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

Revision 7

September 29, 2022

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
		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

Approval

IT Security Procedural Guide: Security and Privacy Awareness and Role Based Training Program, CIO-IT Security 05-29, Revision 7, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
ED717926161544E...

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

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, Information Security Program Plan (restricted document on available to personnel with gsa.gov accounts)

1.2 Scope

Requirements in this guide apply only to GSA employees and contractors holding an enterprise network account, unless otherwise stated. Personnel operating and managing information systems on behalf of GSA (i.e., contractor-owned/contractor-operated, SaaS vendors) are not covered by this training program unless they have an active GSA enterprise network account. This guide does not apply to contractors or vendors accessing GSA systems and/or information that is publicly accessible.

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 (Administrator, Chief Information Officer)

- Ensure that GSA maintains an effective IT Security and Privacy Awareness Training Program.
- Ensure enforcement of mandatory training requirements for all GSA personnel.
- Ensure that GSA identifies personnel with significant security responsibilities.

2.2 GSA Cybersecurity and Privacy Executives (Chief Information Security Officer [CISO], Senior Agency Official for Privacy [SAOP])

- Direct the implementation of the GSA IT Security and Privacy Awareness program.
- Ensure training content with training activities is sufficient and effective for maintaining a cyber-informed workforce.
- Direct the implementation of the Role-Based Training Program that supports personnel with significant security responsibilities.
- Ensure that personnel with significant security responsibilities are aware of their responsibilities.

2.3 Supervisors/Contracting Officers

- Ensure the personnel under their purview complete the training required by this guide.

2.4 GSA IT Cybersecurity Training Manager

- Implement GSA's IT Security and Privacy Awareness Training program.
- Implement the OCISO Role-Based Security Training Program.
- Coordinate with the Chief Privacy Officer to operate/implement both training programs.
- Collaborate with other OCISO divisions to carry out phishing campaigns as part of the training program.

3 General Security and Privacy Awareness Training Program

The Security and Privacy Awareness Training Program trains personnel on basic cybersecurity and privacy practices to keep GSA systems and information safe and secure. Various methods are used to educate and evaluate student learning over time. This program has two parts: mandatory training and routine phishing simulations.

3.1 Mandatory Training

3.1.1 New Employees and Contractors

New GSA personnel must sign the GSA IT Rules of Behavior for General Users within 90 days of their Entry on Duty (EOD) date. This applies to all personnel receiving a GSA enterprise network account (i.e., Long Name Account).

3.1.2 Existing Employees and Contractors

GSA personnel must demonstrate a sufficient understanding of the topics listed in Appendix AAppendix A: every 365 days. Sufficient understanding can be demonstrated by 1) completing the IT Security and Privacy Awareness course, or 2) passing the pre-assessment for IT Security Awareness and Privacy course with a grade of 100%. This option serves as a "test out" and overrides the requirement to complete the entire IT Security and Privacy Awareness course.

3.1.3 Compliance with Mandatory Training Requirements

Demonstrating mastery of the topics listed in Appendix A: is required to maintain network access. Failure to complete the required training or "test-out" from the required training will result in loss of network access.

This enforcement action also applies to new users; failure to read and acknowledge the GSA IT Rules of Behavior for General Users document will also result in loss of network access.

3.2 Routine Phishing Simulations

Phishing simulations improve training outcomes. Therefore, OCISO will conduct routine test phishing campaigns to increase GSA personnel's awareness and reduce the likelihood that bad actors will successfully deceive them through "phishing." 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

OCISO is responsible for the management and coordination of role-based security training within GSA. Roles listed below may also complete additional security training in support of Service and Staff Office (SSO) functions.

OPM 5 CFR Part 930.301 requires each agency to identify personnel with significant security responsibilities and provide them with role-specific training. Appendix D Appendix D: CFR to GSA Role Mappingprovides a mapping between OPM 5 CFR Part 930.301 roles and GSA roles identified as having significant security responsibilities.

4.1 Training Requirements for Roles with Significant Security Responsibilities

This section describes OCISO's training requirements for roles holding significant security responsibilities within GSA. Table 4-1 summarizes the recommended training hours per role. The requirements may be met by taking courses not offered by GSA. Courses must align with a person's role/responsibilities and further their professional development.

Table 4-1: Required Training Hours Based on Role

Role	Required Hours of Training
Authorizing Official (AO)	1
Information Systems Security Manager (ISSM)	3
Information Systems Security Officer (ISSO)	3
Privileged User	1

4.1.1 Authorizing Official (AO)

AOs are the GSA executives who accept risk for GSA systems. AOs listed in the GSA FISMA Systems POC list must complete one hour of training in the following areas:

- Information security basics.
- Policy-level training in security planning and management or in emerging technologies.
- Cybersecurity posture and status updates on information systems under their purview.

AOs can satisfy this training requirement by:

- Attending an event or conference focused on security or an AO's role/responsibilities.
- Completing training provided by OCISO.
- Attending an AO briefing given by the CISO.
- Attending a monthly Security Exchange hosted by OCISO.
- Attending quarterly AO Sync meetings hosted by the OCISO.

4.1.2 Information Systems Security Manager (ISSM), Information Systems Security Officer (ISSO)

Individuals currently serving as ISSMs and ISSOs are also identified in the GSA FISMA Systems POC list. ISSOs and ISSMs are required to complete three hours of training each year which can be accomplished by:

- Completing OCISO-approved courses in GSA's Online University (OLU).
- Participating in OCISO-provided training.
- Completing OCISO-approved vendor-based security training.
- Attending a monthly Security Exchange hosted by OCISO

4.1.3 Privileged Users

A privileged user is defined as a user who:

- Holds a Short Name Account (SNA).
- Utilizes CyberArk to access any endpoint.
- Has Administrator-level privileges to a GSA system.

SSOs may further define the list of privileged users subject to this training requirement. Privileged users are required to read and acknowledge the Rules of Behavior for a Privileged User every 365 days, which satisfies the one-hour annual training requirement.

4.2 Role-Based Training

The OCISO and CPO provide specialized role-based training on a regular basis. This training is open to all GSA personnel with the responsibility to manage, operate, or authorize operations for a GSA system. Topics are selected based on emerging technologies, IT security policies and

procedures, input from team member surveys, and documentation changes that impact the group. These training sessions can be used to satisfy role-based training requirements.

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 list in Table A-1. This list is re-examined annually.

Table A-1: Training Topics

Training Topic*
Rules of Behavior for General Users
Password Management/Making good passwords
The major categories of information at GSA – PII, CUI, Unclassified
Securely sharing PII outside the organization
How to report the mishandling of PII
Cybersecurity threats
Phishing – What it is, how to prevent it, how to report it
How to securely use popular collaborative technologies (e.g., Google Apps) used by GSA
GSA Affiliated Customer Accounts (GACA)

*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 the NIST SP 800-53, Revision 5, Awareness and Training (AT) Control Family listed in Table C-1 are applicable at GSA. They are allocated and documented in GSA CIO-IT Security-18-90, Information Security Program Plan (ISPP). Specific details regarding inheritance and system responsibilities are also documented in CIO-IT Security-18-90.

IMPORTANT: The GSA Awareness Training program, and therefore the controls listed in Table B-1, covers only personnel working directly for GSA. This includes GSA contractors. Personnel operating and managing Information Systems on behalf of GSA (i.e., contractor-owned/contractor-operated, SaaS Vendors) are not covered by this training program unless they have an active GSA Enterprise Network Account.

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-1	(Awareness and Training) Policy and Procedures	OCISO	Covered	Not Covered
AT-2	Literacy Training and Awareness	OCISO	Covered	Not Covered
AT-2 (2)	Literacy Training and Awareness | Insider Threat	Office of Mission Assurance	Covered	Not Covered
AT-2 (3)	Literacy Training and Awareness | Social Engineering and Mining	OCISO	Covered	Not Covered
AT-3	Role-Based Training	OCISO	Covered	Not Covered
AT-3(3)	Role-Based Training | Practical Exercises	Privacy Office	Covered	Not Covered
AT-3(5)	Role-Based Training | Processing Personally Identifiable Information	Privacy Office	Covered	Not Covered
AT-4	Training Records	• Provider of the Training for Managed Training • Individual for self-selected training	Covered	Not Covered

Appendix C: 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, procedures for tracking phishing, and report metrics.

Appendix D: 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 D-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 D-1: 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 E: Training Program Metrics

The tables in this appendix describe the metrics used to measure and manage the IS Security and Privacy Awareness and Training program. Data collection methods will vary depending on the source; some are manual and some are automated. Sources include GSA's Online University, Sailpoint, and Splunk. Reports from Cofense Phishme will also be used for phishing campaigns. Splunk and Google Sheets are often used to perform calculations and correlations.

Some metrics may be added, modified, or removed in between updates to this guide.

Table E-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 Learning Management System (LMS). Used to determine if the enforcement process is improving.

Table E-2: Role-Based Training Metrics

Metric	Description
Quality of role-based training session, rating	A rating of how well an internal role-based training session went. Used to measure the quality of internally run training sessions within OCISO. Captured at the end of each training session via a Google form.
ISSO/ISSM training sessions, count	Number of internal training sessions that each ISSO/ISSM has attended. Used to track compliance with training requirements listed in this guide. Training sessions held by IS are tracked, others are not since the ability to track who goes to which training sessions outside of the organization does not exist.

Table E-3: Phishing Metrics

Metric	Description
Victims - % and Count	Number of people who fell victim (i.e., clicked) to a particular phishing scenario.

Metric	Description
VIP Victims - % and Count	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.