GSA IT

IT Security Procedural Guide: System and Information Integrity (SI) CIO-IT Security-12-63

Revision 3

September 30, 2022

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Version – March 5, 2012		
1	Blanche Heard	New product	Support for 800-53 controls	N/A
		Revision 1 – October 4, 2016		
1	Wilson/ Klemens	Changes made throughout the document to reflect current NIST and GSA requirements and processes.	Update to NIST SP 800-53 Revision 4, align with ISE processes, and update formatting/style.	Throughout
		Revision 2 – February 7, 2019		
1	Dean/ Klemens	Updated format and NIST SP 800-53 control parameters, added a section on SCRM, included EO 13800 and NIST Cybersecurity Framework.	Biennial update.	Throughout
		Revision 3 – September 30, 2022		
1	Dean/ Klemens/ McCormick	Revisions included: • Updated to NIST SP 800-53, Revision 5 controls, parameters, and implementation details. • Edited and updated format.	Align to current NIST guidance, GSA parameters, and guide format. New or substantively changed controls in Revision 5 are: SI-4(10), SI-4(12), SI-4(14), SI-4(20), SI-4(22), SI-5(1), SI-7(15), SI-12(1), SI-12(2), SI-12(3), SI-18, SI-18(4), SI-19.	Throughout

Approval

IT Security Procedural Guide: System and Information Integrity (SI), CIO-IT Security 12-63, Revision 3, is hereby approved for distribution.

DocuSigned by:

Bo Berlas

FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division (ISP) at ispcompliance@gsa.gov.

Table of Contents

Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a webpage or document listed in Appendix C. For example, Google Forms, Google Docs, and websites will have links.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

1 Introduction

Implementing system and information integrity (SI) security controls and mechanisms protects the integrity of a system and its data for the system to perform its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental. The system and information integrity principles and practices described in this guide are based on guidance from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations. Throughout the remainder of this guide, the identifier SI will be used when referring to the NIST SI controls or the control family, otherwise system and information integrity will be used.

Every General Services Administration (GSA) Information Technology (IT) system must follow the practices identified in this guide. Any deviations from the security requirements established in GSA Order CIO 2100.1, GSA Information Technology (IT) Security Policy must be coordinated by the Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and authorized by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form.

Executive Order (EO) 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure requires all agencies to use “The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by NIST or any successor document to manage the agency’s cybersecurity risk.” This NIST document is commonly referred to as the Cybersecurity Framework (CSF).

Executive Order (EO) 13800, Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, requires all agencies to use “The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by NIST or any successor document to manage the agency’s cybersecurity risk.” This NIST document is commonly referred to as the Cybersecurity Framework (CSF). GSA uses the NIST SP 800-37, Revision 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, commonly referred to as the Risk Management Framework (RMF) as its foundation for managing risk, including the implementation of NIST SP 800-53 controls. Further information on how AC controls relate to the CSF is provided in Appendix A.

1.1 Purpose

The purpose of this guide is to provide guidance for the NIST SP 800-53 SI controls and system and information integrity requirements specified in CIO 2100.1. This guide provides GSA Federal employees and contractors with significant security responsibilities, as identified in CIO 2100.1, and other IT personnel involved in implementing system and information integrity with guidance on the specific procedures they are to follow for implementing SI features, mechanisms, and functions for systems under their purview.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in system and information integrity implementation for GSA information systems and information. All GSA systems must adhere to the requirements and guidance provided with regards to the procedures, processes, and methods for implementing system and information integrity as described in this guide. Per CIO 2100.1, a GSA information system is an information system:

- used or operated by GSA; or
- used or operated on behalf of GSA by a contractor of GSA or by another organization.

1.3 Policy

Appendix B contains the CIO 2100.1 policy statements regarding system and information integrity for GSA systems.

1.4 References

Appendix C provides links to references used throughout this guide.

2 Roles and Responsibilities

There are many roles associated with implementing effective system and information integrity policies and procedures. System owners for each information system are responsible for ensuring SI procedures and processes exist for their specific systems and appropriate personnel have been assigned activities/tasks to satisfy the NIST SI control requirements. Appendix D provides a listing of roles and responsibilities related to implementing, administering, managing, and monitoring system and information integrity for systems at GSA.

3 GSA Implementation Guidance for SI Controls

The GSA-defined parameter settings included in the control requirements are in blue, italicized text and offset by brackets in the control text. The GSA implementation guidance stated for each control applies to personnel and/or the systems operated on behalf of GSA. Any additional instructions or requirements for contractor systems are included in the “Additional Contractor System Considerations” portion of each control section.

Table 3-1 identifies the designation of SI controls as Common, Hybrid, or System-Specific controls for Federal and Contractor systems.

- *Common* controls are provided by GSA at the enterprise level or by one of GSA's Major Information Systems (e.g., General Support System),
- *System specific* controls are implemented at the system level, and
- *Hybrid* controls have shared responsibilities.

CIO-IT Security 18-90: Information Security Program Plan (ISPP), describes the GSA enterprise-wide controls and outlines the responsible parties for implementing them.

Note: Until the ISPP is updated to NIST SP 800-53, Revision 5, contact ispcompliance@gsa.gov for guidance if there is a discrepancy between this guide and the ISPP.

Table 3-1: Designation of SI Controls

System Type	Federal	Contractor
Common	SI-1, SI-2(2), SI-2(3), SI-4(2), SI-4(4), SI-4(5), SI-4(12), SI-4(14), SI-4(16), SI-4(18), SI-4(20), SI-4(22), SI-4(23), SI-5, SI-7, SI-7(1), SI-7(7), SI-8, SI-8(2), SI-16	
Hybrid	SI-2, SI-3, SI-4, SI-4(10), SI-5(1), SI-7(2), SI-7(5)	SI-1, SI-2
System-Specific	SI-6, SI-7(15), SI-10, SI-11, SI-12, SI-12(1), SI-12(2), SI-12(3), SI-18, SI-18(4), SI-19	SI-2(2), SI-2(3), SI-3, SI-4, SI-4(2), SI-4(4), SI-4(5), SI-4(10), SI-4(12), SI-4(14), SI-4(16), SI-4(18), SI-4(20), SI-4(22), SI-4(23), SI-5, SI-5(1), SI-6, SI-7, SI-7(1), SI-7(2), SI-7(5), SI-7(7), SI-7(15), SI-8, SI-8(2), SI-10, SI-11, SI-12, SI-12(1), SI-12(2), SI-12(3), SI-16, SI-18, SI-18(4), SI-19

Table 3-2 identifies GSA's SI control applicability at the FIPS 199 Low, Moderate, and High levels, and for GSA's Lightweight (LATO) and Moderate Impact Software-as-a Service (MiSaaS) assessment and authorization (A&A) processes

Table 3-2: SI Control Applicability

FIPS 199 Level	Applicable Controls
Low	SI-1, SI-2, SI-3, SI-4, 5, SI-12
Moderate	SI-1, SI-2, SI-2(2), SI-2(3)*, SI-3, SI-4, SI-4(2), SI-4(4), SI-4(5), SI-4(18)**, SI-4(23)**, SI-5, SI-7, SI-7(1), SI-7(7), SI-8, SI-8(2), SI-10, SI-11, SI-12, SI-12(1)^, SI-12(2)^, SI-12(3)^, SI-16, SI-18^, SI-18(4)^, SI-19^
High	SI-1, SI-2, SI-2(2), SI-2(3)*, SI-3, SI-4, SI-4(2), SI-4(4), SI-4(5), SI-4(10), SI-4(12), SI-4(14), SI-4(18)**, SI-4(20), SI-4(22), SI-4(23)**, SI-5, SI-5(1), SI-6, SI-7, SI-7(1), SI-7(2), SI-7(5), SI-7(7), SI-7(15), SI-8, SI-8(2), SI-10, SI-11, SI-12, SI-12(1)^, SI-12(2)^, SI-12(3)^, SI-16, SI-18^, SI-18(4)^, SI-19^
LATO	SI-2, SI-4, SI-4(2), SI-4(4), SI-4(5), SI-7, SI-10
MiSaaS	SI-2, SI-3, SI-4, SI-4(2), SI-4(4), SI-4(16), SI-4(23), SI-5, SI-7, SI-10, SI-12(1), SI-12(2), SI-18

*-control is applicable at the level listed per GSA OCISO

**-control is applicable at the level listed per GSA OCISO Tailored Moderate Baseline

^-control is applicable at the level if PII is stored, processed, or transmitted

3.1 SI-1 Policy and Procedures

Control:

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
   1. [*Organization-level*] system and information integrity policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the system and information integrity policy and the associated system and information integrity controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the system and information integrity policy and procedures; and

c. Review and update the current system and information integrity:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and
   2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

Common Control Implementation:

GSA's system and information integrity policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding system and information integrity for GSA systems. This policy is disseminated GSA-wide via directive library webpages on GSA.gov and GSA's InSite websites.

GSA's system and information integrity procedures are documented in CIO-IT Security-12-63: System and Information Integrity (SI) [this guide]. The procedures facilitate the implementation of the system and information integrity policy and associated controls. This guide is disseminated GSA-wide via IT Security Procedural Guides webpages on GSA.gov and GSA's InSite websites.

Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides. The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually. The GSA OCISO is responsible for reviewing and updating CIO-IT Security-12-63 every three years and following changes to Federal or GSA policies, requirements, or guidance.

GSA Service and Staff Officers (SSOs) or system owners may augment the system and information integrity policies and procedures included in 2100.1 and CIO-IT Security-01-07 to address additional organizational or system-specific configuration management requirements. Any such policies and procedures must establish timeframes for updates.

Additional Contractor System Considerations:
Vendors/contractors may defer to the GSA policy and guide or implement their own system and information integrity policies and procedures which comply with GSA's requirements with the approval of the AO.

3.2 SI-2 Flaw Remediation

Control:

a. Identify, report, and correct system flaws;
b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;
c. Install security-relevant software and firmware updates within [*the timeframe(s) outlined within the system's system security plan and as required by CIO 2100.1 and CIO-IT Security-06-30, Managing Enterprise Cybersecurity Risk*] of the release of the updates; and
d. Incorporate flaw remediation into the organizational configuration management process.

Control Enhancements:

(2) Flaw Remediation | Automated Flaw Remediation Status. Determine if system components have applicable security-relevant software and firmware updates installed using [*automated mechanisms defined in the SSPP*] [*at the frequency defined in CIO-IT Security-17-80, Vulnerability Management Process*].

(3) Flaw Remediation | Time to Remediate Flaws and Benchmarks for Corrective Actions.

(a) Measure the time between flaw identification and flaw remediation; and

(b) Establish the following benchmarks for taking corrective actions:

[*(1) BOD Timelines*

(a) Within 14 days for vulnerabilities added to CISA's KEV Catalog with a CVE date post FY21.

(b) Per the CISA KEV catalog date or GSA Standard timelines below, whichever is earlier, for vulnerabilities in the CISA KEV catalog with a CVE date in FY21 or earlier.

(c) Within 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.

(2) GSA Standard Timelines

(a) Within 30 days for Critical (Very High) and High vulnerabilities.

(b) Within 90 days for Moderate vulnerabilities

(c) Within 120 days for Low vulnerabilities for Internet-accessible systems/services.]

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

Implementing SI-2 will assist in ensuring information system flaws are identified, reported, and corrected. All security-relevant patches, updates, and hot-fixes for the affected software must be integrated into the system's configuration management process and tested for effectiveness and potential side-effects prior to being applied to the information system. Please refer to the latest CIO-IT Security-01-05: Configuration Management, as well as NIST SP 800-40: Guide to Enterprise Patch Management Technologies, for detailed guidance on integrating flaw remediation into the configuration management process.

Vulnerability scanning activities and requirements are specified in GSA CIO 2100.1 and CIO-IT Security-17-80, with the timeframes also specified in CIO-IT Security-17-80. Operating System (including databases where applicable) and Web Application scans are required for systems at all FIPS 199 levels. Results from vulnerability scans must be documented in a system's POA&M following the procedures in CIO-IT Security-09-44: Plan of Action and Milestones (POA&M) if they cannot be mitigated within the timeframes specified in the parameter for SI-2(3) and further described in CIO-IT Security-17-80.

Systems not using GSA enterprise capabilities for scanning and monitoring flaw remediation must have a capability similar to satisfy the control requirements.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.3 SI-3 Malicious Code Protection

Control:

a. Implement [*signature based and non-signature based*] malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code;
b. Automatically update malicious code protection mechanisms as new releases are available in accordance with organizational configuration management policy and procedures;
c. Configure malicious code protection mechanisms to:
   1. Perform periodic scans of the system [*weekly*] and real-time scans of files from external sources at [*endpoint and network entry/exit points*] as the files are downloaded, opened, or executed in accordance with organizational policy; and
   2. [*Block or quarantine malicious code*]; and send alert to [*system administrator and log*] in response to malicious code detection; and
d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the system.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

GSA manages, operates, administers, and maintains a number of enterprise security tools. Included in those tools are a variety of anti-malware tools, including Tripwire and Bit9. GSA uses both signature and non-signature-based antivirus/anti-malware tools, application whitelisting, perimeter firewalls and spam filtering on its mail servers. All devices, products, and tools are configured in accordance with GSA policy. GSA configures its anti-malware/malicious code protection tools to automatically update and be pushed to systems in accordance with overall configuration management and testing processes and procedures. GSA performs scans of systems as described in CIO-IT Security-17-80 which includes the process for handling false positives.

System owners are responsible for ensuring that their systems utilize the GSA anti-malware/malicious code protection solutions or a solution with similar capabilities that address the control requirements**.**

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.4 SI-4 System Monitoring

Control:

a. Monitor the system to detect:
   1. Attacks and indicators of potential attacks in accordance with the following monitoring objectives: [*ensuring the proper functioning of internal processes and controls in furtherance of regulatory and compliance requirements; examining system records to confirm that the system is functioning in an optimal, resilient, and secure state; identifying irregularities or anomalies that are indicators of a system malfunction or compromise*]; and
   2. Unauthorized local, network, and remote connections;

b. Identify unauthorized use of the system through the following techniques and methods: [*a variety of sources including but not limited to continuous monitoring vulnerability scans, malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers*];
c. Invoke internal monitoring capabilities or deploy monitoring devices:
   1. Strategically within the system to collect organization-determined essential information; and
   2. At ad hoc locations within the system to track specific types of transactions of interest to the organization;
d. Analyze detected events and anomalies;
e. Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the Nation;
f. Obtain legal opinion regarding system monitoring activities; and
g. Provide [*the GSA SSO or Contractor recommended and GSA CISO and AO approved information system monitoring information*] to [*ISSM, ISSO, and System Program Managers who distribute the information to other personnel with system administration, monitoring, and/or security responsibilities*] [*within the timeframe(s) specified in the applicable system security and privacy plan*].

Control Enhancements:

(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis. Employ automated tools and mechanisms to support near real-time analysis of events.

(4) System Monitoring | Inbound and Outbound Communications Traffic.
   (a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;
   (b) Monitor inbound and outbound communications traffic [*continuously*] for [*indicators of compromise (IOCs) including but not limited to known bad IP address(s), URI(s), hash(s) from trusted sources; suspicious DNS activity; large data uploads; and other unusual or unauthorized activities or conditions as determined by the GSA CISO and AO.*]

(5) System Monitoring | System-Generated Alerts. Alert [*all staff with system administration, monitoring, and/or security responsibilities including but not limited to ISSM, ISSO, System Program Managers, Sys/Net/App Admins, etc.*] when the following system-generated indications of compromise or potential compromise occur: [
compromise indicators may include but shall not be limited to the following:
   - *Protected system files or directories have been modified without notification from the appropriate change/configuration management channels.*
   - *System performance indicates resource consumption that is inconsistent with expected operating conditions.*
   - *Auditing functionality has been disabled or modified to reduce audit visibility. - Audit or log records have been deleted or modified without explanation.*
   - *The system is raising alerts or faults in a manner that indicates the presence of an abnormal condition.*

- *Resource or service requests are initiated from clients that are outside of the expected client membership set.*
- *The system reports failed logins or password changes for administrative or key service accounts.*
- *Processes and services are running that are outside of the baseline system profile.*
- *Utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose*].

(10) System Monitoring | Visibility of Encrypted Communications. Make provisions so that [*web traffic*] is visible to [*a web application or next generation firewall*].

(12) System Monitoring | Automated Organization-Generated Alerts. Alert [*System Owner, AO, ISSO, and ISSM*] using [*email*] when the following indications of inappropriate or unusual activities with security or privacy implications occur: [*when notified by the OCISO*].

(14) System Monitoring | Wireless Intrusion Detection. Employ a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises or breaches to the system.

(16) System Monitoring | Correlate Monitoring Information. Correlate information from monitoring tools and mechanisms employed throughout the system.

(18) System Monitoring | Analyze Traffic and Covert Exfiltration. Analyze outbound communications traffic at external interfaces to the system and at the following interior points to detect covert exfiltration of information: [*GSA's mail subsystem and internal firewalls between select subnetworks.*]

(20) System Monitoring | Privileged Users. Implement the following additional monitoring of privileged users: [*logons from disallowed travel locations and from unauthorized devices and/or IP addresses.*]

(22) System Monitoring | Unauthorized Network Services.
(a) Detect network services that have not been authorized or approved by [*the system's defined Change Management or ATO processes*]; and
(b) [Alert *System Owner and ISSO*] when detected.

(23) System Monitoring | Host-Based Devices. Implement the following host-based monitoring mechanisms at [*GSA SSO or Contractor recommended and GSA CISO and AO approved information system components*]: [*GSA SSO or Contractor recommended and GSA CISO and AO approved host-based monitoring mechanisms*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

In general, system monitoring is performed by using system auditing and logging capabilities. Details on configuring specific operating systems are in individual technical hardening guides on the IT Security Technical Guide page. Details on overall auditing and integration with the GSA Enterprise Logging Platform (ELP) which provides support for system monitoring see CIO-IT Security-01-08.

GSA OCISO Security Operations Division (ISO) has implemented a variety of capabilities across the GSA enterprise, including intrusion detection system (IDS)/intrusion prevention system (IPS) tools, and other data sources that feed into the ELP which is utilized to identify unauthorized access to and use of systems in near real time. The level of monitoring is heightened if there is indication of elevated risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information. GSA OCISO consults with GSA Office of General Counsel (OGC) for legal opinion as necessary with regard to information system monitoring activities in accordance with applicable Federal Laws, Executive Orders, directives, policies, or regulations. The ELP is configured to alert appropriate personnel upon signs of compromise.

Systems not connected to the ELP or protected by the GSA IDS/IPSs, and perimeter firewall are responsible for adhering to the control requirements independently.

Similar to the main control, the enhancements for SI-4 generally met by integrating with GSA's enterprise security tools such as the ELP, IDS/IPSs, and firewalls. For FIPS 199 High systems, enhancements SI-4(12) would also require belonging to mail groups that receive alert notifications from the ISO Division, and for SI-4(14) in addition to the aforementioned integration with security tools, CIO 2100.1 requires SSOs to identify wireless access points quarterly to identify rogue access points. For SI-4(16) MiSaaS systems must integrate with a tool that correlates logs from various sources similar to how the ELP operates.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.5 SI-5 Security Alerts, Advisories, and Directives

Control:

a. Receive system security alerts, advisories, and directives from [*US-CERT, NIST, OMB, Product Vendors, and Industry Advisors*] on an ongoing basis;
b. Generate internal security alerts, advisories, and directives as deemed necessary;
c. Disseminate security alerts, advisories, and directives to: [*all staff with system administration, monitoring, and/or security responsibilities including but not limited to ISSM, ISSO, System Program Managers, Sys/Net/App Admins, etc.*]; and
d. Implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.

Control Enhancements:

(1) Security Alerts, Advisories, and Directives | Automated Alerts and Advisories. Broadcast security alert and advisory information throughout the organization using [*email*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

The GSA OCISO ISO Division receives information system security alerts, advisories, and directives (e.g., BODs/EDs) pertaining to enterprise information system security from various sources on an ongoing basis. Sources include but are not limited to US-CERT, NIST, OMB, Product Vendors, Industry Advisors, etc. Security alerts, advisories, and directives are reviewed for relevance to GSA's IT operating environment and distributed to IT and security staff, as applicable.

ISO distributes security alerts, advisories, and directives pertaining to enterprise information system security to internal and external enterprise entities with IT system security responsibility over GSA systems. These entities include all staff with system administration, monitoring, and/or security responsibilities including but not limited to ISSM, ISSO, System Program Managers, Sys/Net/App Admins, etc. Information is disseminated through email distribution lists. ISO maintains the root level email groups, however populating individual group memberships are delegated to the various Division directors.

ISO in coordination with ISE is responsible for overseeing the enterprise implementation of security directives in accordance with established time frames or notifies the issuing organization of the degree of noncompliance.

Information systems may supplement the security alerts, advisories, or directives received from ISO by subscribing to other sources; generating internal system alerts as necessary; disseminating alerts to IT and IT security personnel; and implementing the directives in accordance with established time frames set by GSA consistent with SI-5 requirements.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.6 SI-6 Security and Privacy Function Verification

Control:

a. Verify the correct operation of [*high security functions*];
b. Perform the verification of the functions specified in SI-6a [*on system startup and/or restart and abort; upon command by user with appropriate privilege; at least every 90 days*];
c. Alert [*system administrators*] to failed security and privacy verification tests; and
d. [*Halts the information system or triggers audit alerts when unauthorized modifications to critical security files occur and*] when anomalies are discovered.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

GSA requires FIPS 199 High level systems to be capable of verifying security functionality of all configured security functions upon system startup/restart and periodically every 90 days. Any of the security functions that are not able to perform automated self-tests, must either have compensating controls applied or an acceptance of risk authorized for not performing the verification as required. Any anomalies or issues associated with the correct operation of security functions must be reported to the designated system administrator for corrective action.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.7 SI-7 Software, Firmware, and Information Integrity

Control:

a. Employ integrity verification tools to detect unauthorized changes to the following software, firmware, and information: [*GSA software, firmware, and information*]; and
b. Take the following actions when unauthorized changes to the software, firmware, and information are detected: [*notify the System Owner, ISSO, ISSM, and the GSA Incident Response team.*]

Control Enhancements:

(1) Software, Firmware, and Information Integrity | Integrity Checks. Perform an integrity check of [*GSA software, firmware, and information*] [*at startup; at the occurrence of configuration changes or security-relevant events; at least monthly.*]
(2) Software, Firmware, and Information Integrity | Automated Notifications of Integrity Violations. Employ automated tools that provide notification to [*personnel with system administration, monitoring, or security responsibilities as identified in CIO 2100.1, CIO-IT Security-01-02, and CIO-IT Security-01-08*] upon discovering discrepancies during integrity verification.
(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations. Automatically [*engages GSA SSO or Contractor recommended and GSA CISO and AO approved security safeguards*] when integrity violations are discovered.
(7) Software, Firmware, and Information Integrity | Integration of Detection and Response. Incorporate the detection of the following unauthorized changes into the organizational incident response capability: [*changes to established configuration settings or unauthorized elevation of information system privileges*].
(15) Software, Firmware, and Information Integrity | Code Authentication. Implement cryptographic mechanisms to authenticate the following software or firmware components prior to installation: [*for all vendor supported, 3rd party, or open-source provided software*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

GSA's enterprise security tools include application software that allows or denies software execution and file integrity monitoring of GSA managed assets. This software is integrated into the ELP for notification purposes and is utilized as part of the GSA incident response capability.

Systems not using the tools offered by GSA OCISO and not integrated into GSA's enterprise security tools and the ELP are responsible for adhering to this requirement independently.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.8 SI-8 Spam Protection

Control:

a. Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages; and
b. Maintain records of the system components

Control Enhancements:

(2) Spam Protection | Automatic Updates. Automatically update spam protection mechanisms [*daily*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

GSA utilizes Google GSuite Enterprise for email and collaboration. GSuite is supported by strong spam protection capabilities that automatically and continuously via AI/machine learning (through Gmail) help identify spam and suspicious emails by detecting viruses, finding patterns across messages, and learning from what Gmail users commonly mark as spam or phishing. Additionally, GSA implements other technologies/aspects of email infrastructure, e.g., Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting and Conformance (DMARC), to prevent spoofing of messages originating from outside of the gsa.gov domain sent to gsa.gov addresses and message integrity.

Systems not using the components/technologies offered by GSA are responsible for adhering to this requirement independently.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.9 SI-10 Information Input Validation

Control: Check the validity of the following information inputs: [*character set, length, numerical range, and acceptable values) verifies that inputs match specified definitions for format and content as it relates to:*

(1) Username and password combinations.
(2) Attributes used to validate a password reset request (e.g., security questions).
(3) Personally identifiable information (excluding unique username identifiers provided as a normal part of a transactional record).

(4) Biometric data or personal characteristics used to authenticate identity.
(5) Sensitive financial records (e.g., account numbers, access codes).
(6) Content related to internal security functions: private encryption keys, whitelist or blacklist rules, object permission attributes and settings].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

This control helps ensure requirements for validating and filtering inputs to the information system have been explicitly identified. A set of rules for checking valid syntax and semantics must be developed and implemented on the information system to prevent any input into the system to be unintentionally interpreted as commands.

For example, systems must verify that inputs match specified definitions for syntax, semantics, format, and content as it relates to:

- Username and password combinations.
- Attributes used to validate a password reset request (e.g., security questions).
- Personally identifiable information (PII) (excluding unique username identifiers provided as a normal part of a transactional record).
- Biometric data or personal characteristics used to authenticate identity.
- Sensitive financial records (e.g., account numbers, access codes).
- Content related to internal security functions: private encryption keys, whitelist or blacklist rules, object permission attributes and settings.

The information system must be capable of providing information input validation as close to the point of data entry as possible. For example, a web based application must be configured to filter characters entered into input fields that may also serve as commands/operators within the backend database. Data that is input into these fields must be checked against an explicit set of format and syntax rules. Please refer to CIO-IT Security-07-35: Web Application Security for more detailed guidance regarding the configuration of input validation mechanisms.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.10 SI-11 Error Handling

Control:

a. Generate error messages that provide information necessary for corrective actions without revealing information that could be exploited; and
b. Reveal error messages only to [*Information System Security Manager, Information System Security Officer, System Owners, Acquisitions/Contracting Officers, Custodians*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

This control helps ensure that system generated error messages do not reveal potentially exploitable information yet contain enough information to facilitate timely and useful response. GSA FIPS 199 Moderate and High impact systems must be capable of identifying error conditions and generating error messages which are viewable to authorized personnel only.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.11 SI-12 Information Management and Retention

Control: Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

Control Enhancements:

(1) Information Management and Retention | Limit Personally Identifiable Information Elements. Limit personally identifiable information being processed in the information life cycle to the following elements of personally identifiable information: [*as defined in the System of Records Notices (SORN)*].

(2) Information Management and Retention | Minimize Personally Identifiable Information In Testing, Training, and Research. Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: [*this policy/process is under development and considers the sensitivity of PII, number of individuals and/or records in the research, testing, or training*].

(3) Information Management and Retention | Information Disposal. Use the following techniques to dispose of, destroy, or erase information following the retention period: [*as defined in CIO-IT Security-06-32, Media Protection*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

The requirements of this control serve as a bridge between GSA's information management policies and procedures and any information system output guidelines developed by GSA. Information maintained by GSA systems must be managed in accordance with media access and media storage policies and procedures detailed in CIO-IT Security-06-32. Retention of information output by the system such as event and security logs in addition to system generated reports must follow the guidelines established in CIO-IT Security-06-32, and must comply with requirements established by the National Archives and Records Act (NARA), GSA Order OAS P 1820.1, GSA Records Management Program, and GSA Privacy Program requirements.

For enhancement SI-12(1), the GSA Privacy Office develops privacy policies and manages the GSA privacy program to minimize the use of PII throughout a system's lifecycle. The SORN is used to document the PII used by a GSA system. The GSA Privacy Office collaborates with ISSOs and system owners in minimizing the PII used by a system and documenting it in the SORN.

For enhancement SI-12(2), the use of PII for testing, training, and research is only allowed if the ATO of the system authorizes its use as part of the overall assessment and authorization of the system. The GSA Privacy Office is developing a policy/process to minimize the potential impact to individuals and resulting impacts to organizations. Response approaches may include synthesizing PII for testing and/or training; and if PII is necessary for research purposes, avoiding or accepting the risk as described below:

- Mitigating the risk (e.g., GSA may be able to apply technical and/or policy measures to the systems, products, or services that minimize the risk to an acceptable degree);
- Transferring or sharing the risk (e.g., contracts are a means of sharing or transferring risk to other organizations, privacy notices and consent mechanisms are a means of sharing risk with individuals);
- Avoiding the risk (e.g., GSA may determine that the risks outweigh the benefits, and forego or terminate the data processing); or
- Accepting the risk (e.g., GSA may determine that problems for individuals are minimal or unlikely to occur, therefore the benefits outweigh the risks, and it is not necessary to invest resources in mitigation).

Currently the GSA Privacy Office advises and assists system owners as they implement controls such as masking, redacting or otherwise de-identifying PII to protect it if it must be used for testing, training, and research.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.12 SI-16 Memory Protection

Control: Implement the following controls to protect the system memory from unauthorized code execution: [*GSA SSO or Contractor recommended and GSA CISO and AO approved security safeguards*].

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

GSA employs a variety of anti-malware controls, including system configuration settings and software tools that provide memory protection against unauthorized code execution. The tools used vary based on operating system, application, and system, but the types of tools used include Basic Input/Output System (BIOS) settings, whitelisting and blacklisting, and file signature checking prior to allowing software to execute which could corrupt memory. In addition, modern processes typically provide a level of defense by restricting memory access based on privileged command sets. System Owners are responsible for ensuring their systems use the tools available to protect memory in their systems.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.13 SI-18 Personally Identifiable Information Quality Operations

Control:

a. Check the accuracy, relevance, timeliness, and completeness of personally identifiable information across the information life cycle [*as part of the PIA review process*]; and
b. Correct or delete inaccurate or outdated personally identifiable information.

Control Enhancements:

(4) Information Personally Identifiable Information Quality Operations | Individual Requests. Correct or delete personally identifiable information upon request by individuals or their designated representatives.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

Systems, in collaboration with the GSA Privacy Office, will determine the accuracy, relevance, timeliness, and completeness of PII as part of PIA reviews. Any issues identified as a part of the review must be corrected or deleted.

For enhancement SI-18(4), systems in collaboration with the GSA Privacy Office, will work with individuals and systems to correct or delete PII upon request.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

3.14 SI-19 De-Identification

Control:

a. Remove the following elements of personally identifiable information from datasets: [*PII and sensitive PII defined in the GSA PII Rules Matrix*]; and
b. Evaluate [*as part of the PIA review*] for effectiveness of de-identification.

GSA Implementation Guidance: Control designation as common, hybrid, or system-specific is provided in Table 3-1. Control applicability per FIPS 199 Level/A&A process is listed in Table 3-2.

All GSA systems must remove PII, as defined in the GSA PII Rules Matrix from their datasets unless the system has been approved to include PII due to its business mission requirements. Systems, in collaboration with the GSA Privacy Office, will evaluate the need and effectiveness of de-identification of PII as part of system PIA reviews.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

Appendix A: CSF Categories/Subcategories and the SI Control Family

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's RMF as its primary risk management process. Table A-1 lists the Categories and Subcategories from the CSF that are identified as related to the implementation of policies, procedures, and processes implementing the NIST SP 800-53 SI controls. GSA CIO Order 2100.1 and this procedural guide provide GSA's policies and procedural guidance regarding access control to GSA systems and implementing SI controls.

Table A-1: CSF Categories/Subcategories and the SI Control Family

CSF Category/Subcategory Identifier	Definition/Description
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated *(-1 controls from all security control families)* **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed *(-1 controls from all security control families)*
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets.	**ID.RA-1:** Asset vulnerabilities are identified and documented *(SI-2, SI-4, SI-5)* **ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources *(SI-5)* **ID.RA-3:** Threats, both internal and external, are identified and documented *(SI-5)*
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-5**: Protections against data leaks are implemented *(SI-4)* **PR.DS-6:** Integrity checking mechanisms are used to verify software, firmware, and information integrity *(SI-7, SI-10)* **PR.DS-8:** Integrity checking mechanisms are used to verify hardware integrity
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-8:** Effectiveness of protection technologies is shared *(SI-4)* **PR.IP-12**: A vulnerability management plan is developed and implemented *(SI-2)*

CSF Category/Subcategory Identifier	Definition/Description
Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed *(SI-4)* **DE.AE-2:** Detected events are analyzed to understand attack targets and methods *(SI-4)* **DE.AE-3:** Event data are collected and correlated from multiple sources and sensors *(SI-4)* **DE.AE-4:** Impact of events is determined *(SI-4)*
Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events *(SI-4)* **DE.CM-4:** Malicious code is detected *(SI-3, SI-4, SI-8)* **DE.CM-5:** Unauthorized mobile code is detected *(SI-4)* **DE.CM-6:** External service provider activity is monitored to detect potential cybersecurity events *(SI-4)* **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed *(SI-4)*
Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-3:** Detection processes are tested *(SI-3, SI-4)* **DE.DP-4:** Event detection information is communicated *(SI-4)* **DE.DP-5:** Detection processes are continuously improved *(SI-4)*
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g., external support from law enforcement agencies).	**RS.CO-5:** Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness *(SI-5)*
Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated *(SI-4)* **RS.AN-5:** Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers) *(SI-5)*

Appendix B: Policy

The following extracts from GSA Order CIO 2100.1 contain information regarding requirements related to system and information integrity for GSA IT systems and data.

Chapter 3: Policy for Identify states:

4. Risk Assessment

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

Chapter 4, Policy for Protection states:

3. Data Security

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

Note: IAW is an acronym for “in accordance with,” which is spelled out earlier in 2100.1, therefore this note provides the acronym definition for this guide.

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

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

t. Controls shall be put in place to monitor or detect changes or updates to systems outside the parameters of a system’s baseline operating characteristics. This includes the ability to monitor resource usage and allocation

Chapter 5, Policy for Detect Function, states:

2. Security Continuous Monitoring

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

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

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

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

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

Chapter 6: Policy for Respond Function states:

3. Analysis

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

Appendix C: References

Federal Laws, Standards, Regulations, and Publications:

- Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Directives
- EO 13800: Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure
- FIPS PUB 199: Standards for Security Categorization of Federal Information and Information Systems
- NIST CSF: Framework for Improving Critical Infrastructure Cybersecurity
- NIST SP 800-37, Revision 2: Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- NIST SP 800-40, Revision 4, “Guide to Enterprise Patch Management Planning: Preventative Maintenance for Technology”
- NIST SP 800-53, Revision 5: Security and Privacy Controls for Information Systems and Organizations
- OMB Circular A-130: Managing Information as a Strategic Resource

GSA Policies, Procedures, Guidance:

The GSA policies listed below are available on the GSA.gov Directives Library page.

- GSA Order CIO 2100.1: GSA Information Technology (IT) Security Policy
- GSA Order CIO 1820.2: GSA Records Management Program

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides page with the exception of CIO-IT Security-07-35 and CIO-IT Security-18-90 which are restricted. They are available on the internal GSA InSite IT Security Procedural Guides page.

- CIO-IT Security-01-02: Incident Response (IR)
- CIO-IT Security-01-05: Configuration Management (CM)
- CIO-IT Security-01-07: Access Control (AC)
- CIO-IT Security-01-08: Audit and Accountability (AU)
- CIO-IT Security-06-30: Managing Enterprise Cybersecurity Risk
- CIO-IT Security-06-31: Firewall and Proxy Change Request Process
- CIO-IT Security-06-32: Media Protection (MP)
- CIO-IT Security-07-35: Web Application Security
- CIO-IT Security-09-43: Key Management
- CIO-IT Security 09-44: Plan of Action and Milestones (POA&M)
- CIO-IT Security-17-80: Vulnerability Management Process
- CIO-IT Security-18-90: Information Security Program Plan (ISPP)

Appendix D: Roles and Responsibilities

There are many roles associated with implementing effective system and information integrity policies and procedures. The roles and responsibilities provided in this appendix have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. The responsibilities listed in this guide are focused on system and information integrity; a complete set of GSA security roles and responsibilities can be found in CIO 2100.1. Throughout this guide, specific processes, and procedures for implementing NIST SP 800-53 SI controls are described.

Authorizing Official (AO)

Responsibilities include the following:

- Ensuring that GSA information systems under their purview have implemented the required NIST SP 800-53 SI controls in accordance with GSA and Federal policies and requirements.
- Identifying the level of acceptable risk for an information system and determining whether an acceptable level of risk has been obtained, including risks associated with NIST SP 800-53 SI controls.
- Ensuring all information systems, applications, or sets of common controls under their purview have a current ATO issued per GSA CIO-IT Security-06-30.
- Ensuring a plan of action and milestones (POA&M) entry is developed and managed to address any NIST SP 800-53 SI controls that are not fully implemented.

Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Assisting ISSOs, as necessary, to ensure NIST SP 800-53 SI controls are in place and operating as intended.
- Verifying systems under their purview have appropriately addressed NIST SP 800-53 SI controls.
- Coordinating with the AO, System Owner, ISSOs, and OCISO Directors, as necessary, regarding NIST SP 800-53 SI control implementation and compliance with NIST and GSA requirements.
- Working with the ISSO and System Owner to develop and manage POA&Ms regarding NIST SP 800-53 SI controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.
- Reviewing and coordinating reporting of Security Advisory Alerts (SAA), compliance reviews, security and privacy awareness training, incident reports, contingency plan testing, and other IT security program elements.

Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Ensuring necessary NIST SP 800-53 SI controls are in place and operating as intended.
- Coordinating with ISSMs and System Owners, as necessary, regarding NIST SP 800-53 SI control implementation and compliance with NIST and GSA requirements.
- Working with the System Owner and ISSM to develop and manage POA&Ms regarding NIST SP 800-53 SI controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.
- Evaluating SAAs and known vulnerabilities to ascertain if additional safeguards are needed, and ensuring systems are patched and securely configured, as appropriate;

System Owners

Responsibilities include the following:

- Defining and scheduling software patches.
- Ensuring necessary NIST SP 800-53 SI security controls are in place and operating as intended.
- Coordinating with ISSOs and ISSMs, as necessary, regarding NIST SP 800-53 SI control implementation and compliance with NIST and GSA requirements.
- Working with ISSOs and ISSMs to develop and manage POA&Ms regarding NIST SP 800-53 SI controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.
- Obtaining the resources necessary to securely implement and manage NIST SP 800-53 SI controls for their respective systems.
- Working with Data Owners to audit user activity for indications of fraud, misconduct, or other irregularities.
- 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.

Data Owners

Responsibilities include the following:

- Coordinating with System Owners, ISSMs, ISSOs, and Custodians to ensure data is properly stored, maintained, and protected per GSA policies, regulations and any additional guidelines established by GSA.
- Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of NIST SP 800-53 SI controls in compliance with NIST and GSA requirements.
- Working with the System Owner to ensure the appropriate level of auditing and logging data is enabled and generated to support monitoring activities.
- Working with the System Owner to audit user activity for indications of fraud, misconduct, or other irregularities.
- Working with the System Owner to document all phases of monitoring activity including monitoring procedures, response processes, and steps performed when reviewing user activity.

Custodians

Responsibilities include the following:

- Coordinating with System Owners, ISSMs, ISSOs, to ensure data is properly stored, maintained, and protected per GSA policies, regulations and any additional guidelines established by GSA.
- Establishing, monitoring, and operating information systems in a manner consistent with GSA policies and standards as relayed by the Authorizing Official.

Authorized Users of IT Resources

Responsibilities include the following:

- Familiarizing themselves with any special requirements for accessing, protecting, and using data, including Privacy Act requirements, copyright requirements, and procurement-sensitive data.
- Ensuring that adequate protection is maintained on their workstation, including not sharing passwords with any other person and logging out, locking, or enabling a password protected screen saver before leaving their workstation.

System/Network Administrators

Responsibilities include the following:

- Ensuring the appropriate system and information integrity security requirements are implemented consistent with GSA IT security policies and hardening guidelines.
- Implementing system backups and patching of security vulnerabilities.
- Working with the Custodian/ISSO to ensure appropriate technical system and information integrity security requirements are implemented.
- Identifying and reporting security incidents and assisting the OCISO, in resolving security incidents.