IT Security Procedural Guide: External Information System Monitoring CIO-IT Security-19-101

Revision 5

November 5, 2024

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		Initial Release – October 22, 2019		
N/A	IST	New guide created	Guide needed to monitor external information systems.	All
		Revision 1 – March 11, 2020		
N/A	Klemens	Updated ISSO Checklist due dates, clarified deliverable review/acceptance process, and added usage of Archer for ISSO checklists. Updated process workflow diagram.	Update to reflect current GSA guidance and clarify deliverable review/acceptance process.	Multiple
		Revision 2 – January 25, 2023		
1	McCormick, Klemens	Revisions include: ● Aligned due dates to support due dates in the FY23 Management Implementation Plan. ● Identified which annual deliverables are due in March and July. ● Added deliverable requirements regarding Supply Chain Risk Management. ● Updated to the latest guide format and style.	Periodic update and alignment to GSA policies and guidance.	Throughout
		Revision 3 –March 31, 2020		
1	Klemens	● Corrected due date in Section 4.1. ● Added due dates to Biennial deliverables in Table 6-1.	Correction of due date.	Section 4.1, Table 6.1
		Revision 4 – November 28, 2023		
1	McCormick	● Updated due dates to align with FY24 IT Security Program Management Implementation Plan. - Added Red Team exercise requirements. - Added SA-11(1) Static Code analysis requirement. ● Edited and formatted to current guidance.	Periodic update.	Throughout
		Revision 5 – November 5, 2024		
1	Klemens, Normand	● Updated to align with FY25 IT Security Program Management Implementation Plan (MIP).	Periodic update to align with current GSA and Federal guidance.	Throughout

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		• Added AOR Letter, M-21-31 Data Call, and CUI Data Call requirements. • Moved SCRM Plan to a biennial requirement. • Updated due dates, as applicable.		

Approval

IT Security Procedural Guide: External Information System Monitoring, CIO-IT Security-19-101, Revision 5, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD7179261815444F...

Bo Berlas
GSA Chief Information Security Officer

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

TABLE OF CONTENTS

Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Section 1.3. For example, Google Forms, Google Docs, and websites will have links.

1 Introduction

Many of the General Services Administration's (GSA) Information Technology (IT) systems are external information systems. While GSA does not have day-to-day operational responsibility for securing these systems, Public Law 113-283, "Federal Information Security Modernization Act of 2014," (FISMA) places ultimate responsibility for security with GSA. This requires developing processes to ensure adequate oversight, including having the correct contracting language identified in CIO-IT Security-09-48: Security and Privacy Requirements for IT Acquisition Efforts and ensuring deliverables are provided in a timely manner and meet requirements outlined within this document.

The deliverables identified throughout this guide are monitored via Information Systems Security Officer (ISSO) Checklists generated from GSA's Governance, Risk, and Compliance (GRC) tool. The due dates in this guide have been set to enable the due dates specified in CIO-IT Security-08-39: FY25 IT Security Program Management Implementation Plan, and the ISSO Checklists aligned to those dates, to be met. For example, the due dates in this guide provide time for reviewing, updating as necessary, and accepting/approving deliverables.

1.1 Purpose

This procedural guide defines the processes and procedures that will be used to ensure that external information systems are monitored, and that required deliverables are provided timely and meet GSA security requirements.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees, contractors, and vendors who oversee/protect GSA information systems and data. The guide provides GSA Federal employees, contractors, and vendors as identified in GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy," and other IT personnel involved in the oversight of external information systems, with the specific processes to follow for properly accomplishing oversight of external information systems under their purview.

1.3 References

Note: GSA updates its IT security policies and procedural guides on independent cycles (at a minimum every 3 years) which may introduce conflicting guidance until revised guides are developed. In addition, many of the references listed are updated by external organizations which can lead to inconsistencies with GSA policies and guides. When conflicts or inconsistencies are noticed, please contact ispcompliance@gsa.gov for guidance.

Federal Laws, Standards, Regulations, and Publications:

- Public Law 113-283, "Federal Information Security Modernization Act of 2014"

GSA Guidance Policies, Procedures, Guidance:

The GSA policy listed below is available on the GSA.gov Directives Library webpage.

- GSA Order CIO 2100.1, GSA Information Technology (IT) Security Policy

The GSA CIO-IT Security Procedural Guides listed below are available on the GSA.gov IT Security Procedural Guides webpage.

- CIO-IT Security-08-39, FY25 IT Security Program Management Implementation Plan
- CIO-IT Security-09-44, Plan of Actions and Milestones (POA&M)
- CIO-IT Security-09-48, Security and Privacy Requirements for IT Acquisition Efforts

2 Roles and Responsibilities

There are many roles associated with external information system monitoring. The roles and responsibilities in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. CIO 2100.1 contains a complete listing of roles and responsibilities for GSA management officials and roles with significant IT Security responsibilities.

2.1 GSA Chief Information Security Officer (CISO)

Responsibilities include:

- Implementing and overseeing GSA's IT Security Program by developing and publishing security policies and IT security procedural guides.
- Establishing reporting deadlines for IT Security related issues requiring an agency response affecting the GSA IT Security Program.
- Establishing and maintaining a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency.
- Supporting the GSA CIO in reporting to the GSA Administrator on the effectiveness of the agency information security program, including progress of remedial actions.

2.2 Authorizing Officials (AO)

Responsibilities include:

- Reviewing and approving security safeguards of information systems and issuing ATO approvals for each information system under their purview based on the acceptability of the security safeguards of the system (risk-management approach).
- Providing support to the Information Systems Security Managers (ISSMs) and ISSOs appointed by the GSA CISO for GSA systems under their purview.

2.3 Office of CISO Division Directors (OCISO)

Responsibilities include:

- Monitoring adherence and proper implementation of GSA's IT Security Policy and reporting the results to the CISO.

2.4 Information Systems Security Manager (ISSM)

Responsibilities include:

- Ensuring Assessment and Authorization (A&A) support documentation is developed and maintained for the life of the system, including the usage of GSA's implementation of its current GRC solution;
- Reviewing and approving ISSO checklists submitted in GSA's current GRC solution and coordinating with ISSOs, as necessary, for systems under their purview.
- Ensuring adherence and proper implementation of GSA's IT Security Policy.

2.5 Information System Security Officer (ISSO)

Responsibilities include:

- Ensuring the system is operated, used, maintained, and disposed of in accordance with documented security policies and procedures.
- Completing the recurring activities in ISSO checklists, completing the checklists in GSA's current GRC solution, and submitting the checklists when completed.

2.6 System Owner

Responsibilities include:

- 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, and contingency planning and testing.
- Supporting the security measures and goals established by the CISO.

2.7 Contracting Officer/Contracting Officer Representative (CO/COR)

Responsibilities include:

- Coordinating with the CISO or other appropriate official as required, ensuring that all agency contracts and procurements are compliant with the agency's information security policy and include appropriate security contracting language and security requirements in each contract.
- Ensuring new solicitations for all GSA IT systems include the security contract language from GSA CIO-IT Security-09-48.

3 Deliverable Requirements

There are three types of deliverables in monitoring external information systems at GSA, categorized by frequency: Quarterly, Annual, and Biennial. Unless specified otherwise within this guide, the creation, management, and reporting of each deliverable type is the same. Deliverables that can be attested to by the vendor of the external information system are identified with an "*" in the following sections.

In addition to the periodic requirements listed in the following sections, per Binding Operational Directive (BOD) 22-01, Reducing the Significant Risk of Known Exploitable Vulnerabilities (KEV), vendors must provide an email, within 7 days of the KEV remediation requirement, to the ISSO/ISSM or COR certifying remediation consistent with the BOD 22-01 KEV requirement supported with clean authenticated scan reports.

Federal mandates may be issued regarding Federal Information Systems requiring vendors to provide data regarding any such systems they operate, administer, manage, or maintain. Vendors will be required to provide data in accordance with any such mandate. Per 40 U.S.C [United States Code], Subtitle III, Chapter 113, Section 11331, Definitions, "*The term 'Federal information system' means an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.*"

3.1 Quarterly Deliverables

The following deliverables will be submitted on a quarterly basis. Quarterly deliverables are due one month prior to the end of each quarter.

- Operating System Vulnerability scan Reports
- Web Application Vulnerability scan Reports
- Plan of Action & Milestones (POA&M) Update
- Acceptance of Risk (AOR) Letter Updates, if applicable
- Static Code analysis was performed, as necessary
- FISMA Quarterly Metrics data, as necessary
- Update vulnerability management procedures, as necessary, to address:
  - Subscribing to the Cybersecurity and Infrastructure Security Agency (CISA) KEV Catalog for automated updates.
  - Remediating vulnerabilities identified in the KEV within 14 days of addition.
  - Providing 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.

3.2 Annual Deliverables

The following deliverables will be submitted on an annual basis. As identified below some annual deliverables are due in March and others are due in July. In addition, an annual High Value Asset (HVA) data call will be due in August. If a Self-Attestation Letter is used, it is due on the same schedule as the deliverable being attested to.

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 FY25 due dates where possible.

Due February 25th:

- Annual FISMA Self-Assessment, if applicable
- System Security and Privacy Plan (SSPP)
- Contingency Plan
- Contingency Plan Test Report

- Incident Response (IR) Test Report
- User Certification/Authorization Review Documents
- *Separation of Duties Document/Matrix

Due June 25th:

- Penetration Test Report, if applicable
- Red Team Exercise Results Report, if applicable
- *Information Security Awareness and Training Records
- *System(s) Baseline Configuration Standard Document
- Information Exchange Agreements (IEAs)/Interconnection Security Agreements (ISAs)/Memorandum of Agreements (MOAs), if applicable
- *Rules of Behavior
- Configuration Management Plan
- *Personnel Screening and Security (background investigations)
- System Configuration Settings Verification (e.g., scans)
- Privacy Threshold Assessment/Privacy Impact Assessment, if applicable (i.e., an update is required)

Due May 30th:

- HVA Data Call, if applicable
- CUI Data Call

Due July 25th:

- M-21-31 Data Call

*Attestation acceptable in a Vendor Attestation Statement (Annual).

3.3 Biennial Frequency Deliverables

The following deliverables will be submitted on a biennial basis. The deliverables listed, or a Self-Attestation Letter, if used, is due on June 25th in even numbered years.

- *System Maintenance (MA) Policy and Procedures
- *System and Information Integrity (SI) Policy and Procedures
- *System and Communication Protection Policy and Procedures
- *Security Awareness and Training Policy and Procedures
- *Incident Response (IR) Policy and Procedures
- *Access Control (AC) Policy and Procedures
- *Audit and Accountability (A&A) Policy and Procedures
- *Identification and Authentication (IA) Policy and Procedures
- *Key Management Policy
- *Media Protection (MP) Policy and Procedures
- *Personnel Security Policy and Procedures
- *Physical and Environmental Policy and Procedures
- *Supply Chain Risk Management Policy and Procedures
- *Supply Chain Risk Management Plan (associated with SR-2 control)

*Attestation acceptable in Vendor Attestation Statement (Biennial)

4 Deliverable Submission and Review Timelines

As noted in previous sections, submission due dates are used to ensure adequate time is allowed for deliverable creation, review, corrective action, and reporting. Submission dates are aligned to allow reporting based on the Federal Fiscal Year (FY) (October 1st – September 30th). The FY quarters end on the last day of December, March, June, and September. The FY ends on the last day of September, and Biennial deliverables are aligned with even number FYs (e.g., 2024, 2026).

4.1 Vendor Submissions

The Vendor Security Deliverable Quality Checklist is used to ensure all supporting artifacts meet GSA requirements, including documents identified in vendor attestation statements. The vendor is encouraged to use the quality checklist to verify that their deliverables meet GSA's requirements. The GSA ISSO uses the quality checklist to validate that the deliverables are acceptable. Deliverable submissions are due as indicated below.

- Quarterly Artifacts/Deliverables are due one month prior to the completion of each quarter. Due dates are the last workday of the months listed:
  - **Quarter 1 – November**
  - **Quarter 2 – February**
  - **Quarter 3 – May**
  - **Quarter 4 – August**
- Annual Deliverables and Vendor Attestation Statements with supporting artifacts are due by February 25th or June 25th, or other dates as identified in Section 3.2.
- Biennial Vendor Attestation Statements are due June 25th in even numbered years.

4.2 Review Process

The deliverables submission and review process is depicted in Figure 5.1 and summarized in the steps below.

Step 1A and 1B. The vendor produces the required deliverables, including vendor attestation letters, as appropriate. The deliverables are then delivered to GSA.

Step 2A and 2B. The GSA ISSO and Contracting Officer/Contracting Officer Representative (CO/COR) review the deliverables and, based on contractual requirements and the Vendor Security Deliverable Quality Checklist, determine their acceptability.

Step 2C. The GSA ISSO and ISSM use the Contractor ISSO Checklists implemented in GSA's GRC tool to document reviews and actions based on those reviews.

Steps 3, 4A, and 4B. If there are issues with the deliverables, the ISSO coordinates with the vendor to correct minor issues. Major issues are coordinated between the ISSO and ISSM. Any issues resulting in non-compliance (checklist and attestation letter) will be handled through the POA&M process as defined in CIO-IT Security-09-44.

Step 4A and 5. The ISSM reviews deliverables and coordinates with the vendor/ISSO to correct any minor issues Major issues that cannot be resolved are handled via the system's POA&M.

Step 6. GSA's GRC tool is used to report on status and is also used by ISSMs and others to analyze checklist data for possible process improvements.

4.3 Tracking and Monitoring Reviews

Quarterly, Annual, and Biennial Contractor ISSO Checklists have been implemented in GSA's GRC tool for vendor deliverables. These checklists are used by ISSOs to document deliverable reviews and actions taken based on those reviews. Checklist campaigns are created based on the frequency of the deliverables and assigned to ISSOs who receive an email notification. ISSOs complete a checklist and submit it in the GRC tool, which generates an email to ISSMs indicating a checklist has been submitted for their review and approval. ISSMs approve or reject submitted checklists. ISSOs review rejected checklists and coordinate with the ISSM and the vendor to address any issues until a checklist is able to be resubmitted and approved.

5 External Information System Monitoring Process

Figure 5-1 depicts the workflow associated with the external information system monitoring process.

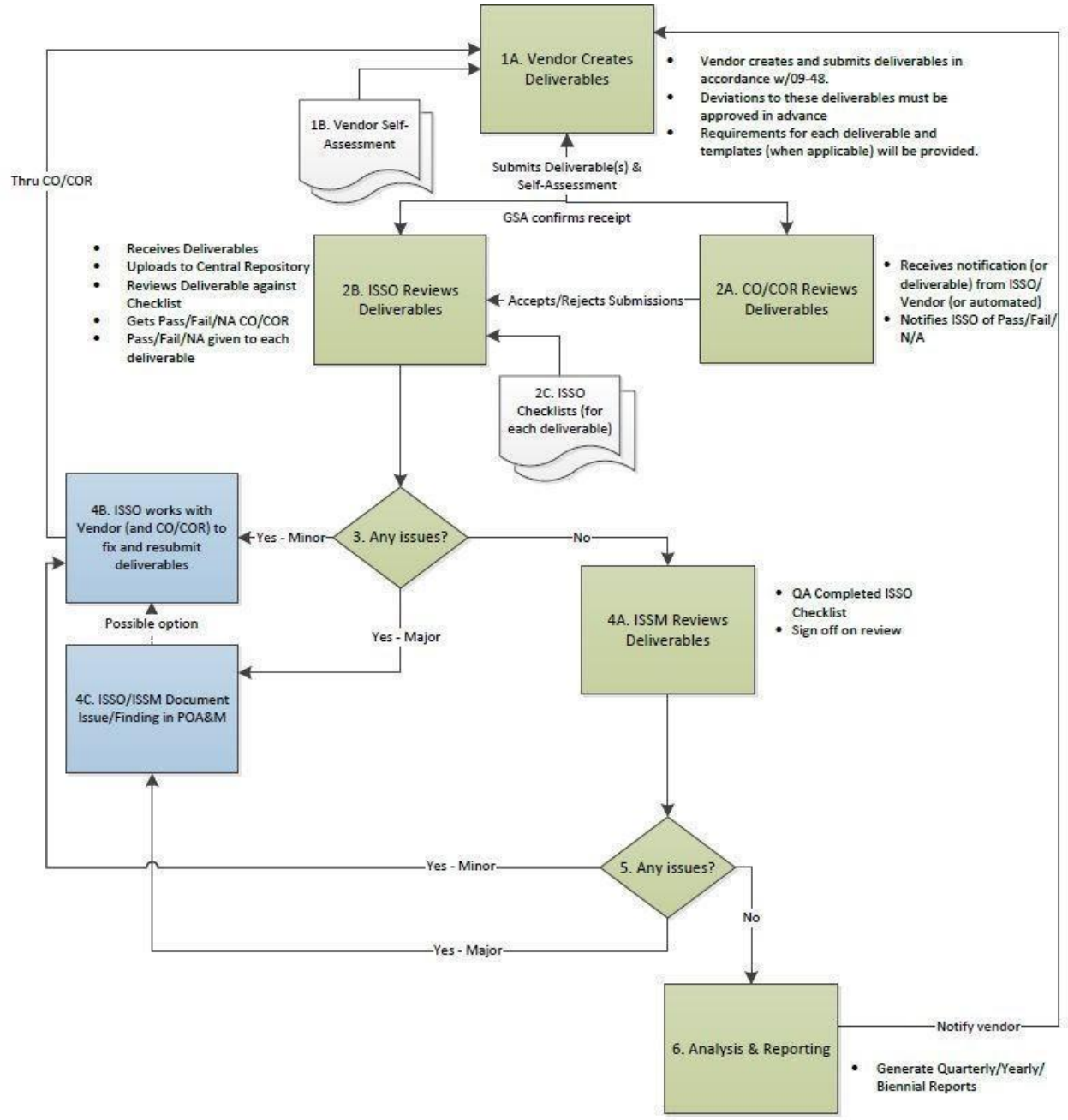

Figure 5-1: Workflow for External System Monitoring Process

5.1 Vendor Requirements

The vendor is responsible for providing all deliverables/artifacts that meet or exceed the checklist criteria on or before the submission date. Any questions or concerns should be discussed with the ISSO and/or CO/COR.

The vendor should submit the documents to both the CO/COR and the ISSO and if sent by email the artifacts should be encrypted.

5.2 CO/COR Requirements

The CO/COR is responsible for reviewing the contractor submissions as it deems fit. The CISO's office will not prescribe a checklist for the CO/COR.

The CO/COR is required to notify the ISSO with their acceptance or rejection of the submissions, so their information is included for the ISSM review.

5.3 ISSO Requirements

The ISSO is responsible for ensuring timely submission by the vendor as well as ensuring that the submission meets the requirements identified in the checklist.

The ISSO will identify any issues with the submissions and will work with the vendor and CO/COR to adjust the submissions prior to the end of the ISSO review period. If adjustments are made, the ISSO checklists should be updated and the adjusted submissions should be stored on the Team Drive.

Prior to the ISSO finalizing their review, they need confirmation from the CO/COR that a review was performed. If any issues were observed, the ISSO must report that information to the ISSM.

The ISSO can, at any time, elevate items or issues. The ISSO should initially attempt to elevate items to the ISSM, but they may also, as necessary, include the System Owner, Authorizing Official, or CISO.

The ISSO is responsible for disseminating checklists to the vendor POCs.

5.4 ISSM Requirements

The ISSM will perform a quality assurance check on the ISSM checklist items and review the submissions for additional security concerns. For each submission period, the ISSM will evaluate the system for risk based on the submissions and prior issues, to include POA&M items. If the ISSM does not find any significant issues, they will approve the checklist for that period.

The ISSM is responsible for ensuring the ISSO has access to the latest checklists and recommending updates to the checklists and overall process.

When issues are observed, the ISSM will take action appropriate for the risk. Any issues resulting in non-compliance (checklist and attestation letter) will be handled through the POA&M process as defined in CIO-IT Security-09-44.

5.5 System Management

System Management (including Authorizing Official and System Owner) will typically be involved on a periodic basis throughout the reporting process for status and lower risk issues. System management will also be involved on an ad hoc basis as higher risk issues arise. Minimally, reporting will be quarterly and yearly, unless a more frequent reporting frequency is required.

Ad hoc issues will usually be reported from the ISSO to the ISSM. The ISSM will report to the office of the CISO. Depending on the nature of the issue, one or more of the following roles will likely be brought in to assist in resolving the issue: Authorizing Official, System Owner, CO/COR, ISSM, ISSO, or vendor staff.

6 Storage of A&A Artifacts

A&A artifacts must be stored in the location and per the frequency identified below. Artifacts required biennially are only required in even numbered FYs.

Table 6-1: Deliverable Locations and Frequencies

Deliverable	Frequency	Storage Location	Self-Attestation Eligible
Operating System (including databases) vulnerability scan reports	Quarterly	Google Drive	No
Web Application vulnerability scan reports	Quarterly	Google Drive	No
POA&M Update	Quarterly	Google Drive	No
AOR Letter Update, if applicable	Quarterly	Google Drive	No
Static Code analysis report	Quarterly	Google Drive	No
FISMA Quarterly Metrics data, as necessary	Quarterly	Google Drive	No
Update vulnerability management procedures, as applicable	Quarterly	Google Drive	No
Annual FISMA Self-Assessment, if applicable	Annual-2/25	Google Drive	No
SSPP	Annual-2/25	GRC Tool	No
Contingency Plan	Annual-2/25	GRC Tool	No
Contingency Plan Test Report	Annual-2/25	GRC Tool	No
Incident Response Test Report	Annual-2/25	GRC Tool	No
User Certification/Authorization Review Documents	Annual-2/25	GRC Tool	No
Separation of Duties Document/Matrix	Annual-2/25	GRC Tool	Yes
HVA Data Call, if applicable	Annual-5/30	GRC Tool	No
CUI Data Call	Annual-5/30	GRC Tool	No
Penetration Test Report	Annual-6/25	GRC Tool	No
Red Team Exercise Results Report, if applicable	Annual-6/25	GRC Tool	No
Information Security Awareness and Training Records	Annual-6/25	GRC Tool	Yes
System(s) Baseline Configuration Standard Document	Annual-6/25	GRC Tool	Yes
IEAs/ISAs/MOAs, if applicable	Annual-6/25	GRC Tool	No
Rules of Behavior	Annual-6/25	GRC Tool	Yes
Configuration Management Plan	Annual-6/25	GRC Tool	No
Personnel Screening and Security (background investigations)	Annual-6/25	GRC Tool	Yes
System Configuration Settings Verification (e.g., scans)	Annual-6/25	GRC Tool	No
PTA/PIA	Annual-6/25	GRC Tool	No
M-21-31 Data Call	Annual-7/25	GRC Tool	No
System Maintenance Policy and Procedures	Biennial-6/25	GRC Tool	Yes

Deliverable	Frequency	Storage Location	Self-Attestation Eligible
System and Information Integrity Policy and Procedures	Biennial-6/25	GRC Tool	Yes
System and Communication Protection Policy and Procedures	Biennial-6/25	GRC Tool	Yes
Security Awareness and Training Policy and Procedures	Biennial-6/25	GRC Tool	Yes
Incident Response Policy and Procedures	Biennial-6/25	GRC Tool	Yes
Access Control Policy and Procedures	Biennial-6/25	GRC Tool	Yes
Audit and Accountability Policy and Procedures	Biennial-6/25	GRC Tool	Yes
Identification and Authentication Policy and Procedures	Biennial-6/25	GRC Tool	Yes
Key Management Policy	Biennial-6/25	GRC Tool	Yes
Media Protection Policy and Procedures	Biennial-6/25	GRC Tool	Yes
Personnel Security Policy and Procedures	Biennial-6/25	GRC Tool	Yes
Physical and Environmental Policy and Procedures	Biennial-6/25	GRC Tool	Yes
Supply Chain Risk Management Policy and Procedures	Biennial-6/25	GRC Tool	Yes
Supply Chain Risk Management Plan (associated with SR-2 control)	Biennial-6/25	GRC Tool	Yes

Appendix A – Related Artifacts

Below are documents that are maintained separate from this procedural guide:

Stakeholder list by system. This Google Sheet identifies the ISSM, ISSO, System Owner, Authorizing Official, Contracting Officer, and Contracting Officer Representative for GSA external information systems. Please contact the system's ISSO or ISSM if access to the Google Sheet or information from it is needed.

The following forms/templates are available on the IT Security Form and Aids webpage.

- **Vendor Security Deliverable Quality Checklist (Quarterly)**
- **Vendor Attestation Statement (Annual)**
- **Vendor Attestation Statement (Biennial)**