IT Security Procedural Guide: Security and Privacy Awareness and Role Based Training Program CIO-IT Security-05-29

Revision 9

March 3, 2025

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 4 – November 11, 2015		
1	Graham/ Sitcharing	Changes throughout the document to correspond with revisions made to CIO-IT-Security-06-30 and CIO P2100.1	Updated to reflect correlation of the CIO-IT Security Guide and CIO P2100.1	Throughout
2	Heard/ Mott/ Searcy/ Sitcharing	Inclusion of OCISO program common controls and privacy information	To ensure consistency with current agency policies and guidelines/800-53 Rev 4	Throughout
		Revision 5 – October 20, 2016		
1	Pierce/ Wilson/ Desai	Updated the guide's formatting and structure, updated the guide name, updated the role based training section, updated the role based course mapping section, and modified the annual training hours requirements.	Updated guide to better reflect current Federal and GSA requirements.	Multiple
		Revision 6 –May 1, 2020		
1	Thomsen	Updates include: • Integration of training policy into guide. • Revised NIST SP 800-53 AT controls to refer to the Information Security Program Plan for details. • Reduced and consolidated roles/responsibilities. • Updated appendices to include training topics, roles, metrics, controls, and artifacts.	Updated to reflect current GSA guidance on security training.	Throughout
		Revision 7 – September 29, 2022		
1	Thomsen	Updates include: • Updated Table B-1 to NIST SP 800-53, Revision 5 controls and added responsibility and personnel coverage. • Updated Table D-1, OPM 5 CFR to GSA role mappings. • Updated referenced location for supporting artifacts. • Added Security Exchange as means to satisfy training hours	Rev. 5 alignment milestone.	Throughout
2	McCormick/ Klemens	Edited and formatted guide.	Align to current guide format. New or substantively changed controls in Revision 5 are: AT-2, AT-2(2), AT-2(3), AT-3, AT-3(5).	Throughout
		Revision 8 – May 23, 2023		
1	Thomsen	Updates include: • Requiring New Users to either complete security awareness training or test out. • Revised Program Metrics introduction.	Update new user security awareness training requirement.	Section 3.1.1, Appendix E
2	Klemens	Edited and formatted guide.	Align to current guide style/ format.	Throughout
		Revision 9 – March 3, 2025		

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
1	Thomsen, Normand, Klemens	Updates include: • Reformatted and restructured guide. • Clarified completion timelines and enforcement actions. • Added System Owner to role based training. • Added section on Compliance with requirements. • Added Appendix E on Enforcement Playbook.	Align to current GSA guidance.	Throughout

Approval

IT Security Procedural Guide: Security and Privacy Awareness and Role Based Training Program, CIO-IT Security 05-29, Revision 9, is hereby approved for distribution.

Signed by:
Dovarius Peoples
34793E3A1E88420...

Dovarius Peoples
Acting 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

1 Introduction

1.1 Purpose

This procedural guide describes the Security and Privacy Awareness and Role Based Training requirements for all General Services Administration (GSA) employees and contractors, and aligns with the following agency policy and federal guidelines:

Federal Laws, Standards, Regulations, and Publications:

- NIST SP 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations
- Office of Personnel Management (OPM) Code of Federal Regulations (CFR) Title 5 Volume 2 Section 930.301, Information Security Responsibilities for Employees who Manage or Use Federal Information Systems
- Public Law 113-283, Federal Information Security Modernization Act of 2014

GSA Policies, Procedures, Guidance:

- GSA Order CIO 2100.1, GSA Information Technology (IT) Security Policy
- CIO-IT Security-18-90, Common Control Catalog

1.2 Scope

This guide applies to GSA employees and contractors holding enterprise (gsa.gov) network accounts.

2 Roles and Responsibilities

This section describes the roles and responsibilities required to maintain an effective cybersecurity training program within GSA.

2.1 GSA Executive Leadership

Roles Included:

- Administrator
- Deputy Administrator
- Chief Information Officer

Responsibilities:

- Ensure maintenance of the GSA IT Security and Privacy Awareness Training Program.
- Require mandatory security training for all GSA personnel.

2.2 GSA Cybersecurity and Privacy Executives

Roles Included:

- Chief Information Security Officer (CISO)
- Deputy Chief Information Security Officer (Deputy CISO)
- Senior Agency Official for Privacy (SAOP)

Responsibilities:

- Direct GSA IT Security and Privacy Awareness Training implementation.
- Ensure content effectively maintains a cyber-informed workforce.
- Direct the implementation of a Role-Based Training Program for key security personnel.
- Identify roles with significant security and privacy responsibilities.
- Ensure personnel understand their security roles and responsibilities.

2.3 Supervisors/Contracting Officers

Responsibilities:

- Monitor and ensure personnel complete mandatory training.
- Identify personnel fulfilling roles with significant security

2.4 GSA IT Cybersecurity Training Manager

Responsibilities:

- Develop and manage the OCISO Role-Based Security Training Program.
- Develop and manage the GSA IT Security and Privacy Awareness Program.

3 General Security and Privacy Awareness Training Program

The Security and Privacy Awareness Training Program educates personnel on foundational cybersecurity and privacy practices to safeguard GSA systems and information. Various methods are employed to ensure effective learning and retention over time.

3.1 Mandatory Security and Privacy Awareness Training

All GSA personnel are required to complete the Security and Privacy Awareness Training course offered through the GSA's Learning Management System - GSA Online Learning University (OLU). This course equips employees with the essential skills and knowledge necessary to protect GSA systems, data, and operations.

The training is developed collaboratively by the Security and Privacy teams, ensuring comprehensive coverage of critical topics. These topics are selected based on legal requirements and the agency's commitment to maintaining a secure operational environment. A list of covered topics can be found in Appendix A.

3.1.1 Enforcement and Timelines

OCISO enforces strict adherence to mandatory training requirements. Table 3-1 outlines personnel categories, completion timelines, and enforcement actions:

Table 3-1. Training Completion Timelines for Personnel

Personnel Type	Required Completion Within	Enforcement Action
Existing Personnel	120 days of assignment	Quarantine/Account Disablement
New Personnel	90 days after Entry on Duty (EOD)*	Quarantine/Account Disablement

*Official start date for new personnel.

3.1.2 Overlapping Timelines

When the annual training campaign launches within 90 days of a new employee's EOD, they will be required to complete the current year's training campaign. Any incomplete training from the previous year will be replaced with the current year's requirements.

For example, if an employee is hired in November 2024 and the 2025 training campaign launches in January 2025, the 2024 requirements will be replaced by the 2025 course. Completion of the 2024 training does not waive the requirement to complete the 2025 version.

This policy ensures fairness while maintaining a consistent security posture across all personnel categories.

3.1.3 Accountability and Compliance

Strict enforcement of training timelines is critical to safeguarding GSA's assets, ensuring operational readiness, and maintaining compliance with federal security standards. Personnel who fail to meet these deadlines will face access restrictions, including network quarantine or account disablement, until training is completed.

This structured approach ensures all employees are prepared to meet GSA's security needs while accommodating unique scenarios like overlapping timelines.

3.1.4 Supplemental Artifacts Supporting OCISO Training Program

Artifacts describing or supporting the operation of the OCISO Security and Privacy Awareness Training Program are maintained on Google Drive and available by request. Artifacts may include but are not limited to organizational charts for the Information Security (IS) Training organization and procedures for tracking and reporting metrics.

3.2 Routine Phishing Simulations

Phishing simulations (i.e., fraudulent emails that appear to come from a reputable source) improve training outcomes. OCISO will conduct routine phishing simulations to increase GSA personnel's awareness of this attack type and reduce the likelihood that bad actors will successfully deceive them. Campaigns will vary in difficulty and target different user groups. Only GSA personnel with GSA email addresses will be phished. Phishing campaigns will also be coordinated across GSA IT service teams.

4 Role-Based Security and Privacy Training

The OCISO is responsible for managing and coordinating role-based security training within GSA. In compliance with OPM 5 CFR Part 930.301, agencies must identify personnel with significant security responsibilities and ensure they receive role-specific training. Appendix C provides a detailed mapping between the roles defined in OPM 5 CFR Part 930.301 and GSA-specific roles that carry significant security responsibilities.

4.1 Training Requirements for Roles with Significant Security Responsibilities

Beginning in FY25, personnel identified as holding significant security responsibilities (see Table 4-1) must complete mandatory role-based training through the GSA OLU. Successful completion of the designated training courses satisfies the role-based training requirements outlined in this guide.

Table 4-1: Training Completion Timelines for Personnel

Role	Assignment Criteria	Enforcement Action
Authorizing Official	AO Designation Letter	Quarantine/Account Disablement
Information System Security Officer	ISSO Designation Letter	Quarantine/Account Disablement
Information System Security Manager	ISSM Designation Letter	Quarantine/Account Disablement
System Owner	SO Designation Letter	Quarantine/Account Disablement
Privileged User	Holds a Short Name Account (SNA) account or is designated as a privileged user by the System Owner.	Disablement of SNA account or privileged access within the system.

4.2 Role of GSA's Governance, Risk, and Compliance (GRC) Tool

GSA's GRC Tool will serve as the official repository for listing individuals assigned to critical security roles, including Information System Security Officer (ISSO), Information System Security Manager (ISSM), and System Owner. GSA's GRC Tool facilitates the centralized assignment and tracking of individuals holding significant security responsibilities, ensuring clear accountability and streamlined management in alignment with organizational security policies.

4.3 Privileged Users

Privileged users include individuals meeting one or both of the following criteria:

SNA Account Holder: All active users with an SNA account.

System Owner Designation: Any contractor or federal employee explicitly designated as a privileged user by the System Owner, provided they have a valid GSA email account.

Training requirements apply only to privileged accounts accessing GSA-managed systems, ensuring that training focuses on roles with direct impact on system security.

5 Compliance with Mandatory Training Requirements

Adhering to training requirements is a collective responsibility essential for safeguarding GSA assets, maintaining operational readiness, and ensuring compliance with Federal laws, and security standards. To ensure adherence to training requirements and uphold the integrity of GSA's security posture, the following structured approach is in place:

- **Automated Tracking:** Training completion is monitored through the GSA OLU reports.
- **Supervisor Accountability:** Supervisors hold direct responsibility for ensuring their teams complete the required training within the designated timelines. They play a key role in fostering compliance and addressing delays.
- **Extensions[1]:** In cases where a student is unable to complete mandatory training by the required date due to an extended absence, a management authority familiar with the student's situation can submit an extension request. Extensions are reviewed on an ad-hoc basis and ultimately operate on an honor-based system to ensure fairness and flexibility. It is important to note that students cannot submit extensions for themselves, and such submissions will be rejected.

  Extensions are accounted for in enforcement and chase processes, ensuring alignment with revised due dates for both annual and new user courses. This process is designed to balance accountability with flexibility. A detailed description of the workflows and tracking mechanisms are contained in the Training Extension SOP.
- **Enforcement Process:** Non-compliance leads to access restrictions, including network quarantine or account disablement. Temporary, limited access may be granted to allow individuals to complete their training. Full access is restored only after compliance is verified through the GSA OLU reports. Additional information can be found in Appendix E, Enforcement Playbook for Mandatory Training.

[1] Typically, 200-300 extension requests (approximately 1.5% of the student population) are submitted annually out of a total of 18,000-20,000 students.

Appendix A: Mandatory Training Topics for Cybersecurity and Privacy Awareness Training

GSA's IT Security and Privacy Awareness Training program will train personnel on the topics listed in Table A-1. This list identifies the minimal topics to be covered, additional topics may be covered. The topics are re-examined annually and updated as appropriate.

Table A-1: Training Topics

Training Topic*
IT Security Awareness Training - Cyber Threats - Protecting GSA Information Systems
Sharing Securely in a Collaborative Environment
Safeguarding GSA Sensitive Information
GSA IT Rules of Behavior

*The training topics in Table A-1 are not listed in order of importance.

Appendix B: Awareness and Training (AT) Controls

The security controls and control enhancements from NIST SP 800-53, Revision 5, Awareness and Training (AT) Control Family listed in Table B-1 are applicable at GSA. They are allocated and documented in GSA CIO-IT Security-18-90: Common Control Catalog (CCC). Specific details regarding inheritance and system responsibilities are also documented in CIO-IT Security-18-90.

IMPORTANT: The GSA Security and Privacy Awareness Training program, and therefore the controls listed in Table B-1, covers only personnel working directly for GSA.

Table B-1: AT Controls, Responsibility, and Personnel Coverage

Control ID	Control Name	Implementation Responsibility	Personnel with a gsa.gov account	Personnel without a gsa.gov account
AT-01	(Awareness and Training) Policy and Procedures	OCISO	Covered	Not Covered
AT-02	Literacy Training and Awareness	OCISO	Covered	Not Covered
AT-02 (02)	Literacy Training and Awareness | Insider Threat	Office of Mission Assurance	Covered	Not Covered
AT-02 (03)	Literacy Training and Awareness | Social Engineering and Mining	OCISO	Covered	Not Covered
AT-03	Role-Based Training	OCISO	Covered	Not Covered
AT-03(05)	Role-Based Training | Processing Personally Identifiable Information	Privacy Office	Covered	Not Covered
AT-04	Training Records	• Training provider • Individual for self-selected training	Covered	Not Covered

Appendix C: CFR to GSA Role Mapping

OPM 5 CFR Part 930.301 requires each executive agency to identify employees with significant security responsibilities and provide them with training on those responsibilities. Table C-1 provides mapping between the OPM CFR roles and GSA roles. OPM CFR roles are defined in OPM 5 CFR Part 930.301 and GSA roles are defined in CIO 2100.1.

Table C-2: CFR to GSA Role Mapping

OPM 5 CFR Part 930.301 Role	GSA Role Identified
• Executives	• AO • CISO
• Program Manager • Functional Manager	• System Owner
• Chief Information Officer (CIO) • IT Security Program Manager • Auditor • Other security-oriented personnel (e.g., System/Network administrators, System/Application Security Officers)	• CISO • ISSM • ISSO • Privileged User
• IT Function Management • Operations Personnel	• Privileged User

Appendix D: CFR to GSA Role Mapping

The tables in this appendix identify the metrics used to monitor and manage the training program. Data collection methods will vary depending on the source; some are manual, and some are automated. Sources include GSA's OLU, Sailpoint, and Splunk. Reports from Cofense Phishme will also be used for phishing campaigns.

Leadership may modify, add, or remove reporting metrics based on new areas of interest.

Table D-1: Security Awareness and Training Metrics

Metric	Description
Baseline - Count	Number of personnel assigned a module/course at the time of launch.
Completers/Non-Completers - % and Count, unadjusted	Number of people from baseline who have completed or not completed the training MINUS people on the baseline whose Active Directory account has been disabled.
Days from campaign closure to account disablement, count	The amount of time it took to disable accounts after the training campaign ended. The campaign end date is the due date for the course as specified in the GSA OLU. Used to determine if the enforcement process is improving.

Table D-2: Phishing Metrics

Metric	Description
Victims - % and Count	Percentage and number of people who fell victim (i.e., clicked) to a particular phishing scenario.
VIP Victims - % and Count	Percentage and number of Executives (pay grades of E*) or Privileged Users that fell victim (i.e., clicked) to a phishing scenario.
High Risk VIPs - Count	Executives/Privileged Users that fell victim (i.e., clicked) to more than 3 phishing scenarios over a 365 day period.
User Contact (Count)	Number of times a single user is phished over a pre-defined time period.

Appendix E: Enforcement Playbook for Mandatory Training

Purpose

Effective training compliance is essential for maintaining organizational security, operational readiness, and adherence to legal requirements.

This playbook outlines the procedures for ensuring compliance with mandatory training requirements, including:

1. Reporting training completion.
2. Management reporting.
3. Escalation procedures for non-compliance.
4. Enforcement measures, including account quarantine or disablement.

Scope

This playbook applies to:

- The **Training Manager** responsible for facilitating, monitoring, and enforcing compliance.
- Supervisors and other stakeholders involved in ensuring that employees complete required training.
- Employees required to complete mandatory training courses, such as Security Awareness and Role-Based Training.

Responsibilities

1. **Training Manager:**

    - Monitor training completion using the GSA OLU.
    - Send automated notifications and reminders to users and supervisors.
    - Generate compliance reports for management review.
    - Escalate non-compliance cases as needed.

2. **Supervisors:**

    - Ensure their direct reports complete training on time.
    - Act on notifications regarding non-compliance, including following up with employees.

3. **OCISO Leadership:**

    - Oversee campaign progress and provide guidance on escalation and enforcement actions.

4. **Employees:**

    - Complete assigned training within specified timelines.
    - Respond promptly to reminders and notifications.

Workflow

1. Reporting Training Completion:

- Training completion is tracked using the GSA OLU.
- Automated reminders are sent at pre-defined intervals to employees and supervisors based on the training schedule.
- The GSA OLU data is updated in real-time and serves as the authoritative record for compliance tracking.

2. Management Reporting:

- **Bi-Weekly Compliance Summary:** (during the first two-thirds of the campaign, shifting to weekly towards the end unless leadership requests otherwise) Generated for OCISO Leadership, including overall completion rates, department-level performance, and progress trends. In turn, the CISO can share these more widely with their peers and supervisor to ensure appropriate oversight and encourage completion.
- **Supervisor Reports:** Supervisors are CC'd on overdue reminders sent to students to keep them informed about non-compliance.

3. Escalation Procedures for Non-Compliance:

- **Remind Phase:**
  - During the campaign, students receive reminders at pre-defined thresholds prior to the due date.
  - As the due date gets near, supervisors are cc'd on the student reminders.

- **Escalation Phase (Grace Period):**
  - Students and supervisors continue receiving weekly reminders with language indicating increased urgency and consequences.
  - Additionally, chase lists are provided to the Chiefs of Staff in GSA business lines in an attempt to encourage completion prior to enforcement.

- **Enforcement Phase:**
  - Training Manager escalates persistent non-compliance to OCISO/GSA IT leadership for enforcement.
  - If compliance is still not achieved, enforcement measures are initiated.
  - For new users, enforcement is manually initiated based on leadership pre-approval.

4. Enforcement Measures:

- **Actions Taken:**
  - Quarantine accounts where technically feasible, restricting access to the GSA OLU and email. If Quarantine is not possible, accounts are disabled instead.
  - Notify employees and supervisors of the actions taken and provide instructions for regaining access upon compliance.
  - Example: In a recent campaign, 85% of quarantined accounts were reactivated within 15 days of completing the required training, demonstrating the effectiveness of timely enforcement measures.

General Framework for Enforcement Mechanisms:

1. Training Manager identifies non-compliant employees via the GSA OLU data.
2. Final reminder sent at the end of the Grace Period.
3. Decision escalated to CIO/CISO for final decision.
4. Quarantine or disablement implemented to enforce.
5. Compliance validated through the GSA OLU, and accounts reinstated upon completion of training.