
# IT Security Procedural Guide: FY24 IT Security Program Management Implementation Plan CIO-IT Security-08-39

**Revision 11**

November 13, 2023

*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:<br>• Summarized previous revision descriptions.<br>• Updated guide to current GSA processes, timelines, and guidance.<br>• Updated to current guide formatting and style. | Re-establishing guide for FY21. | Throughout |
| | | **Revision 9 – April 6, 2022** | | |
| 1 | Dean, Klemens | Changes include:<br>• Updated Authorizing Officials.<br>• Updated vulnerability mediation timelines to align with NIST SP 800-53 control parameters for RA-5 and SI-2(3).<br>• Updated dates for FISMA Quarterly Reports and POA&Ms.<br>• Updated Showstopper list.<br>• Added FISMA Self-assessments to AO Sync Meeting metrics. | FY22 Update | Throughout |

| Change Number | Person Posting Change | Change | Reason for Change | Page Number of Change |
|---|---|---|---|---|
| | | **Revision 10 – January 30, 2023** | | |
| 1 | Berlas, Desai, Klemens | Changes include:<br>• Updated Authorizing Officials.<br>• Added Responsibility for each activity.<br>• Updated activity descriptions for select activities.<br>• Added Static Code Analysis to monthly checklist<br>• Added HVA Data Call to annual activities.<br>• Added PTA/PIA review/update to Contractor annual activities.<br>• Added SCRM Plan review/update to Contractor annual activities.<br>• Added SCRM Policies and procedures review/update to Biennial checklist.<br>• Updated dates to reflect current year guidance, including two dates for annual activities with an exception noted for contractor systems.<br>• Updated format, edited. | FY23 Update | Throughout |
| | | **Revision 11 – November 13, 2023** | | |
| 1 | Normand, McCormick, Klemens | • Updated PTA/PIA guidance.<br>• Updated due dates for various activities.<br>• Added Static Code Analysis to Contractor activities per applicability of SA-11(1).<br>• Added Red Team exercise requirements.<br>• Added Privacy Analyst in Roles and Responsibilities.<br>• Edited and formatted to align with current GSA guidance. | FY24 Update | Throughout |

# CONCURRENCE

DocuSigned by:
David Shive
A3AE4284A2754E9...

David Shive, Authorizing Official
GSA Chief Information Officer

DocuSigned by:
Philip Klokis
6E8E4C8418E2469...

Phillip Klokis, Authorizing Official
Public Building IT Services (IP)

DocuSigned by:
April Kestyn
3D6BC257BDAC4FE...

Sagar Samant, Authorizing Official
Acquisition IT Services (IQ)

DocuSigned by:
Elizabeth DelNegro
70F7CFD8F9654DA...

Elizabeth DelNegro, Authorizing Official
Corporate IT Services (IC)

DocuSigned by:
Ann Lewis
11CE699C3B8A4E9...

Ann Lewis, Authorizing Official
Technology Transformation Services (TTS)

DocuSigned by:
41786C5520FC42C...

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

## Approval

IT Security Procedural Guide: FY24 IT Security Program Management Implementation Plan, CIO-IT Security 08-39, Revision 11, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161644F...

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:** Hyperlinks in running text will be provided if they link to a location within this document or to an external source unless the source is GSA policies or guides, in which case a link to that web page will be provided on the first reference in the text.

# 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, "Managing Information as a Strategic Resource," 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 CISO (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 Fiscal Year 2024 (FY24) 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 aide 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.

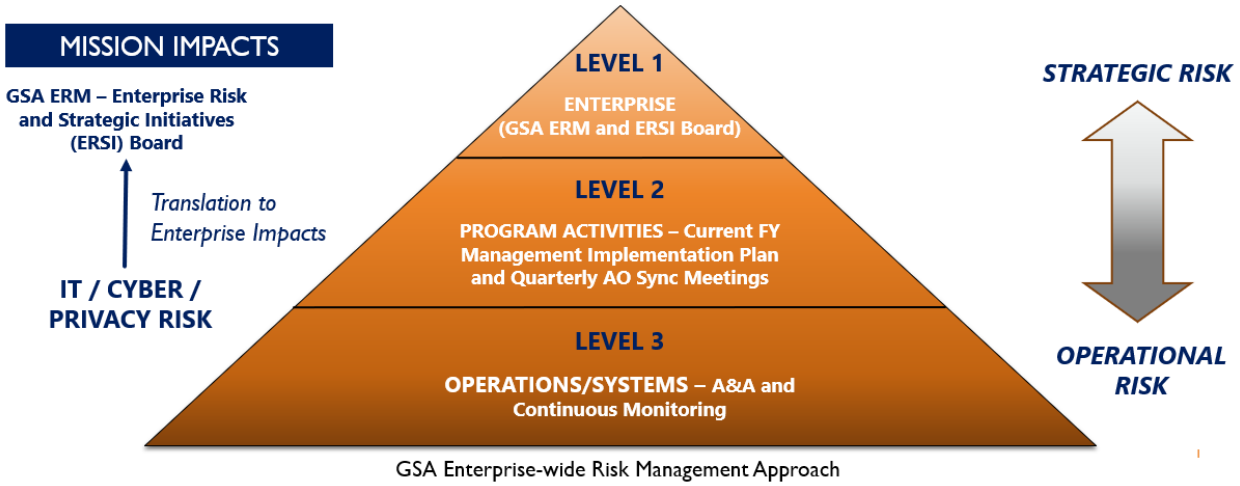


**Figure 1. GSA Three-Tiered Risk Management Approach**

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 FY24 will help ensure continued success in realizing agency goals in managing and protecting information and system resources. This guide identifies management roles and responsibilities (see Appendix B), the required information security activities for FY24, and a feedback loop between the CISO and AOs 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 FY24. 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 system resources and allow the OCISO, AOs, System Owners, Information System Security Managers (ISSMs) and Information System Security Officers (ISSOs) the ability to effectively monitor the security posture and maintain cyber hygiene of systems 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 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 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 2100.1:

> "Implementing IT security performance measures to evaluate the effectiveness of technical and non-technical safeguards protecting GSA information and information systems."

### 1.4 References

Appendix A provides links to references used throughout this guide.

## 2 Roles and Responsibilities

There are many roles associated with the security of GSA information systems. Appendix B provides a listing of roles and responsibilities related to the management and implementation of security for GSA IT systems.

## 3 Major Information Security Activities

The tables provided in this section list security activities by frequency and, where appropriate, designate specific activities as being applicable to Federal or Contractor systems. CIO 2100.1, CIO-IT Security-06-30, and GSA's implementation of NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," security controls are the primary basis for activity/milestone requirements. Additional information regarding activities designated for contractor systems is included in CIO-IT Security-19-101: External Information System Monitoring. The System Owner is responsible for ensuring that the activities listed in the tables are performed in coordination with the system's ISSM and ISSO. In each table the position/role, team, or group responsible for performing the activity is identified.

**Note:** Throughout this guide, security activities related to the ISSO Checklists are from GSA's implementation of the Archer Governance, Risk, and Compliance (GRC) solution. Not every detail in GSA's Archer GRC ISSO checklists is replicated in this guide, and since updates to the checklists may occur after publication of this guide the Archer GRC ISSO 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 |
|---|---|---|
| | **All Systems** | |
| **Department of Homeland Security (DHS) Cybersecurity & Infrastructure Agency (CISA) Binding Operational Directive (BOD), Cybersecurity Coordination, Assessment, and Response (C-CAR) protocol, and Emergency Directive (ED) adherence**<br><br>**Responsibility: System Owner/Team** | CISA develops and oversees the implementation of BODs, C-CARs, and EDs 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.<br><br>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 CISA's Cybersecurity Directives |
| **Incident Reporting**<br><br>**Responsibility: System Team and Incident Response Team** | 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**<br><br>**Responsibility: System Owner/Designee per System Security and Privacy Plan (SSPP)** | System Owners or designated representatives, as specified in the SSPP, 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 Plan of Action and Milestones (POA&M) Reviews**<br><br>**Responsibility: ISP POA&M Team** | GSA's OCISO Policy and Compliance Division (ISP) reviews a system's POA&M whenever an ATO Letter is issued. | ATO is issued |
| **Audit Log Reviews**<br><br>**Responsibility: System Owner/Team** | Systems must perform audit log reviews and document the performance of the reviews as specified in CIO-IT Security-01-08: Audit and Accountability (AU) and the system's SSPP. | As specified in the system's SSPP |

| Security Activity | Activity Description | Condition/ Trigger |
|---|---|---|
| **Review Vulnerability Scan Reports (e.g., Operating system, Web Application)**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | Vulnerability scans occur as specified in CIO-IT Security-17-80: Vulnerability Management Process and the 06-30 Scanning Parameter Spreadsheet<br><br>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.<br><br>**Vulnerabilities Remediation Timelines:**<br>**(1) BOD Timelines**<br>(a) Within 14 days for vulnerabilities added to CISA's Known Exploitable Vulnerabilities (KEV) Catalog with a (Common Vulnerabilities and Exposures) CVE date post FY21.<br>(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.<br>(c) Within 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.<br>**(2) GSA Standard Timelines**<br>(a) Within 30 days for Critical (Very High) and High vulnerabilities.<br>(b) Within 90 days for Moderate vulnerabilities.<br>(c) Within 120 days for Low vulnerabilities for Internet-accessible systems/services. | Weekly to ensure remediation timelines can be met |
| **Conduct Impact Analysis of Changes**<br><br>**Responsibility:**<br>**ISSO, ISSM, and System Team coordination per Configuration Management (CM) Plan** | Assist in analyzing changes to the system to determine potential security and privacy impacts prior to change implementation. | As needed for significant changes |
| **Audit/Independent Assessment Support**<br><br>**Responsibility:**<br>**System Owner/Team, ISSM, ISSO** | If selected for an audit or independent assessment (e.g., DHS High Value Asset [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 |
| **Identity, Credential, and Access Management (ICAM) Portfolio Review**<br><br>**Responsibility:**<br>**System Owner/Team and ICAM Team** | In accordance with CIO 2183.1, "Enterprise Identity, Credential, and Access Management (ICAM) Policy," all new or modernizing GSA applications must have their ICAM capabilities reviewed and approved by the ICAM Portfolio prior to production usage. | New or modernizing applications that include users |

## 3.2 Monthly Information Security Milestones/Activities

There are no specific monthly contractor system security milestones. However, for all systems, reviews of vulnerability scans must be performed at least weekly as described in the on demand/as required table in order to meet remediation timelines. The monthly checklist requirement is a verification that reviews have occurred and does not imply that vulnerability scans can only be reviewed monthly.

**Table 3-2. Monthly Security Activities**

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **Federal Systems** | | |
| **Completion of the Monthly Federal ISSO Checklist***<br><br>**Responsibility:**<br>**ISSO completion, ISSM approval** | Using Archer GRC, ISSOs for Federal Systems will complete the checklist, including providing evidence as necessary. Checklist items include:<br><br>● Verifying review of OS vulnerability scans and identifying actions taken.<br>● Verifying review of unauthenticated web application vulnerability scans and identifying actions taken.<br>● Verifying review of configuration compliance scans/approved deviations for non-compliance settings.<br>● Verifying static code analysis was performed (as applicable).<br>● Determining if any security impact analyses were performed.<br>● Verifying review/update of system inventories. | 25th of each month<br><br>Note: Monthly ISSO Checklists are made available on the 1st of each month; ISSM reviews are due the 10th of the following month, or modified deadlines as determined by the CISO. |
| **Review OS Vulnerability Scans**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | ISSO reviews the OS vulnerability scans and identifies actions taken. | By the 25th of each month |
| **Review Unauthenticated Web Application Vulnerability Scans**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | ISSO reviews unauthenticated web application vulnerability scans and identifies actions taken. | By the 25th of each month |
| **Review Configuration Compliance Scans/Approved Deviations**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | ISSO reviews configuration compliance scans/approved deviations for non-compliance settings. | By the 25th of each month |

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **Static Code Analysis**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO verifies that static code analysis was performed prior to code base changes being placed into production, as applicable for the month.<br><br>**Applicability:** FIPS 199 High and Moderate**, Limited ATO (LATO), and Moderate Software-as-a-Service (MiSaaS) systems.<br>**all software except closed-source COTS | By the 25th of each month |
| **Assist in Security Impact Analysis (as requested)**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | Identify if assistance for security impact analyses was requested and performed. | By the 25th of each month |
| **Review/Update System Inventories**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews updates of FISMA system inventories. | By the 25th of each month |
| **Verify Personnel on the Separation Report have had Accounts Disabled/Deleted**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | 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. |

*Due to Holidays, December checklist dates are: Submission-December 28th, Review-January 12th

## 3.3 Quarterly Information Security Milestones/Activities

Reviews of vulnerability scans must be performed at least weekly as described in the on demand/as required table in order to meet remediation timelines. The quarterly checklist requirement for Contractor systems is a verification that reviews have occurred and does not imply that vulnerability scans can only be reviewed quarterly. Similarly, POA&Ms and Acceptance of Risk Letters (AORs) have timelines and update frequencies that could be at any time during a week, month, or quarter, the checklist activity is verification that such updates have taken place during the quarter, not once a quarter.

### Table 3-3. Quarterly Security Activities

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| | **All Systems** | |
| **FISMA Quarterly Metric Reports**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | 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 - 01/12/2024<br>Q2 - 04/05/2024<br>Q3 - 07/05/2024<br>Q4 - 10/07/2024 |
| | **Federal Systems** | |
| **Completion of the Quarterly Federal ISSO Checklist***<br><br>**Responsibility: ISSO completion, ISSM approval** | Using Archer GRC, ISSOs will complete the checklist, including providing evidence as necessary. The checklist consists of:<br><br>● Verifying the system POA&M has been updated and submitted for the quarter.<br>● Verifying AOR Letters have been reviewed and re-issued, as necessary. | Q1 - 12/28/2023<br>Q2 - 03/25/2024<br>Q3 - 06/25/2024<br>Q4 - 09/25/2024<br><br>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, or modified deadlines as determined by the CISO. |
| **Update the POA&M**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO updates and submits the POA&M. | Q1 - 12/01/2023<br>Q2 - 03/01/2024<br>Q3 - 06/03/2024<br>Q4 - 09/03/2024 |
| **Update AORs (if applicable)**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO performs quarterly reviews and makes necessary updates to AORs due in the quarter. Updates and re-issues AOR Letters, as applicable. | Q1 - 12/01/2023<br>Q2 - 03/01/2024<br>Q3 - 06/01/2024<br>Q4 - 09/01/2024 |

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| | **Contractor Systems** | |
| **Completion of the Quarterly Contractor ISSO Checklist***<br><br>**Responsibility:**<br>**ISSO completion, ISSM approval** | Using Archer GRC, ISSOs will complete the checklist, including providing evidence as necessary. The checklist consists of:<br><br>● Verifying operating system (OS) (including databases) vulnerability scans have been performed and delivered to the government.<br>● Verifying web application scans have been performed and delivered to the government.<br>● Verifying static code analysis was performed, as applicable.<br>● Verifying the system POA&M has been updated and submitted. | Q1 - 12/28/2023<br>Q2 - 03/25/2024<br>Q3 - 06/25/2024<br>Q4 - 09/25/2024<br><br>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, or modified deadlines as determined by the CISO. |
| **Review OS Vulnerability Scans**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | ISSO reviews OS vulnerability scans and identifies actions taken. | Q1 - 12/28/2023<br>Q2 - 03/25/2024<br>Q3 - 06/25/2024<br>Q4 - 09/25/2024 |
| **Review Unauthenticated Web Application Vulnerability Scans**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | ISSO reviews web application vulnerability scans and identifies actions taken. | Q1 - 12/28/2023<br>Q2 - 03/25/2024<br>Q3 - 06/25/2024<br>Q4 - 09/25/2024 |
| **Static Code Analysis, if applicable**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | ISSO verifies that static code analysis was performed prior to code base changes being placed into production, as applicable for the quarter.<br><br>**Applicability:** FIPS 199 High and Moderate**, Limited ATO (LATO), and Moderate Software-as-a-Service (MiSaaS) systems.<br>**all software except closed-source COTS | Q1 - 12/28/2023<br>Q2 - 3/25/2024<br>Q3 - 6/25/2024<br>Q4 - 9/25/2024 |
| **Update the POA&M**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | ISSO updates and submits the POA&M. If POA&Ms are associated with AORs, review and re-issue AORs, as applicable. | Q1 - 12/01/2023<br>Q2 - 03/01/2024<br>Q3 - 06/03/2024<br>Q4 - 09/03/2024 |

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **Reducing the Significant Risk of Known Exploitable Vulnerabilities (BOD 22-01)**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | Vendors are required to update their vulnerability management procedures in accordance with BOD 22-01.<br><br>● Subscribe to CISA KEV Catalog automated updates;<br>● Remediate vulnerabilities identified in the KEV within 14 days of addition;<br>● Provide within 7 days from the required remediation date an email to the ISSO/ISSM or Contracting Officer Representative (COR) certifying remediation consistent with BOD 22-01 requirements supported with clean authenticated scan reports. | As KEV Catalog is published, 14 days +7 days |

*Due to Holidays, December checklist dates are: Submission-December 28th, Review-January 12th

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

The OA semiannual reviews listed in Table 3-4 are in scope for Federal systems that have completed the GSA OA onboarding process as described in GSA CIO-IT Security-12-66: Information Security Continuous Monitoring (ISCM) Strategy & Ongoing Authorization (OA) Program, and have received an Ongoing ATO (OATO).

**Table 3-4. Semiannual OA Security Activities**

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **Ongoing Authorization (OA) System Program Management Reviews (PMR)**<br><br>**Responsibility: ISP OA Team, ISSM, ISSO** | For systems in OA, ISP, ISSOs, and ISSMs will collaborate on the following metrics as described in GSA CIO-IT Security-12-66.<br><br>● Hardware asset management<br>● Software asset management<br>● Configuration settings management<br>● Vulnerability management<br>● Event Management<br>● Periodic Deliverables<br>● Annual Deliverables<br>● Showstopper Controls Status | 03/29/2024 and 09/30/2024 |

## 3.5 Annual Information Security Milestones/Activities

### 3.5.1 Federal System Annual Activities

As identified by the due dates in Table 3-5-1, a number of annual activities are now due in March instead of July to better align with the annual Office of Inspector General (OIG) FISMA Audit.

### Table 3-5-1. Annual Security Activities (Federal Systems)

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **HVA Annual Data Call**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | Annually a data call is generated to comply with BOD 18-02 for reporting HVAs to CISA via CyberScope. | 09/13/2024 |
| **Completion of the Annual Federal ISSO Checklist**<br><br>**Responsibility:**<br>**ISSO completion, ISSM approval** | Using Archer GRC, ISSOs will complete the checklist, including providing evidence as necessary. The checklist consists of:<br><br>● Verifying review of authenticated web application vulnerability scans and identifying actions taken.<br>● Verifying a penetration test exercise has been completed, as applicable.<br>● Verifying a Red Team exercise results report has been completed and delivered to the government, as applicable.<br>● Verifying, if applicable, the systems FISMA self-assessment has been completed.<br>● Verifying, if applicable, all Information Exchange Agreements (IEAs)/Interconnection Security Agreements (ISAs)/Memorandum of Agreements (MOAs) have been updated.<br>● Verifying the SSPP has been updated.<br>● Verifying the Privacy Threshold Assessment (PTA) or Privacy Impact Assessment (PIA), as applicable, has been created and is kept current per its approved expiration date or data usage changes.<br>● Verifying the review of the incident response plan (IRP) and updating, as applicable.<br>● Verifying the IR capability testing has been completed.<br>● Verifying the review of the Contingency Plan (CP) and updating, as applicable.<br>● Verifying the CP testing has been completed.<br>● Verifying the annual user recertification process has been completed. | 07/25/2024<br><br>Note: ISSM reviews are due within 30 days of annual due dates. |
| **Complete FISMA Self-Assessment (if applicable)**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | ISSO completes the FISMA self-assessment (if applicable) with the system team. | 03/25/2024 |
| **Review/Update SSPP**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | ISSO reviews and updates System Security and Privacy Plan with the System Owner and system team. | 03/25/2024 |

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **Review/Update the IRP**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews and updates the IRP with the System Owner and system team. | 03/25/2024 |
| **Complete the IR Test**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO coordinates completion of the IR capability test with the System Owner and system team. | 03/25/2024 |
| **Review/Update the CP**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews and updates the CP with the System Owner and system team. | 03/25/2024 |
| **Complete the CP Plan Test**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO coordinates completion of the contingency/continuity plan test with the System Owner and system team. | 03/25/2024 |
| **Review/Update User Account Recertification**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO coordinates the review and update of the certification of user accounts requiring access to the system with the System Owner and system team. | 03/25/2024 |
| **Review Authenticated Web Application Vulnerability Scans**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO schedules and reviews authenticated web application vulnerability scans (as applicable) and identifies actions taken. | 07/25/2024 |
| **Review Penetration Test Results (if applicable)**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews penetration test results (as applicable) and identifies actions taken. | 07/25/2024 |
| **Review/Update Information Exchange Agreements (IEA)/Interconnection Security Agreements (ISA)/Memorandum of Agreements (MOA), (if applicable)**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews and updates IEAs/ISAs/MOAs (as applicable) with the System Owner and system team. | 07/25/2024 |

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **Create and maintain an approved PTA/PIA (as applicable) per Privacy Office policy.**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team and Privacy Team** | ISSO reviews, updates, and maintains the PTA or PIA (as applicable) with the System Owner, Data Owner, system team, and privacy team. Performed per initial creation, data usage changes, recertification due dates, and A&A cycles. | As applicable |

### 3.5.2 Contractor System Annual Activities

As identified by the due dates in Table 3-5-2 a number of annual activities are now due in March instead of July to better align with the annual Office of Inspector General (OIG) FISMA Audit.

Vendors with an annual security deliverable schedule and due dates which do not align with the due dates listed, may follow the contract schedule until a contract modification is issued. Vendors are encouraged to align with the FY24 due dates where possible.

**Table 3-5-2. Annual Security Activities (Contractor Systems)**

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **HVA Annual Data Call**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | Annually a data call is generated to comply with BOD 18-02 for reporting HVAs to CISA via CyberScope. | 9/13/2024 |
| ***Denotes an item eligible for | Self-Attestation per CIO-IT Security-19-101. | |

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **Completion of the Annual Contractor ISSO Checklist**<br><br>**Responsibility:**<br>**ISSO completion, ISSM approval** | Using Archer GRC, ISSOs will complete the checklist, including providing evidence as necessary. The checklist consists of:<br><br>● Verifying a penetration test report has been completed and delivered to the government.<br>● Verifying a Red Team exercise results report has been completed and delivered to the government, as applicable.<br>● Ensuring, if applicable, the system's FISMA self-assessment has been completed and uploaded.<br>● Verifying the annual review/update of the CP, and delivery to the government.<br>● Verifying the annual CP test, and delivery of the CP test report to the government<br>● Verifying the annual IR Test Report and its delivery to the government.<br>● Verifying the results, and delivery of the security awareness training for all employees and contractors that support the operation of the system.<br>● Verifying a well-defined, documented, and up-to-date baseline configuration has been provided.<br>● Ensuring all IEAs/ISAs/MOAs have been updated and delivered to the government, as applicable.<br>● Verifying the SSPP has been delivered to the government.<br>● Verifying the rules of behavior has been reviewed and/or updated for the current year.<br>● Verifying that the results of the annual review and validation of system users' accounts have been provided to the government.<br>● Verifying the CM plan has been delivered to the government.<br>● Verifying the separation of duties matrix has been reviewed and updated as necessary.<br>● Ensuring documentation reflecting favorable adjudication of background investigations for all personnel supporting the system has been provided.<br>● Ensuring OS configuration compliance scan reports have been delivered showing compliance against the documented configuration settings.<br>● Verifying the PTA or PIA, as applicable, has been created and is kept current per its approved expiration date or data usage changes. | 7/25/2024<br><br>Note: ISSM reviews are due within 30 days of the annual due dates. |

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **Complete FISMA Self-Assessment (if applicable)**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO completes the FISMA self-assessment (as applicable) with the system team. | 3/25/2024 |
| **Review/Update SSPP**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews and updates the SSPP with the System Owner and system team. | 3/25/2024 |
| **Review/Update CP**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews/updates the CP with the System Owner and system team. | 3/25/2024 |
| **Review CP Test Report**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews the CP test report with the System Owner and system team. | 3/25/2024 |
| **Review IR Test**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews the IR test report with the System Owner and system team. | 3/25/2024 |
| **Review/Update User Account Recertification**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews/updates the certification of user accounts requiring access to the system with the System Owner and system team. | 3/25/2024 |
| ***Review/Update Separation of Duties Matrix**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews and updates the Separation of Duties Matrix with the system team. | 3/25/2024 |
| **Review Penetration Test Results (if applicable)**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team and Pen Testers** | ISSO reviews the Penetration Test results (as applicable) and identifies actions taken with the and system team. | 7/25/2024 |
| **Review Red Team Exercise Results (if applicable)**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews Red Team exercise results (as applicable) and identifies actions taken. | 7/25/2024 |

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| ***Review Results of Security Awareness Training**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews the results of the annual security awareness training with the system team. | 7/25/2024 |
| ***Review/Update Baseline Configuration Document**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO Reviews/updates the baseline configuration document with the system team. | 7/25/2024 |
| **Review/Update IEAs/ISAs/MOAs, if applicable**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews and updates IEAs/ISAs/MOAs (as applicable) with the System Owner and system team. | 7/25/2024 |
| **Review/Update Rules of Behavior**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews/updates the Rules of Behavior with the system team. | 7/25/2024 |
| **Review/Update CM Plan**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews/updates the CM Plan with the System Owner and system team. | 7/25/2024 |
| ***Review/Update Personnel Background Investigations**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews/updates documentation reflecting personnel supporting the system have appropriate background investigations, with the System Owner and system team. | 7/25/2024 |
| **Review/Update Operating System Configuration Compliance Scans**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team** | ISSO reviews configuration compliance scans/approved deviations for non-compliance settings. | 7/25/2024 |
| **Create and maintain an approved PTA/PIA (as applicable) per Privacy Office policy.**<br><br>**Responsibility: ISSO/ISSM in coordination with System Team and Privacy Team** | ISSO reviews, updates, and maintains the PTA or PIA (as applicable) with the System Owner, Data Owner, system team, and privacy team. Performed per initial creation, data usage changes, recertification due dates, and schedule A&A cycles. | As applicable |

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| ***Review/Update Supply Chain Risk Management Plan**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Team** | ISSO reviews/updates the SCRM Plan with the System Owner and system team. | 7/25/2024 |

## 3.6 Biennial Information Security Milestones/Activities

Biennial activities are in scope for Contractor systems. All biennial items are eligible for Self-Attestation per CIO-IT Security-17-101.

**Table 3-6. Biennial Security Activities**

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **Contractor Systems** | | |
| **Completion of the Biennial Contractor ISSO Checklist**<br><br>**Responsibility:**<br>**ISSO completion, ISSM approval** | Using Archer GRC, ISSOs will complete the checklist, including providing evidence as necessary. The checklist consists of:<br><br>● Verifying the following policies and procedures have been reviewed, and updated as necessary:<br>○ Maintenance<br>○ System and Information Integrity<br>○ System and Communication Protection<br>○ Security Awareness and Training<br>○ Incident Response<br>○ Access Control<br>○ Audit and Accountability<br>○ Identification and Authentication<br>○ Key Management<br>○ Media Protection<br>○ Personnel Security<br>○ Physical and Environmental<br>○ Supply Chain Risk Management | 07/25/2024 |
| **Review/Update Maintenance Policies/Procedures**<br><br>**Responsibility:**<br>**ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews /updates the Maintenance Policies/Procedures with the System Owner and system team. | 07/25/2024 |
| **Review/Update System and Information Integrity Policies/Procedures**<br><br>**Responsibility:** | ISSO reviews/updates the System and Information Integrity Policies/Procedures with the System Owner and system team. | 07/25/2024 |

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **ISSO/ISSM in coordination with System Owner/System Team** | | |
| **Review/Update System and Communication Protection Policies/Procedures**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews/updates the System and Communication Protection Policies/Procedures with the System Owner and system team. | 07/25/2024 |
| **Review/Update Security Awareness and Training Policies/Procedures**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews /updates the Security Awareness and Training Policies/Procedures with the System Owner and system team. | 07/25/2024 |
| **Review/Update Incident Response Policies/Procedures**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews/updates the Incident Response Policies/Procedures with the System Owner and system team. | 07/25/2024 |
| **Review/Update Access Control Policies/Procedures**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews/updates the Access Control Policies/Procedures with the System Owner and system team. | 07/25/2024 |
| **Review/Update Audit and Accountability Policies/Procedures**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews/updates the Audit and Accountability Policies/Procedure with the System Owner and system team. | 07/25/2024 |
| **Review/Update Identification and Authentication Policies/Procedures**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews /updates the Identification and Authentication Policies/Procedures with the System Owner and system team. | 07/25/2024 |

| Security Activity | Activity Description | Due Dates |
|---|---|---|
| **Review/Update Key Management Policies/Procedures**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews Review/updates the Key Management Policies/Procedures with the System Owner and system team. | 07/25/2024 |
| **Review/Update Media Protection Policies/Procedures**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews/updates the Media Protection Policies/Procedures with the System Owner and system team. | 07/25/2024 |
| **Review/Update Personnel Security Policies/Procedures**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews/updates the Personnel Security Policies/Procedures with the System Owner and system team. | 07/25/2024 |
| **Review/Update Physical and Environmental Policies/Procedures**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews/updates the Physical and Environmental Policies/Procedures with the System Owner and system team. | 07/25/2024 |
| **Review/Update Supply Chain Risk Management Policies/Procedures**<br><br>**Responsibility: ISSO/ISSM in coordination with System Owner/System Team** | ISSO reviews/updates the Supply Chain Risk Management Policies/Procedures with the System Owner and system team. | 07/25/2024 |

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

# 4 Measures of Progress

Although this guide identifies the activities required to monitor and manage the security of GSA information and systems, 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 cybersecurity risk posture and assess how well their systems are performing to GSA's security policy, processes, and procedures, the NIST Risk Management Framework (RMF), and DHS/OMB established FISMA security metrics.

Table 4-1 lists key security performance and risk 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 |
|---|---|---|
| **Showstopper Controls** | Listing of High/Critical risk showstopper controls either not fully satisfied or without a POA&M/AOR.<br>● Multi-Factor Authentication (MFA) for Privileged & User-level access<br>● Critical and High vulnerabilities remediated within established timeframes<br>● Remote Code Execution (RCE) vulnerabilities<br>● End-of-Life (EOL) Software<br>● System Architecture approved by ISE<br>● Integration with GSA's Security Stack (Internal Systems)<br>● Encryption of Sensitive Data (i.e., personally identifiable information [PII], payment card information (PCI), Authenticators, other sensitive data per AO) at rest and in transit)<br>● Compliance with CISA EDs/BODs | All showstopper controls are implemented or have a POA&M/AOR.<br><br>Compliance with EDs/BODs is maintained or there is an POA&M/AOR.<br><br>Note: Additional details about the Showstopper controls are available in CIO-IT Security-06-30. |
| **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. |
| **ATO Status** | % of FISMA systems with a current ATO in accordance with GSA policy and guidance | 100% |
| **Audit Findings** | Listing of audit findings (e.g., Office of Inspector General [OIG], Government Accountability Office [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;<br>Number of High Risk POA&Ms delayed 30 days beyond scheduled completion date;<br>Number of Moderate Risk POA&Ms delayed 90 days beyond scheduled completion date. | <5% of open POA&Ms are delayed;<br>0 High > 30 days;<br>0 Moderate > 90 days. |
| **FISMA Self - Assessment Results** | Listing of other than fully satisfied controls with POA&Ms; number with overdue milestones. | All other than fully satisfied controls have POA&Ms; no overdue milestones. |

## 4.2 AO Briefing Schedule

AO briefings for FY24 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 discuss any relevant threats applicable to the Associate CIO's portfolio of systems.

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. Any system or program risks with the potential to impact the GSA mission will be elevated to the GSA ERSI Board for consideration. The board will determine if any strategic actions are required to address such risks at the enterprise level.

# Appendix A: References

**Federal Laws, Standards, Regulations, and Publications:**

- DHS Cybersecurity Directives
- HVA Assessment Program Supplemental Guidance, Version 3.0
- 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 5, Security and Privacy Controls for 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 Policies, Procedures, Guidance:**

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

- GSA Order CIO 1878.3 CHGE 3, Developing and Maintaining Privacy Threshold Assessments, Privacy Impact Assessments, Privacy Act Notices, and System of Records Notices
- GSA Order CIO 2100.1, GSA Information Technology (IT) Security Policy
- GSA Order CIO 2183.1, Enterprise Identity, Credential, and Access Management (ICAM) Policy
- GSA Order CIO 2200.1, GSA Privacy Act Program

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 GSA.gov IT Security Procedural Guides page with the exception of CIO-IT Security-18-90: GSA IT Common Control Catalog, which is restricted. It is available on the internal GSA InSite IT Security Procedural Guides page. The procedural and technical 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 (MA)
- 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: GSA IT Common Control Catalog (CCC)
- 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

# Appendix B: Roles and Responsibilities

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 listing of roles 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.

## 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.

## Authorizing Officials (AOs)

An AO is the Federal Government management official with the responsibility of issuing an authorization 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 A&A processes defined in CIO-IT Security-06-30.
- Reviewing and approving deviations to policy and AoR letters as specified in CIO 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 CIO 2200.1, CIO 1878.3, and NIST SP 800-53, Revision 5.
- Supporting the security measures and goals established by the CISO.

## System Owners

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 in accordance with 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, CM, 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 SSPP 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 POA&M for their respective systems in accordance with CIO-IT Security-09-44.
- 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 a PTA on all systems to ascertain whether the system collects information on individuals or when new systems are developed, acquired, or purchased; developing a PIA when applicable.
- Defining and scheduling software patches, upgrades, and system modifications.
- Supporting the security measures and goals established by the CISO.

### 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. Communicate any issues or challenges in completing these activities/deliverables to OCISO as soon as they are identified.
- Updating the annual checklist items within 30 days of an activity/deliverable being completed.
- Ensuring the system is operated, used, maintained, and disposed of in accordance with 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 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/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 the Enterprise Logging Platform (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 in accordance with 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.

### 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.
- 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 in accordance with 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.

## Privacy Analysts

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

- Approving system categorizations for systems that contain PII in accordance with FIPS 199 and overseeing proper implementation of privacy controls.
- Overseeing proper implementation of privacy controls.
- Approving the SSPP.
- Reviewing PTAs to ensure privacy controls address the risks associated with collecting, using, processing, storing, and disseminating PII. Once a system is identified as having potential privacy implications, the Privacy Analyst determines if a PIA is required.

## Appendix C - Systems with Expiring ATOs in FY24

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

| Responsible Org/System Name | ATO Date | Renewal Date |
|---|---|---|
| **Federal Acquisition Services (Q)-Sagar Samant** | | |
| Legacy System for Award Management (LSAM) | 9/26/2023 | 11/30/2023 |
| Symplicity Cloud System (SCS) | 10/19/2023 | 1/18/2024 |
| e-Gov Travel - Concur Government Edition (eGT CGE) | 7/24/2023 | 2/28/2024 |
| Federal Public Key Infrastructure (FPKI) | 3/24/2021 | 3/24/2024 |
| USAccess | 3/24/2021 | 3/24/2024 |
| MetTel MTIPS | 5/22/2023 | 3/31/2024 |
| Network Hosting Center (NHC) | 4/2/2021 | 4/2/2024 |
| Order Management System (OMS) | 8/12/2022 | 7/30/2024 |
| GSA SmartPay Content Systems (GSPCS) | 8/31/2023 | 8/31/2024 |
| Network Services Ordering Billing System (NSOBS) | 10/13/2022 | 9/30/2024 |
| **GSA IT - Office of Acquisition IT Services (IQ)-Sagar Samant** | | |
| MyGEOTAB (GEOTAB) | 12/7/2020 | 12/7/2023 |
| Personal Property Management System (PPMS) | 12/15/2022 | 12/15/2023 |
| Enterprise Service Oriented Architecture (eSOA) | 2/17/2023 | 12/30/2023 |
| FAS Cloud Service (FCS) | 3/30/2023 | 12/31/2023 |
| Cloud Acquisition Tools (CAT) | 9/19/2023 | 1/31/2024 |
| System for Award Management (SAM) | 12/30/2021 | 5/21/2024 |
| Sales Automation System (SASy) | 6/2/2021 | 6/2/2024 |
| GSA Enhanced Checkout (GECO) | 6/8/2021 | 6/8/2024 |
| Contract Acquisition Lifecycle Management System (CALM) | 9/14/2022 | 7/30/2024 |
| SmartPay - Data Warehouse | 9/3/2021 | 9/3/2024 |
| **Federal Acquisition Services (Q)-Ann Lewis** | | |
| Identity Verification API (IDVA) | 12/6/2022 | 12/21/2023 |
| USA.GOV | 9/28/2023 | 12/29/2023 |
| Search.gov | 6/29/2023 | 1/30/2024 |
| Federalist | 9/18/2023 | 2/29/2024 |
| GSA Implementation of Zendesk | 7/1/2021 | 7/1/2024 |
| Touchpoints (TP) | 7/13/2021 | 7/13/2024 |
| Tock | 9/2/2021 | 9/2/2024 |
| Federal Audit Clearinghouse (FAC) | 9/5/2023 | 9/5/2024 |
| Data.gov | 9/23/2021 | 9/23/2024 |
| Challenge.gov | 9/24/2021 | 9/24/2024 |
| **GSA IT - Office of Corporate IT Services (IC)-Elizabeth DelNegro** | | |
| eRulemaking | 10/11/2023 | 1/16/2024 |
| Enterprise Application Services (IC-EAS) | 3/21/2023 | 2/28/2024 |
| GSA Ancillary Corporate Applications (ACA) | 9/29/2023 | 2/29/2024 |

| Responsible Org/System Name | ATO Date | Renewal Date |
|---|---|---|
| Pegasys | 3/30/2023 | 3/13/2024 |
| HRLinks | 3/31/2021 | 3/31/2024 |
| Enterprise Content Application Services II (ECAS II) | 9/13/2021 | 9/14/2024 |
| **GSA IT - Office of the Chief Information Officer (I)-David Shive** | | |
| Enterprise Application Services (I-EAS) | 3/21/2023 | 2/28/2024 |
| **GSA IT - Office of Public Building IT Services (IP)-Philip Klokis** | | |
| Agile Custom Real Estate (ACRE) | 8/24/2023 | 11/24/2023 |
| National Computerized Maintenance Management System (NCMMS) | 6/26/2023 | 12/26/2023 |
| Lease Management Tool (LMT) Management Analysis Review System (MARS) | 2/22/2023 | 2/22/2024 |
| BI Framework | 9/30/2021 | 9/30/2024 |
| **Office of Governmentwide Policy (M)-Dan Pomeroy** | | |
| N/A | N/A | N/A |