

(1) Any access or permissions clearly violating separation of duties 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) 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 user to inspect, review, audit, or test the input to determine that the input meets certain requirements should not permit the same user to both enter and verify the data.

(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).

(4) Proper separation of duties must be ensured for GSA IT system maintenance, management, and development processes.
(5) SSOs must:
(a) 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 have concurrent access to the development and production environment.
(b) Review user account privileges across their application portfolio to assess incompatible and non-compliant role assignments. For example, the review of user access assignments across systems, including the sharing of data or passing of transactions, to identify conflicts regarding separation of duties.
(c) Establish physical and logical access controls to enforce separation of duties policy and alignment with organizational and individual job responsibilities.
(6) Annual account and privilege reviews must verify separation of duties is still maintained.

l. Physical access to GSA facilities, non-GSA facilities containing GSA IT assets, and assets (e.g., servers, routers, networking equipment), including visitor access records, must be managed and implemented IAW GSA CIO-IT Security-12-64: Physical and Environmental Protection (PE) and GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC). Facilities management offices may be heavily involved in implementing these controls, especially where controls are associated with multiple systems.

m. Users must protect GSA-owned 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. Lost or stolen devices must be reported IAW the Report IT Security incidents & suspicious activity InSite page.

6.2 Awareness and Training

This section identifies the cybersecurity and awareness training requirements for GSA employees and contractors accessing GSA's systems and data.

a. All GSA employees and contractors must complete cybersecurity and privacy awareness training IAW GSA CIO-IT Security-05-29: Security and Privacy

Awareness and Role Based Training Program, including acknowledging the GSA IT General Rules of Behavior.

b. GSA employees and contractors with specialized security roles must complete role-based training IAW GSA CIO-IT Security-05-29: Security and Privacy Awareness and Role Based Training Program.

c. GSA employees and contractors with incident response responsibilities must be trained on their roles and responsibilities IAW GSA CIO-IT Security-01-02: Incident Response (IR).

d. GSA employees and contractors with contingency planning responsibilities must be trained in their roles and responsibilities IAW GSA CIO-IT Security-06-29: Contingency Planning (CP).

e. All GSA employees and contractors must comply with the prohibited and allowed personal use of GFE, services (e.g., email, Internet), and social media IAW:

(1) GSA Order ADM 7800.11A, "Personal Use of Agency Office Equipment;"
(2) GSA Order CIO 2104.1C, "GSA IT General Rules of Behavior;"
(3) GSA Order CIO 2160.2B CHGE 4, "GSA Electronic Messaging and Related Services;"
(4) GSA Order CIO 2165.2C, "GSA Telecommunications Policy;" and
(5) GSA Order OSC 2106.2A, "GSA Social Media Policy."

6.3 Data Security

This section identifies the requirements for managing the protection of data to ensure its confidentiality, integrity, and availability throughout its lifecycle.

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) using FIPS 140-3/140-2 level encryption IAW:

- GSA CIO-IT Security-06-32: Media Protection (MP);
- GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk;
- GSA CIO-IT Security-14-69, SSL/TLS Implementation Guide;
- GSA CIO-IT Security-09-43: Key Management;
- GSA CIO-IT Security-07-35: Web Application Security;
- GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts;
- GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC); and
- GSA CIO-IT Security-19-93: Application Programming Interface (API) Security.

b. System Owners, Data Owners, and users must ensure PII and CUI are protected IAW the:

- GSA Privacy Program Webpage;
- CUI Webpage;
- GSA Order CIO 2180.2, "GSA Rules of Behavior for Handling Personally Identifiable Information (PII);"
- GSA CIO-IT Security-01-07: Access Control (AC);
- GSA CIO-IT Security-01-08: Audit and Accountability (AU);
- GSA CIO-IT Security-06-32: Media Protection (MP);
- GSA CIO-IT Security-21-112: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Process;
- GSA CIO-IT Privacy-24-01: Personally Identifiable Information Processing and Transparency (PT) Controls and the following requirements.

(1) Non-GFE must not contain CUI, PII, or other data deemed sensitive by the data owner.
(2) Access to PII or CUI must be limited to only individuals with a lawful government purpose for such access.
(3) Documents and media containing CUI, including PII, must be marked and may only be disseminated in accordance with those markings. Dissemination outside of GSA (e.g., via email, mail, etc.) requires following additional processes for encryption and logging as specified by the web pages and guides listed above.
(4) PII and CUI must not be physically removed from GSA facilities or accessed remotely without written approval from the employee's supervisor, data owner, and the system Authorizing Official.
(5) Computer-readable data extracts from databases holding PII must be logged, including creator, date, type of information, and user.

c. System Owners and Data Owners must ensure the integrity of systems and information are protected against unauthorized access, tampering, alteration, loss, and destruction IAW GSA CIO-IT Security-12-63: System and Information Integrity (SI) and GSA CIO-IT Security-01-07: Access Control (AC).

d. System media must be physically and securely stored within controlled areas with access restricted to authorized individuals.

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

f. Contingency Plan/Continuity of Operations Plan Data and Supporting Media:

(1) Contact lists containing only a person's name and home phone number and kept on a password protected electronic device (i.e., a government approved

smartphone, tablet, laptop, USB drive) do not require written permission or encryption.
(2) 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
(3) All paper and supporting media must be kept in a locked facility or an otherwise secure location when not in use.

g. 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.

h. Users who plan to take GFE on international travel must:

(1) Submit a GSA IT Service Desk ticket for loaner GFE devices (e.g., a GSA laptop, GSA phone) to take with them.
(2) Comply with GSA Order ADM 5400.1A, "Meetings with Representatives of Foreign Governments or Foreign Industry, Foreign Travel, and Foreign Contact."
(3) Use a GSA virtual interface (e.g., VDI) if access to the GSA network is required.
(4) Limit WiFi connections to trusted outlets (e.g., business office); do not use public WiFi.

i. System owners must ensure system backups and their protection and testing are accomplished IAW GSA CIO-IT Security-06-29: Contingency Planning.

6.4 Platform Security

This section identifies how the GSA manages risks associated with the hardware, software, and services of its physical and virtual platforms.

a. All GSA systems, including applications, must apply configuration settings and manage the overall configuration of assets IAW GSA CIO IT-Security-01-05: Configuration Management (CM) and GSA CIO IT Security Technical guides. GSA security benchmark requirements in the technical guides must be implemented within 180 days of the benchmark's publication.

b. All GSA software and hardware must be maintained, replaced, and removed, including access authorization and use of approved technologies and tools, IAW:

- GSA CIO IT-Security-01-05: Configuration Management (CM);
- GSA CIO IT-Security-10-50: Maintenance (MA);
- GSA CIO IT-Security-06-30: Managing Enterprise Cybersecurity Risk; and
- GSA CIO IT-Security-06-32: Media Sanitization (MP).

c. Systems shall be implemented per the enterprise architecture principles in GSA Order CIO 2101.3, “GSA Integrated Information Technology Management.” The principles contained in GSA Order CIO 2101.3 are consistent with OMB Circular A-130, “Managing Information as a Strategic Resource,” which establishes the framework for architectures to address security controls for components, applications, and systems.

   - In addition to the principles set forth in GSA Order CIO 2101.3, architecture practices cited in OMB's Federal Segment Architecture Methodology must be used during planning a new system or significant capability enhancement.

   - 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-Privacy-18-90: Common Control Catalog (CCC).

d. Systems, including applications, must generate audit records/logs and review and maintain them IAW GSA CIO-IT Security-01-08: Audit and Accountability (AU) and GSA CIO IT Security Technical guides.

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

f. Users and GSA systems must only use software:

   - Approved through the IT Standards process and the Chief Technology Officer;
   - Licensed for GSA use and conforms to copyright laws;
   - Configured to run with user level rights for user software;
   - Explicitly authorized to execute IAW GSA CIO IT-Security-01-05: Configuration Management (CM), preventing all unauthorized software from executing;

g. Users must not use hardware or software tools to evaluate (e.g., scan, test) or compromise GSA resources, or bypass security controls unless authorized by the OCSIO. For example, tools used to defeat copy protection, discover passwords, identify security vulnerabilities, or decrypt encrypted files are prohibited.

h. System Owners and developers must integrate secure software development practices into their development lifecycle and monitor the performance of those practices IAW:

   - GSA Order CIO 2101.3, “GSA Integrated Information Technology Management.”
   - GSA Solutions Life Cycle (SLC) Handbook;
   - GSA CIO IT-Security-01-05: Configuration Management (CM);

- GSA CIO-IT Security-12-63: System and Information Integrity (SI);
- GSA CIO IT-Security-16-72: Software Security Testing;
- GSA CIO-IT Security-17-80: Vulnerability Management Process; and
- GSA CIO IT-Security-19-102: OCISO DevSecOps Program.

6.5 Technology Infrastructure Resilience

This section identifies how GSA's security architectures are managed to protect asset confidentiality, integrity, availability, and organizational resilience.

a. System owners must protect their networks and environments (i.e., production, test, and development), including components, services, and applications from unauthorized access and usage IAW the GSA IT Security Procedural guides and IT Security Technical guides.

b. Non-GFE must be restricted to the GSA's Guest networks, wired or wireless, which allow only access to the Internet, including GSA's publicly available resources (e.g., gsa.gov).

   (1) Guest wireless accounts are not ENT accounts.
   (2) GSA Guest network traffic will be subject to the same content filtering as traffic on the production network.

c. Users requiring access to GSA resources must connect to the GSA network (wired or wireless) using GFE or remotely as specified on the InSite Telework page.

d. The OCISO must approve all requests for access through a GSA network firewall or desktop firewall. Firewall change requests must follow the process outlined in GSA CIO-IT Security-06-31: Firewall and Proxy Change Request Process.

e. System contingency plans must address the ability to continue missions under all operating conditions and threats (e.g., disasters/attacks, recovery, and restoration to normal operations) IAW GSA CIO-IT Security-06-29: Contingency Planning (CP).

f. System Owners must plan for adequate resource capacity (e.g., memory, processing power, storage, power, network bandwidth) to ensure the availability of systems and assets is maintained during development and monitoring resources during operation.

g. All GSA systems operating under a DevOps or DevSecOps model have the responsibility to adhere to the requirements contained in GSA CIO-IT Security-19-102: OCISO DevSecOps Program.

h. System owners must ensure facilities in which their systems reside provide protection against water damage, fire, and environmental damage (e.g.,

excessive heat and humidity) IAW GSA CIO-IT Security-12-64: Physical and Environmental Protection (PE).

i. Systems must be implemented IAW GSA Order CIO 2101.3, "GSA Integrated Information Technology Management," including enterprise architecture and solutions life cycle principles identified therein.

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

k. 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 in 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.

l. 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.

7. Policy for Detect

This section identifies requirements and processes the GSA implements to detect and analyze cybersecurity attacks and compromises. Additional details on monitoring GSA's assets, analysis of indicators of compromise, identification of adverse events and cybersecurity incidents can be found in GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program, GSA CIO-IT Security-17-80: Vulnerability Management Process, and GSA CIO-IT Security-01-02: Incident Response (IR).

7.1 Continuous Monitoring

This section identifies continuous monitoring capabilities GSA has implemented to detect anomalies, indicators of compromise, and adverse events across its managed systems, networks, physical environments and external services.

a. All GSA networks and network services must be monitored to identify potentially adverse events as specified IAW:

- GSA CIO-IT Security-01-02: Incident Response (IR);
- GSA CIO-IT Security-01-08: Audit and Accountability (AU);

- GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy and Ongoing Authorization (OA) Program;
- GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk;
- GSA CIO-IT Security-12-63: System and Information Integrity (SI);
- GSA CIO-IT Security-17-80: Vulnerability Management Process; and
- GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC).

b. Access to physical spaces housing GSA assets must be monitored for unauthorized access and suspicious incidents as described in GSA CIO-IT Security-12-64: Physical and Environmental Protection (PE).

c. User and personnel activity must be monitored to detect potentially adverse events (e.g., fraud, misconduct, etc.) IAW:

(1) GSA CIO-IT Security-01-08: Audit and Accountability (AU);
(2) GSA CIO-IT Security-01-07: Access Control (AC); and
(3) GSA CIO IT Technical guides.

d. Systems, including applications, must present users with a use notification or banner before gaining access to the system IAW GSA CIO-IT Security-01-07: Access Control (AC). Non-publicly accessible systems must use the following banner IAW with the instructions below, although variation is allowed as specified in the guide.

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.

**********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]

****

e. External service provider activities and services must be monitored to detect potentially adverse events IAW:

(1) GSA CIO-IT Security-01-07: Access Control (AC);
(2) GSA CIO-IT Security-01-08: Audit and Accountability (AU);
(3) GSA CIO-IT Security-19-101: External Information System Monitoring;

(4) GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts

f. Systems, including their hardware, software, runtime environments, and associated data must be monitored for adverse events and conditions (e.g., unauthorized changes or updates, excessive resource usage or allocation) IAW:

(1) GSA CIO-IT Security-01-08: Audit and Accountability (AU);
(2) GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk;
(3) GSA CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts;
(4) GSA CIO-IT Security-12-63: System and Information Integrity (SI);
(5) GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy and Ongoing Authorization (OA) Program;
(6) GSA CIO-IT Security-12-67: Securing Mobile Applications and Devices;
(7) GSA CIO-IT Security-17-80: Vulnerability Management Process;
(8) GSA CIO-IT Security-Privacy-18-90: Common Control Catalog (CCC); and
(9) GSA CIO-IT Technical guides.

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

7.2 Adverse Event Analysis

This section identifies GSA's approach to analyzing anomalies, compromise indicators, and adverse events to determine their characteristics and detect future incidents.

a. Security incidents, including potential incidents, must be analyzed IAW GSA CIO-IT Security-01-02: Incident Response (IR) to understand what occurred, determine if there is an incident, and take actions as necessary to resolve the incident.

b. Information from various sources (e.g., logs, agents, sensors, etc.) must be correlated when investigating incidents IAW GSA CIO-IT Security 01-08: Audit and Accountability (AU) and GSA CIO-IT Security-01-02: Incident Response (IR).

c. The GSA Incident Response Team, in collaboration with others, must determine the impact and scope of adverse events/incidents based on Federal and GSA guidance IAW GSA CIO-IT Security-01-02: Incident Response (IR).

d. Information on adverse events (e.g., incidents, attacks) must be shared and reported to internal and external organizations and personnel using the methods and tools identified in GSA CIO-IT Security-01-02: Incident Response (IR).

e. The GSA Incident Response Team, in collaboration with others, must include information from cyber threat intelligence sources, the system environment, and

other credible sources as part of the incident analysis IAW GSA CIO-IT Security-01-02: Incident Response (IR).

f. Incidents must be formally declared by the Incident Response Team based on Federal and GSA guidance and criteria IAW GSA CIO-IT Security-01-02: Incident Response (IR). The determination whether a major incident has occurred (requiring Congressional reporting) will be made as described in GSA CIO-IT Security-01-02 and GSA Order CIO 9297.2C CHGE1, "GSA Information Breach Notification Policy."

8. Policy for Respond

This section identifies the required actions regarding a detected cybersecurity incident. Additional details that support the ability to contain and respond to a potential cybersecurity incident can be found in GSA CIO-IT Security-01-02: Incident Response (IR), GSA CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk, and individual systems' IR plans.

8.1 Incident Management

This section identifies the requirements for responding to and managing cybersecurity incidents.

a. Incident response plans for systems must be executed in collaboration with the GSA Incident Response Team; and coordinated with system personnel and any relevant third parties as specified in the system's IR Plan and GSA CIO-IT Security-01-02: Incident Response (IR).

b. Incidents must be reported to the ITServiceDesk@gsa.gov or 866-450-5250 as described in GSA CIO-IT Security-01-02: Incident Response (IR) and on the Report IT Security incidents & suspicious activity web page. ISSOs must report any security incidents reported to them to the GSA IT Service Desk and GSA OCISO.

c. Lost or stolen GFE (e.g., laptops, tablets, phones, token keys, portable storage devices, GSA Access Cards) and sensitive information (e.g., PII, CUI) must be reported immediately to the GSA IT Service Desk and as follows:

    i. All losses to the Federal Protective Service via the appropriate Regional Hotline, and as directed by the appropriate ISSO or the GSA IT Service Desk.
    ii. Any loss occurring outside of Federal facilities to the local police.

d. Reported incidents must be investigated and validated by the GSA Incident Response Team in collaboration with system personnel and additional OCISO personnel as specified in the system's IR Plan and GSA CIO-IT Security-01-02: Incident Response (IR).

e. For all validated incidents, the GSA Incident Response Team, as outlined in GSA CIO-IT Security-01-02: Incident Response (IR), must:

   (1) Categorize and prioritize the incident to determine appropriate response actions;

   (2) Escalate the incident based on severity, scope and mission impact, as appropriate.

f. The GSA Incident Response Team and System Owners are responsible for initiating incident recovery actions based on criteria in the system's IR Plan and GSA CIO-IT Security-01-02: Incident Response (IR).

8.2 Incident Analysis

This section identifies the requirements for investigating cybersecurity incidents and determining their cause, scope and impact.

a. IAW GSA CIO-IT Security-01-02: Incident Response (IR), the GSA Incident Response Team must perform analysis, including forensic investigation as necessary, during and after each incident to determine what occurred, its impact, and to identify the root cause.

b. The integrity of records produced in the course of an incident investigation must be preserved IAW GSA CIO-IT Security-01-02: Incident Response (IR). The GSA Incident Response Team will:

   (1) Collect and preserve data and metadata regarding the incident; and

   (2) Determine the magnitude of an incident in coordination with other personnel/organization, as appropriate.

8.3 Incident Response Reporting and Communication

This section identifies the requirements for reporting and sharing information on cybersecurity incidents.

a. The GSA OCISO will notify both internal and external stakeholders of incidents, as appropriate, IAW GSA CIO-IT Security-01-02: Incident Response (IR).

b. The GSA Incident Response Team will share information with internal and external stakeholders as appropriate and IAW GSA CIO-IT Security-01-02: Incident Response (IR).

c. The GSA Incident Response Team in coordination with the GSA CISO, will report incidents as specified in GSA CIO-IT Security-01-02: Incident Response (IR).

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, "GSA Information Breach Notification Policy."

8.4 Incident Mitigation

This section identifies the requirements for containing, mitigating, and eradicating cybersecurity incidents.

a. The GSA Incident Response Team, in coordination with system personnel and others, as necessary, will contain incidents IAW GSA CIO-IT Security-01-02: Incident Response (IR).

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

9. Policy for Recover

This section identifies the requirements for the restoration of assets affected by a cybersecurity incident. Additional details about incident response, including recovery or restoration to normal operations can be found in GSA IO-IT Security-01-02: Incident Response (IR), GSA IO-IT Security-06-29: Contingency Planning (CP), and an individual system's IR and CP Plans.

9.1 Incident Recovery Plan Execution

This section identifies how the GSA ensures systems and services are restored after they have been affected by a cybersecurity incident.

a. The recovery actions for a system or asset must be performed in collaboration with the GSA Incident Response Team and System Owner based on the scope of an incident and as specified in the system's IR and Contingency Plans.

b. The integrity of backups and system assets being restored must be verified as specified in GSA CIO-IT Security-06-29: Contingency Planning (CP) and GSA CIO-IT Security-01-02: Incident Response (IR).

c. The Business Impact Analysis (BIA) and Contingency Plan (CP) for a system must prioritize its resources, and their recovery, based on a consideration of the criticality of the system's business functions, services, and its components.

d. The GSA Incident Response Team and System Owners are responsible for verifying the integrity of restored assets, systems, and services and the restoration of business operations.

e. The GSA Incident Response Team and System Owners are responsible for declaring an incident resolved, returning the system or asset to service, and completing any required documentation.

9.2 Incident Recovery Communication

This section identifies the requirements for coordinating and communicating recovery activities following a cybersecurity incident.

a. The GSA OCISO is responsible for communicating incident recovery activities, both internally and externally. The OCISO will notify and coordinate as necessary with other GSA officials.

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