IT Security Procedural Guide: FY21 IT Security Program Management Implementation Plan CIO-IT Security-08-39

Revision 8

April 19, 2021

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Revision 1 – December 5,2008		
1	Berlas	Updated milestone dates and dates for submission of quarterly reports.	FY 2009 update.	8-15
		Revision 2 – November 4, 2009		
1	Berlas	Updated milestone dates and dates for submission of quarterly reports.	FY 2010 update.	8-15
		Revision 3 – January 14, 2011		
1	Berlas	Updated milestone dates and dates for submission of quarterly reports. Updated to Assessment and Authorization (A&A) terminology.	FY 2011 update.	Throughout
		Revision 4 – March 15, 2012		
1	Berlas	Updated milestone dates and dates for submission of quarterly reports.	FY 2012 update.	8-15
		Revision 5 – December 7, 2012		
1	Berlas	Updated milestone dates and dates for submission of quarterly reports.	FY 2013 update.	8-15
		Revision 6 – December 13, 2013		
1	Berlas	Updated milestone dates and dates for submission of quarterly reports.	FY 2014 update.	8-15
		Revision 7 – October 30, 2014		
1	Sitcharing, Kearns, Heard	Updated milestone dates	Updated milestones, responsibilities, edited throughout.	Throughout
		Revision 8 – April 19, 2021		
1	Desai, Heard, Normand, Klemens, Dean	Changes include: • Summarized previous revision descriptions. • Updated guide to current GSA processes, timelines, and guidance. • Updated to current guide formatting and style.	Re-establishing guide for FY21.	Throughout

CONCURRENCE

X DocuSigned by: Sagar Samant EAD7396185D84A7...

Sagar Samant, Authorizing Official
Acquisition IT Services (IQ)

X DocuSigned by: Phil Klokis 6F8E4C8418E2469...

Philip Klokis, Authorizing Official
Public Builiding IT Services (IP)

X DocuSigned by: David Shive A3AE4284A2754F9...

David Shive, Authorizing Official
GSA Chief Information Officer

X DocuSigned by: Elizabeth DelNegro 70F7CFB0F9654DA...

Elizabeth DelNegro, Authorizing Official
Corporate IT Services (IC)

X DocuSigned by: Aidan Feldman 5D660E51B21E415...

Aidan Feldman, Authorizing Official
Technology Transformation Service (TTS)

X DocuSigned by: 41786C5520EC42C...

Daniel Pomeroy, Authorizing Official
Office of Governmentwide Policy (OGP)

Approval

IT Security Procedural Guide: FY21 IT Security Program Management Implementation Plan, CIO-IT Security 08-39, Revision 8, is hereby approved for distribution.

X DocuSigned by: Bo Berlas FB7179201815444F...

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

Note: 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

The General Services Administration (GSA) Chief Information Security Officer (CISO) is responsible for implementing and administering an information security program to protect the agency's information resources, support business processes and the GSA mission. The program must implement a mandatory set of processes and system controls per federal regulations, Executive Orders, including the Federal Information Security Modernization Act of 2014 (FISMA); the Office of Management and Budget (OMB) Circular A-130, and National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) and Special Publications (SPs) documents to ensure the confidentiality, integrity, and availability of system related information and information resources.

To meet these requirements, GSA has implemented an agency-wide, risk-based information security program as defined in GSA CIO Order 2100.1, "GSA Information Technology (IT) Security Policy." The agency policy provides requirements to support procedures, guidelines, and formalized processes coordinated through the Office of the Chief Information Security Officer (OCISO). These elements form the foundation for GSA's information security program and define requirements for GSA systems and employees/contractors with significant security responsibilities, ensuring implementation of information security requirements.

The FY21 Management Implementation Plan identifies the key information security activities and milestones (due dates) for the Fiscal Year involved in managing enterprise-level risk for GSA information systems. The guide is an aid to agency employees and contractors with security responsibilities to identify and proactively implement key existing IT security requirements codified in Federal law and GSA policy. The system specific requirements herein integrate into GSA's broader enterprise risk management approach as depicted in the three-tiered approach in Figure 1 that addresses risk at the organization level; mission/business process level; and at the information system level.

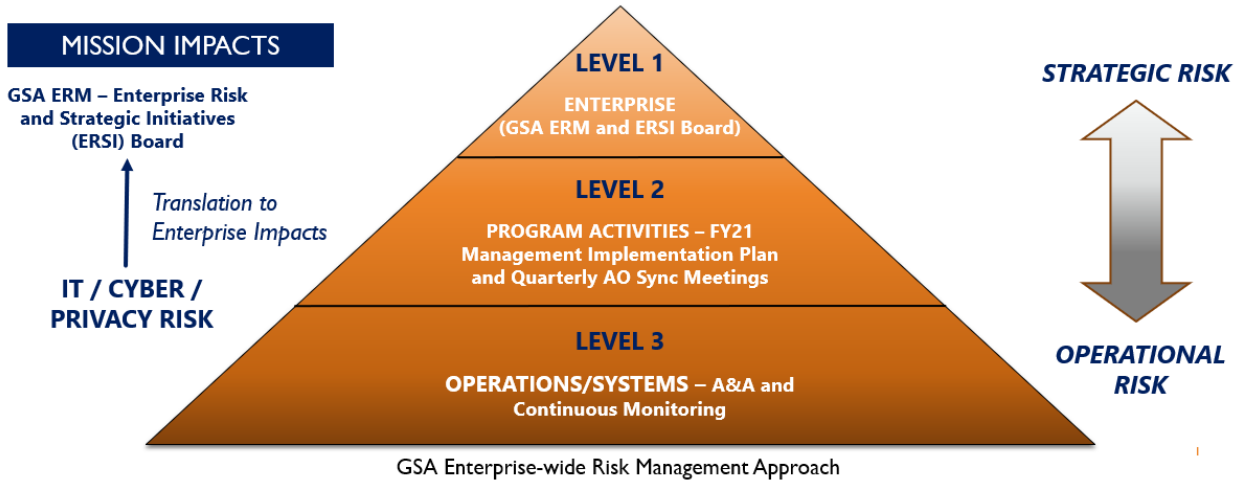

Figure 1. GSA Three-Tiered Risk Management Approach

System/Operations risks and risk management activities are conducted at Level 3 - Operations/System; they form the foundation for GSA's overall Enterprise-wide Risk Management Approach. Information system risks are aggregated with other systems and operational risks and are communicated to GSA Authorizing Officials (AOs) at Level 2 - Program Activities. Complex, interconnected, and distributed enterprise risks to GSA mission delivery identified and addressed at Level 1 - Enterprise, through the GSA Enterprise Risk and Strategic Initiatives (ERSI) Board. The risk management process is carried out seamlessly across the three tiers with the overall objective of continuous improvement in GSA's risk-related activities and effective communication among relevant stakeholders having a shared interest in the mission/business success of the GSA.

Implementation of the security requirements identified herein in FY21 will help ensure continued success in realizing agency goals in managing and protecting information and system resources. The following sections in this guide describe management roles and responsibilities, the required information security activities for FY21, and a feedback loop between the CISO and Authorizing Officials (AO) to keep them informed, on at least a quarterly basis on how well the systems for which they are responsible are performing the required activities.

1.1 Purpose

The purpose of this guide is to gain management agreement with the security milestones, activities, and measures of progress documented herein for implementation in FY21. It supports the implementation of key IT Security measures of progress to gauge performance in meeting requirements from FISMA and other Federal and GSA policies and guidelines. It does not establish new requirements.

Implementation of the security milestones will assist in ensuring the security of GSA information and information system resources and allow the OCISO, AOs, System Owners, Information System Security Managers (ISSMs) and ISSOs the ability to effectively monitor the security posture and maintain cyber hygiene of information system(s) for which they are responsible.

1.2 Scope

GSA employees and contractors with significant security responsibilities as identified in the GSA IT Security Policy are to implement the IT security milestones in this guide for the systems they are responsible to support. All information systems in GSA's FISMA System Inventory are subject to the requirements of this guide based on the Assessment & Authorization (A&A) process under which an authorization to operate (ATO) was granted and the classification of the system as Federal or Contractor per CIO-IT Security-06-30, "Managing Enterprise Cybersecurity Risk." The definitions of Federal and Contractor System from CIO-IT Security-06-30 are provided below.

- **Contractor System.** An information system in GSA's inventory processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor in non-GSA facilities.
- **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.

1.3 Policy

GSA's information security program provides policy and guidance regarding information security for the information and information systems supporting the operations and assets of GSA as required by Federal Laws and regulations. This guide establishes the CISO's performance measures as required by the CISO responsibility below from Chapter 2 of CIO Order 2100.1:

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

1.4 References

- DHS Cybersecurity Directives
- FIPS 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- FIPS 200, "*Minimum Security Requirements for Federal Information and Information Systems*"
- HSPD-12, *"*Homeland *Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors"*
- NIST SP 800-53, Revision 4[1], *"Security and Privacy Controls for Federal Information Systems and Organizations"*
- OMB Circular A-130*, "Managing Information as a Strategic Resource"*
- Privacy Act of 1974 (5 U.S.C. § 552a)
- Public Law 97-255, "*Federal Managers Financial Integrity Act of 1982*"
- Public Law 113-274, "*Cybersecurity Enhancement Act of 2014*"
- Public Law 113-283*, "Federal Information Security Modernization Act of 2014"*
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy"*
- GSA Order CIO 2135.2, "*GSA Policy for Information Technology (IT) Capital Planning and Investment Control (CPIC)"*

[1] NIST SP 800-53, Revision 5, "*Security and Privacy Controls for Information Systems and Organizations*," became final in September 2020 and NIST SP 800-53B, "*Control Baselines for Information Systems and Organizations*," became final in October 2020. This guide remains aligned with Revision 4 and its baselines; the next revision of this guide will be updated to reflect the GSA's alignment with the new NIST guidance.

GSA CIO-IT Security Procedural and Technical Guides and Standards are key in implementing and managing security at GSA. Technical guides and standards are available at the IT Security Technical Guides and Standards InSite page. Non-technical procedural guides are available on the IT Security Procedural Guides page. The procedural guides listed below are key in implementing and managing IT security at GSA.

- GSA CIO-IT Security-01-01, *"Identification and Authentication (IA)"*
- GSA CIO-IT Security-01-02, "*Incident Response (IR)"*
- GSA CIO-IT Security-01-05, "*Configuration Management (CM)"*
- GSA CIO-IT Security-01-07, "*Access Control (AC)*"
- GSA CIO-IT Security-01-08, "*Audit and Accountability (AU)"*
- GSA CIO-IT Security-03-23, "*Termination and Transfer*"
- GSA CIO-IT Security-04-26, "*Federal Information Security Modernization Act (FISMA) Implementation"*
- GSA CIO-IT Security-05-29, "*Security and Privacy Awareness and Role Based Training Program"*
- GSA CIO-IT Security-06-29, "*Contingency Planning (CP)"*
- GSA CIO-IT Security-06-30, "*Managing Enterprise Cybersecurity Risk"*
- GSA CIO-IT Security-06-32, "*Media Protection (MP)"*
- GSA CIO-IT Security-07-35, *"Web Application Security"*
- GSA CIO-IT Security-08-41, "*Web Server Log Review"*
- GSA CIO-IT Security-09-43, *"Key Management"*
- GSA CIO-IT Security-09-44, "*Plan of Action and Milestones (POA&M)"*
- GSA CIO-IT Security-09-48, "*Security and Privacy Requirements for IT Acquisition Efforts"*
- GSA CIO-IT Security-10-50, "*Maintenance"*
- GSA CIO-IT Security-11-51, "*Conducting Penetration Test Exercises"*
- GSA CIO-IT Security-12-63, "*System and Information Integrity (SI)"*
- GSA CIO-IT Security-12-64, "*Physical and Environmental Protection (PE)"*
- 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"*
- GSA CIO-IT Security-18-90, "*Information Security Program Plan (ISPP)"*
- GSA CIO-IT Security-18-91, "*Risk Management Strategy (RMS)*"
- GSA CIO-IT Security-19-95, "*Security Engineering Architecture Reviews*"
- GSA CIO-IT Security-19-101, "*External Information System Monitoring*"

2 Roles and Responsibilities

There are many roles associated with the security of GSA information systems. The complete roles and responsibilities for agency management officials and others with significant IT Security responsibilities are defined fully in Chapter 2 of CIO 2100.1. The following sections identify key responsibilities from CIO 2100.1 related to the management and implementation of security for GSA IT systems. The responsibilities may have been edited or paraphrased to align with this plan.

2.1 Chief Information Security Officer (CISO)

The CISO is the focal point for all GSA IT security and has the following key responsibilities related to implementing and managing IT security for GSA.

- Establishing performance monitoring and quarterly Authorizing Official briefings to ensure activities are performed and deliverables are submitted, reviewed, and approved in accordance with the requirements of this guide.
- Implementing and overseeing GSA's IT Security Program by developing and publishing IT Security Procedural Guides that are consistent with CIO 2100.1.
- Developing and implementing IT security performance metrics to evaluate the effectiveness of technical and non-technical safeguards used to protect GSA information and information systems.
- Assessing IT security measures and goals periodically to assure implementation of GSA policy and procedures.

2.2 Authorizing Officials (AOs)

An AO is the Federal Government management official with the responsibility of authorizing to operate or not to operate an information system, application, or a set of common controls based on assessing the level of risk of their operation. AOs have the following key responsibilities related to implementing and managing IT security for GSA.

- Meeting quarterly with the CISO to ensure System Owners are meeting the timelines for activities and deliverables identified in this guide.
- Ensuring all information systems, applications, or sets of common controls under their purview have a current ATO issued in accordance with (IAW) A&A processes defined in GSA CIO-IT Security-06-30.
- Reviewing and approving deviations to policy and AOR letters as specified in CIO Order 2100.1.
- Reviewing and approving security safeguards of information systems and issuing accreditation statements for each information system under their jurisdiction based on the acceptability of the security safeguards of the system (risk-management approach).
- Ensuring IT systems that handle privacy data meet the privacy and security requirements of the Privacy Act and privacy law and IT information security laws and regulations. This includes GSA Order CIO 2200.1, GSA Order CIO 1878.3, and NIST SP 800-53, Revision 4.
- Supporting the security measures and goals established by the CISO.

2.3 System Owners (SOs)

System Owners are management officials within GSA with responsibility for the acquisition, development, maintenance, implementation, and operation of GSA's IT systems. The System Owner has primary responsibility for managing system risks. System Owners have the following key responsibilities related to implementing and managing IT security for GSA.

- Ensuring all activities and deliverables are completed per the schedules established in this guide.
- Ensuring systems and the data each system processes have necessary security controls in place and are operating as intended and protected IAW GSA regulations and any additional guidelines established by the OCISO and relayed by the ISSO or ISSM.
- Obtaining the resources necessary to securely implement and manage their systems.
- 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.
- Participating in activities related to the A&A of the system to include security planning, risk assessments, security and incident response testing, configuration management (CM), and contingency planning (CP) and testing.
- Obtaining a written ATO following GSA A&A processes prior to making production systems operational and/or Internet accessible. Developing and maintaining the system security plan (SSP) and ensuring that the system is deployed and operated according to the agreed-upon security requirements.
- Working with the ISSO and ISSM to develop, implement, and manage Plan of Action and Milestones (POA&M) for their respective systems IAW GSA CIO-IT Security-09-44, "*Plan of Action and Milestones (POA&M).*"
- Reviewing the security controls for their systems and networks annually as part of the FISMA self-assessment, when significant changes are made to the system and network, and at least every three years or via continuous monitoring if the system is in GSA's information security continuous monitoring program.
- Conducting annual reviews and validations of system users' accounts to ensure the continued need for access to a system and verify users' authorizations (rights/privileges).
- Conducting Privacy Threshold Assessments (PTA) on all systems to ascertain whether the system collects information on individuals or when new systems are developed, acquired, or purchased; performing Privacy Impact Assessments (PIA) when applicable.
- Defining and scheduling software patches, upgrades, and system modifications.
- Supporting the security measures and goals established by the CISO.

2.4 Information Systems Security Officers (ISSOs)

ISSOs are responsible for ensuring implementation of adequate system security for GSA systems. ISSOs are responsible for completing ISSO checklists managed in GSA's implementation of Archer GRC. ISSOs have the following key responsibilities related to implementing and managing IT security for GSA.

- Supporting System Owners to ensure all activities and deliverables are completed per the schedules established in this guide, including reviewing deliverables.
- Ensuring the system is operated, used, maintained, and disposed of IAW documented security policies and procedures. Necessary security controls should be in place and operating as intended.

- Assisting system owners in completing and maintaining the appropriate A&A documentation as specified in GSA CIO-IT Security-06-30, including the usage of Archer GRC.
- Completing the recurring activities in ISSO checklists, completing the checklists in Archer GRC, and submitting the checklists when completed.
- Assisting the AO, Data Owner and Contracting Officer (CO)/Contracting Officer Representative (COR) in ensuring users have the required background investigations, the required authorization and need-to-know, and are familiar with internal security practices before access is granted to the system. Verifying systems not integrated with the GSA ELP (and for logs not sent to the ELP for systems integrated with the ELP) perform log reviews to identify potential security issues.
- Assisting in the identification, implementation, and assessment of a system's security controls, including common controls.
- 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.
- Working with the System Owner and ISSM to develop, implement, and manage POA&Ms for their respective systems IAW GSA CIO-IT Security-09-44.
- Supporting internal and external audits (e.g., FISMA, OIG, GAO, etc.).
- Supporting the security measures and goals established by the CISO.

2.5 Information Systems Security Managers (ISSMs)

ISSMs serve as an intermediary to the system owner and the OCISO Director responsible for ISSO services. ISSMs have the following key responsibilities related to implementing and managing IT security for GSA.

- Coordinating with the System Owners and ISSOs to ensure all activities and deliverables are completed per the schedules established in this guide, including performing reviews of deliverables.
- Providing guidance, advice, and assistance to ISSOs on IT security issues, the IT Security Program, and security policies.
- Ensuring A&A support documentation is developed and maintained for the life of GSA systems, including the usage of GSA's implementation of the Archer GRC solution;
- Reviewing ISSO checklists submitted in Archer GRC and coordinating with ISSOs, as necessary, for systems under their purview.
- Managing system assessments (including A&A package requirements and PCI DSS Report on Compliance [for IT systems that process, store, or transmit payment card data or purchase/credit card numbers]), and forwarding them to the AO and appropriate OCISO Directors.
- Forwarding to the IST Division Director, copies of A&A documents to be signed by the appropriate individuals as required in A&A guidance.
- Working with the ISSO and System Owner to develop, implement, and manage POA&Ms for their respective systems IAW GSA CIO-IT Security-09-44

- Ensures A&A support documentation is developed and maintained.
- Reviews and coordinates reporting of Security Advisory Alerts (SAA), compliance reviews, security training, incident reports, CP testing, and other IT security program requirements.
- Supporting internal and external audits (e.g., FISMA, OIG, GAO, etc.).
- Supporting the security measures and goals established by the CISO.

3 Major Information Security Activities

The tables provided in this guide list security activities by frequency and, where appropriate, designate specific activities as being applicable to Federal or Contractor systems. Light blue shading is used in the tables to highlight activities for Federal systems. CIO Order 2100.1, CIO-IT Security-06-30, and GSA's implementation of NIST SP 800-53, Revision 4 security controls are the primary basis for activity/milestone requirements.

Note: Throughout this guide, security activities related to the ISSO Checklists are from GSA's implementation of Archer GRC. Not every detail in the Archer GRC checklists is replicated in this guide, and since updates to the checklists may occur after publication of this guide the Archer GRC checklists are authoritative for those activities.

3.1 On Demand Information Security Activities

The information security activities in Table 3-1 are mandatory on an on demand, or as required basis, based on specific conditions or triggers for all GSA systems.

Table 3-1. On Demand Security Activities

Security Activity	Activity Description	Condition/ Trigger
Department of Homeland Security (DHS) Binding Operational Directives (BOD) and Emergency Directives (ED) Implementations	DHS develops and oversees the implementation of "binding operational directives" and "emergency directives," which require action to safeguard Federal information and information systems from a known or reasonably suspected information security threat, vulnerability, or risk; protecting the information system from, or mitigating, an information security threat. GSA's Security Operations Division (ISO) collects and reports data on the directives, as necessary. BODs and EDs are compulsory. Federal agencies are required to comply per 44 U.S.C. § 3552 (b)(1)(A)(B)(C) and 44 U.S.C. § 3554 (a)(1)(B)(v)	Timelines established by DHS' Cybersecurity Directives
Incident Reporting	Reporting of cybersecurity incidents is performed by the OCISO. OCISO coordinates with system teams to collect appropriate data as needed.	Cybersecurity incident involving a system
Authorization of User Accounts/Access for Systems	System Owners authorize user access to their systems when a user account is initially created with associated access privileges.	Creation of a user account (privileged or non-privileged)
ATO POA&M Reviews	GSA's OCISO Policy and Compliance Division (ISP) reviews a system's POA&M whenever an ATO Letter is issued.	ATO is issued (New or Renewal)
Audit Log Reviews	Systems not integrated with the Enterprise Logging Platform (ELP) and logs not sent to the ELP (i.e., database, application, tool logs), the system owner maintains the responsibility of reviewing information system logs per their SSP and maintaining a log that such a review has taken place. Database, application, and tool logs are only required to be reviewed if PII or sensitive data (e.g., financial, CUI) is in scope.	As specified in the system's SSP

Security Activity	Activity Description	Condition/ Trigger
Review Vulnerability Scan Reports	Vulnerability scans occur as follows: ● Weekly authenticated scans for operating systems (OSs) ● Monthly unauthenticated scans for web applications ● Annual authenticated scans for web applications Although acknowledgement of scan reviews is included in the ISSO checklists, the timeframes for remediation (see below) can only be met by more frequent reviews. **For Internet-accessible IP addresses** (a) Any Critical (Very High) scan vulnerabilities must be remediated within 15 days. (b) Any High scan vulnerabilities must be remediated within 30 days. (c) Any Moderate scan vulnerabilities must be remediated within 90 days. **For all other assets** (a) Any Critical (Very High) and High scan vulnerabilities must be remediated within 30 days. (b) Any Moderate scan vulnerabilities must be remediated within 90 days.	Weekly to ensure remediation timelines can be met
Conduct Security Impact Analysis of Changes	Assist in performing security impact analyses and supporting the CM approval process.	If analysis is requested
Audit/Independent Assessment Support	If selected for an audit or independent assessment (e.g., DHS HVA assessment), the ISSO/ISSM, System Owner, and system personnel (e.g., system administrators) complete a pre-audit checklist and provide support through the audit cycle.	If selected for audit or assessment

3.2 Monthly Information Security Milestones/Activities

Table 3-2. Monthly Security Activities

Security Activity	Activity Description	Due Dates
Federal Systems		
Completion of the Monthly Federal ISSO Checklist	Using Archer GRC, ISSOs for Federal Systems will complete the checklist, including providing evidence as necessary. Checklist items include: ● Verifying review of OS vulnerability scans and identifying actions taken. ● Verifying review of unauthenticated web application vulnerability scans and identifying actions taken. ● Verifying review of configuration compliance scans/approved deviations for non-compliance settings. ● Determining if any security impact analyses were performed. ● Verifying review/update of system inventories.	25th of each month Note: Monthly ISSO Checklists are made available on the 1st of each month; ISSM reviews are due the 10th of the following month.
Review OS Vulnerability Scans	Review OS vulnerability scans and identify actions taken.	By the 25th of each month
Review Unauthenticated Web Application Vulnerability Scans	Review unauthenticated web application vulnerability scans and identify actions taken.	By the 25th of each month
Review Configuration Compliance Scans/Approved Deviations	Review configuration compliance scans/approved deviations for non-compliance settings.	By the 25th of each month
Assist in Security Impact Analysis (as requested)	Identify if assistance for security impact analyses was requested and performed.	By the 25th of each month
Review/Update System Inventories	Review/update of system inventories.	By the 25th of each month
Disable/delete Accounts of Separated GSA Employees/Contractors	Each month upon receipt of the Separations Report, ISSOs review the report to verify accounts for separated users on their systems have been disabled or deleted, as appropriate.	Within 30 days of receipt of report.

3.3 Quarterly Information Security Milestones/Activities

Table 3-3. Quarterly Security Activities

Security Activity	Activity Description	Due Dates
All Systems		
FISMA Quarterly Metric Reports	Each quarter ISP captures ATO metrics and coordinates, as necessary, with ISSOs/ISSMs the collection of data regarding FISMA systems. ISP coordinates with other Divisions and GSA components to collect additional FISMA reportable data.	Q1 - 1/15/2021 Q2 - 4/16/2021 Q3 - 7/16/2021 Q4 - 9/15/2021
Federal Systems		
Completion of the Quarterly Federal ISSO Checklist	Using Archer GRC, ISSOs will complete the checklist, including providing evidence as necessary. Checklist consists of: ● Verifying the system POA&M has been updated and submitted for the quarter. ● Verifying that any unnecessary functions, ports, protocols, and services have been eliminated.	Q1 - 12/25/2020 Q2 - 3/25/2021 Q3 - 6/25/2021 Q4 - 9/25/2021 Note: Quarterly ISSO Checklists are made available on the 1st of the month they are due; ISSM reviews are due the 10th of the following month.
Update the POA&M	Update and submit the POA&M.	Q1 - 12/25/2020 Q2 - 3/25/2021 Q3 - 6/25/2021 Q4 - 9/25/2021
Review Functions, Ports, Protocols, and Services	Review functions, ports, protocols, and services; eliminate any that are unnecessary.	Q1 - 12/25/2020 Q2 - 3/25/2021 Q3 - 6/25/2021 Q4 - 9/25/2021

Security Activity	Activity Description	Due Dates
Contractor Systems		
Completion of the Quarterly Contractor ISSO Checklist	Using Archer GRC, ISSOs will complete the checklist, including providing evidence as necessary. Checklist consists of: ● Verifying OS (including databases) vulnerability scans have been performed and delivered to the government. ● Verifying web application scans have been performed and delivered to the government. ● Verifying the system POA&M has been updated and submitted.	Q1 - 12/25/2020 Q2 - 3/25/2021 Q3 - 6/25/2021 Q4 - 9/25/2021 Note: Quarterly ISSO Checklists are made available on the 1st of the month they are due; ISSM reviews are due the 10th of the following month.
Review OS Vulnerability Scans	Review OS vulnerability scans and identify actions taken.	Q1 - 12/25/2020 Q2 - 3/25/2021 Q3 - 6/25/2021 Q4 - 9/25/2021
Review Unauthenticated Web Application Vulnerability Scans	Review unauthenticated web application vulnerability scans and identify actions taken.	Q1 - 12/25/2020 Q2 - 3/25/2021 Q3 - 6/25/2021 Q4 - 9/25/2021
Update the POA&M	Update and submit the POA&M.	Q1 - 12/25/2020 Q2 - 3/25/2021 Q3 - 6/25/2021 Q4 - 9/25/2021

3.4 Semiannual Ongoing Authorization (OA) System Program Management Reviews (PMRs)

Table 3-4. Semiannual OA Security Activities

Security Activity	Activity Description	Due Dates

Ongoing Authorization (OA) System Program Management Reviews (PMR)	For systems in OA, ISP, ISSOs, and ISSMs will collaborate on the following metrics as described in GSA CIO-IT Security-12-66, "*Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program"*.
	
	● Inventory of hardware assets
	● Inventory of software assets
	● Configuration settings
	● Vulnerability management
	  ○ OS (including databases) and web application vulnerability scans
	  ○ AORs
	● OS logs integrated with the ELP
	● POA&Ms updated
	● Annual Deliverables
	  ○ FISMA Self-Assessment, if applicable
	  ○ SSP updated
	  ○ Penetration Test, if applicable
	  ○ CM Plan updated, if applicable
	  ○ CP Test
	  ○ PTA/PIA updated
	  ○ User recertification
	● Showstopper Controls Status
		3/31/2021 and 10/29/2021

3.5 Annual Information Security Milestones/Activities

Table 3-5. Annual Security Activities

Security Activity	Activity Description	Due Dates
Federal Systems		
Completion of the Annual Federal ISSO Checklist	Using Archer GRC, ISSOs will complete the checklist, including providing evidence as necessary. Checklist consists of: ● Verifying review of authenticated web application vulnerability scans and identifying actions taken. ● Verifying a penetration test exercise has been completed, if necessary. ● Verifying, if applicable, the systems FISMA self-assessment has been completed. ● Verifying, if applicable, all interconnection security agreements have been updated. ● Verifying the SSP has been updated. ● Verifying the PTA or PIA, as applicable, has been updated. ● Verifying the review of the incident response plan and updating, if necessary. ● Verifying the security incident response capability testing has been completed. ● Verifying the review of the contingency/continuity plan and updating, if necessary. ● Verifying the annual user recertification process has been completed.	7/31/2021 Note: Annual ISSO Checklists will be made available on 1/4/2021; ISSM reviews are due within 4 weeks of completion or 8/13/2021
Review Authenticated Web Application Vulnerability Scans	Review authenticated web application vulnerability scans and identify actions taken.	7/31/2021
Review Penetration Test Results (if applicable)	Review penetration test results (if applicable) and identify actions taken.	7/31/2021
Complete FISMA Self-Assessment (if applicable)	Complete FISMA self-assessment (if applicable).	7/31/2021
Review/Update Interconnection Security Agreements (if applicable)	Review and update Interconnection security agreements (if applicable).	7/31/2021
Review/Update System Security Plan	Review and update System Security Plan.	7/31/2021
Review/Update PTA and PIA (if applicable)	Review and update PTA and PIA (if applicable).	7/31/2021
Review/Update Incident Response Plan	Review and update Incident Response Plan.	7/31/2021

Security Activity	Activity Description	Due Dates
Complete Incident Response Test	Complete incident response capability test.	7/31/2021
Review/Update Contingency/Continuity Plan	Review and update Contingency/Continuity Plan.	7/31/2021
Complete Contingency/Continuity Plan Test	Complete contingency/continuity plan test.	7/31/2021
Review/Update User Account Recertification	Review and update user accounts for the system.	7/31/2021

Security Activity	Activity Description	Due Dates
Contractor Systems (*denotes item eligible for Self-Attestation)		
Completion of the Annual Contractor ISSO Checklist	Using Archer GRC, ISSOs will complete the checklist, including providing evidence as necessary. Checklist consists of: ● Verifying a penetration test report has been completed and delivered to the government. ● Ensuring if applicable the systems FISMA self-assessment has been completed and uploaded. ● Verifying the review of the CP, and delivery to the government. ● Verifying the results, and delivery of the security awareness training for all employees and contractors that support the operation of the system. ● Verifying a well-defined, documented, and up-to-date baseline configuration has been provided. ● Verifying an incident response test report has been completed and delivered to the government. ● Ensuring all internet security agreements have been updated and delivered to the government. ● Verifying the SSP has been delivered to the government. ● Verifying the rules of behavior has been reviewed and/or updated for the current year. ● Verifying that the results of the annual review and validation of system users' accounts have been provided to the government. ● Verifying the CM plan has been delivered to the government. ● Verifying the separation of duties matrix has been reviewed and updated as necessary. ● Ensuring documentation reflecting favorable adjudication of background investigations for all personnel supporting the system has been provided. ● Ensuring OS configuration compliance scan reports have been delivered showing compliance against the documented configuration settings.	7/31/2021 Note: Annual ISSO Checklists will be made available on 1/4/2021; ISSM reviews are due within 4 weeks of completion or 8/31/2021

Security Activity	Activity Description	Due Dates
Review Penetration Test Results (if applicable)	Review Penetration Test results (if applicable) and identify actions taken.	7/31/2021
Complete FISMA Self-Assessment (if applicable)	Complete the FISMA self-assessment (if applicable).	7/31/2021
Review/Update Contingency/Continuity Plan	Review/update the Contingency/Continuity Plan.	7/31/2021
Review Contingency/ Continuity Plan Test Report	Review Contingency/Continuity Plan test report.	7/31/2021
***Review Results of Security Awareness Training**	Review the results of the annual security awareness training.	7/31/2021
***Review/Update Baseline Configuration Document**	Review/update the baseline configuration document.	7/31/2021
Review Incident Response Test	Review the incident response test report.	7/31/2021
Review/Update Interconnection Security Agreements (if applicable)	Review/update Interconnection Security Agreements (if applicable).	7/31/2021
Review/Update System Security Plan	Review/update the System Security Plan.	7/31/2021
Review/Update Rules of Behavior	Review/update the Rules of Behavior.	7/31/2021
Review/Update User Account Recertification	Review/update the certification of user accounts requiring access to the system.	7/31/2021
Complete Configuration Management Plan	Review/update the Configuration Management Plan.	7/31/2021
***Review/Update Separation of Duties Matrix**	Review and update the Separation of Duties Matrix.	7/31/2021
***Review/Update Personnel Background Investigations**	Review/update documentation reflecting personnel supporting the system have appropriate background investigations.	7/31/2021
Review/Update Operating System Configuration Compliance Scans	Review configuration compliance scans/approved deviations for non-compliance settings.	7/31/2021

3.6 Biennial Information Security Milestones/Activities

Table 3-6. Biennial Security Activities

Security Activity	Activity Description	Due Dates
Contractor Systems (all biennial items are eligible for Self-Attestation)		
Completion of the Biennial Contractor ISSO Checklist	Using Archer GRC, ISSOs will complete the checklist, including providing evidence as necessary. Checklist consists of:	Not Applicable See Note below.

Security Activity	Activity Description	Due Dates
	● Verifying the following policies and procedures have been reviewed, and updated as necessary: ○ Maintenance ○ System and Information Integrity ○ System and Communication Protection ○ Security Awareness and Training ○ Incident Response ○ Access Control ○ Audit and Accountability ○ Identification and Authentication ○ Key Management ○ Media Protection ○ Personnel Security ○ Physical and Environmental	
Review/Update Maintenance Policies	Review/Update the Maintenance Policies.	Not Applicable See Note below.
Review/Update System and Information Integrity Policies	Review/Update the System and Information Integrity Policies.	Not Applicable See Note below.
Review/Update System and Communication Protection Policies	Review/Update the System and Communication Protection Policies.	Not Applicable See Note below.
Review/Update Security Awareness and Training Policies	Review/Update the Security Awareness and Training Policies.	Not Applicable See Note below.
Review/Update Incident Response Policies	Review/Update the Incident Response Policies.	Not Applicable See Note below.
Review/Update Access Control Policies	Review/Update the Access Control Policies.	Not Applicable See Note below.
Review/Update Audit and Accountability Policies	Review/Update the Audit and Accountability Policies.	Not Applicable See Note below.
Review/Update Identification and Authentication Policies	Review/Update the Identification and Authentication Policies.	Not Applicable See Note below.
Review/Update Key Management Policies	Review/Update the Key Management Policies.	Not Applicable See Note below.
Review/Update Media Protection Policies	Review/Update the Media Protection Policies.	Not Applicable See Note below.
Review/Update Personnel	Review/Update the Personnel Security Policies.	Not Applicable

Security Activity	Activity Description	Due Dates
Security Policies		See Note below.
Review/Update Physical and Environmental Policies	Review/Update the Physical and Environmental Policies.	Not Applicable See Note below.

Note: Biennial ISSO Checklists are only issued in even numbered years.

4 Measures of Progress

Although the activities in this guide identify what should be done, a continuous feedback mechanism is also required to inform AOs how well the systems under their purview are performing to the established due dates/measures. The OCISO will conduct quarterly briefings with AOs to report on the implementation status of their systems. The briefings will provide a practical tool with which AOs can gauge the effectiveness of their information security arrangements and assess how well their systems are performing. The AO Briefings are open to others the AO or CISO wish to attend such as IS Directors, System Owners, and Program and Project Managers.

Table 4-1 lists the security measures that will be included in the AO quarterly briefings and the goal for each measure.

Table 4-1. Security Measures and Goals

Security Measure	Description	Goal
AORs	AORs with dates and status (High/Critical)	No expired AORs or overdue actions
ATO Conditions	ATO conditions with dates and status	No overdue ATO conditions.

Security Measure	Description	Goal
Showstopper Controls	Listing of High/Critical risk showstopper controls either not fully satisfied or without a POA&M/AOR. ● Multi-Factor Authentication (MFA) for Privileged & User-level access ● Critical and High vulnerabilities remediated within established timeframes ● Remote Code Execution (RCE) vulnerabilities ● End-of-Life (EOL) Software ● System Architecture approved by ISE ● Integration with GSA's Security Stack (Internal Systems) ● Encryption of Sensitive Data (i.e., PII, PCI, Authenticators)	All showstopper controls are implemented or have a POA&M/AOR. Note: Additional details about the Showstopper controls are available in CIO-IT Security-06-30, "*Managing Enterprise Cybersecurity Risk*."
ATO Status	% of FISMA systems with a current ATO IAW GSA policy and guidance	100%
Audit Findings	Listing of audit findings (e.g., OIG, GAO, Financial) with POA&Ms; number with overdue milestones	All audit findings have POA&Ms; no overdue milestones.
POA&Ms	Number of POA&Ms delayed beyond scheduled completion date; Number of High Risk POA&Ms delayed 30 days beyond scheduled completion date; Number of Moderate Risk POA&Ms delayed 90 days beyond scheduled completion date.	<5% of open POA&Ms; 0 High > 30 days; 0 Moderate > 90 days.

4.1 AO Briefing Schedule

AO briefings for FY21 will be arranged with each AO. In general, the briefings will occur within one month after the end of the quarter. The briefings will provide an opportunity to engage in dialogue around key security measures and goals as defined in Table 4.1; discuss any major modernization efforts impacting security or ATOs; and discussion of any relevant threats applicable to the ACIO's portfolio of systems. The AO Briefings are open to others the AO or CISO wish to attend such as IS Directors, System Owners, and Program and Project Managers.

The briefings integrate into GSA's broader enterprise risk management approach, tracking risks at the organization level; mission/business process level; and at the information system level.

System and program risks that are or have the potential to become more complex, interconnected, and distributed enterprise risks with the potential to impact GSA mission delivery; requiring more strategic coordination, or resourcing will be elevated to the GSA ERSI Board.

Appendix A - Systems with Expiring ATOs in FY21

The information in this table is as of the date this document was published. The renewal dates will be impacted as systems are decommissioned, transferred, or extended.

Responsible Org/System Name	ATO Date	Renewal Date
Federal Acquisition Services (Q)		
Federal Procurement Data System (FPDS)	2/26/2021	5/3/2021
Federal Public Key Infrastructure (FPKI)	11/5/2020	5/5/2021
Verizon MTIPS	6/28/2018	6/28/2021
Touchpoints (TP)	3/22/2021	6/30/2021
Tock	7/3/2018	7/3/2021
Federalist	2/25/2021	7/6/2021
SmartPay - Citibank	2/12/2021	7/19/2021
GSA Federal Government Managed Lodging Program (Fedrooms)	7/26/2018	7/26/2021
Data.gov	3/22/2021	7/31/2021
System for Award Management (SAM)	7/30/2020	7/31/2021
Federal Relay Service (FRS)	8/6/2018	8/6/2021
Order Management System (OMS)	10/31/2019	8/9/2021
Contracts Awarded Labor Category 2.0 (CALC)	12/14/2020	9/30/2021
GSA IT - Office of Acquisition IT Services (IQ)		
ClearPath	3/31/2020	4/15/2021
Oasis Discovery Market Tool Research (Discovery)	4/30/2018	4/30/2021
GSA Enhanced Checkout (GECO)	3/24/2021	5/14/2021
Sales Automation System (SASy)	9/14/2020	6/25/2021
eOffer	3/17/2021	7/30/2021
SmartPay - Data Warehouse	8/20/2020	9/7/2021
Steps to Performance Based Acquisition (SPBA)	2/2/2021	9/30/2021
GSA IT - Office of Corporate IT Services (IC)		
eRulemaking	12/16/2020	4/30/2021
GSAJOBS	1/25/2021	5/31/2021
Enterprise RPA Platform (ERPA)	6/17/2020	6/19/2021
Enterprise Content Application Services II (ECAS II)	6/24/2020	6/24/2021
ePayroll (PAR)	8/22/2019	9/19/2021
GSA Online University (GSAOLU)	9/28/2020	9/28/2021
GSA IT - Office of Public Building IT Services (IP)		
GSA Enterprise Physical Access Control System (EPACS)	5/31/2018	5/31/2021
BI Framework	3/25/2021	9/30/2021
Office of GSA IT (I)		
Security Tools (SecTools)	4/27/2018	4/27/2021
IT Dashboard (ITDB)	6/16/2020	6/16/2021
Enterprise Call Center (CTL)	8/2/2020	8/1/2021
Data to Decisions (D2D)	9/14/2018	9/14/2021