DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

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

Revision 6

May 1, 2020

Office of the Chief Information Security Officer

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

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

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

Approval

IT Security Procedural Guide: Security and Privacy Awareness and Role Based Training Program, CIO-IT Security 05-29, Revision 6, is hereby approved for distribution.

X DocuSigned by:
Bo Berlas
FD717926161544F...

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.

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

Table of Contents

Table of Figures and Tables

Note: It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

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 contractor, and aligns with agency policy and federal guidelines listed here:

- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- 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*"
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"

1.2 Scope

Requirements in this guide apply to all GSA employees and contractors holding an enterprise network account (i.e., Long Name Account), unless otherwise stated. This guide does not apply to contractors or vendors accessing GSA IT System and/or Information that is publicly accessible.

2 Roles and Responsibilities

This section lists the high-level roles and responsibilities for the Information Security (IS) Training program. Detailed responsibilities for operating and managing the IS training program are contained in standard operating procedures posted to the Office of the Chief Information Security Officer (OCISO) Wiki.

2.1 GSA Executive Leadership (i.e., Administrator, Chief Information Officer)

- Ensure that GSA creates and maintains an effective and functional IT Security and Privacy Awareness program
- Ensure enforcement of mandatory training requirements on all GSA personnel.
- Ensure that GSA identifies personnel with significant security responsibilities.

2.2 GSA Cyber and Privacy Executives (Chief Information Security Officer [CISO] and 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.

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

- 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 their employees, and/or their contractors, complete all mandatory training required under this program.
- Ensure their employees and/or supporting contractors fulfill their significant security responsibilities.

2.4 GSA IT CyberSecurity Training Manager

- Implement GSA's IT Security and Privacy Awareness program.
- Implement the OCISO role-based security training program.
- Coordinate with the Chief Privacy Officer to operate/implement both programs.
- Collaborate with other OCISO divisions to carry out phishing campaigns.

3 General Security and Privacy Awareness Training Program

The Security and Privacy Awareness training program trains personnel on basic cyber security and privacy practices to keep GSA systems and information safe and secure. A variety of methods are used to educate and evaluate student learning over time. To that end, this program has the following parts: Mandatory Training and Routine Phishing Simulations.

3.1 Mandatory Training

3.1.1 New Employees or 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 B 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 100%.

The second option serves as a "test out" and overrides the requirement to complete the entire IT Security and Privacy Awareness course.

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

3.1.3 Compliance with Mandatory Training Requirements

Demonstrating mastery of topics listed in Appendix B 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" will also result in loss of network access.

3.2 Routine Phishing Simulations

Phishing simulations improve training outcomes. Therefore, OCISO will conduct routine phishing campaigns to reduce the likelihood that a bad actor will successfully deceive a GSA person by phishing 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

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

OPM 5 CFR Part 930.301 requires each agency to identify personnel with significant security responsibilities and provide them with role-specific training. Please see Appendix E to see the mapping between OPM 5 CFR Part 930.301 and roles identified as having significant security responsibilities within GSA.

4.1 Training Requirements for Roles with Significant Security Responsibilities

This section states OCISO's training requirements for roles holding significant security responsibilities within GSA. The table below provides an overview of the required hours of training based on roles.

Table 4-1: Required Training Hours based on Role

Role	Required Hours of Training
Authorizing Official	1
Information Systems Security Manager	3
Information Systems Security Officer	3
Privileged User	1

4.1.1 Authorizing Officials (AO)

Executives, who are Authorizing Officials (AOs) listed in the OCISO FISMA Inventory, must receive 1 hour of training in 1) information security basics or 2) policy-level training in security planning and management or 3) emerging technologies 4) cyber security posture and status

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

updates on information systems under their purview. AOs are the GSA executives that accept risk for IT systems.

Authorizing Officials can meet this 1-hour requirement by:

- Completing a course listed for Authorizing Officials in Appendix B.
- Attending an event or conference listed in Appendix B.
- Completing training provided by the Office of the OCISO.
- Attending an AO briefing given by the Chief Information Security Officer.

4.1.2 Information Systems Security Managers (ISSM), Information Systems Security Officers (ISSO)

Individuals currently serving as an Information Systems Security Manager (ISSM) and Information Systems Security Officer (ISSO) are also identified in GSA's FISMA inventory. ISSO/ISSMs are required to complete 3 hours of training each year, and can be accomplished by:

- Completing OCISO-approved courses in GSA's Online University (OLU) (See Appendix B).
- Participating in OCISO provided training.
- Completing OCISO-approved vendor-based security training.

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 end-point.
- Has Admin-Level privileges to a GSA information system.

S/SO 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. Completing the "Rules of Behavior for a Privileged User" satisfies the 1-hour annual 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 who have the responsibility to manage, operate, or authorize operations for a GSA information 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 training requirements listed in section 4.1 above.

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

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

GSA's IT Security and Privacy Awareness training will contain content aligned with these topics. This list will be re-examined annually and updated with topics considered mandatory by Executive Leadership.

Table A-1: Training Topics

Topic (not in order of importance)
Cybersecurity threats
Phishing – What is, how to prevent, how to report
The major categories of information at GSA – PII, CUI, Unclassified
How to report the mishandling of PII
Securely sharing PII outside the organization
Rules of Behavior for General Users
How to securely use popular collaborative technologies (e.g., Google Apps) used by GSA
GSA Affiliated Customer Accounts (GACA)
Password Management / Making good passwords

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

Appendix B: OCISO-Approved Courses for Roles with Significant Security Responsibilities

Requirements in Section 4.1 can be met by taking training course not offered by GSA. Courses should align with the person's significant security responsibilities and further their professional development. The OCISO Wiki will be updated the training platforms personnel can use to satisfy these requirements. Specific courses may also be listed. Check the OCISO Wiki for the latest.

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

Appendix C: Awareness and Training (AT) Controls that FISMA Systems Can Inherit

The four security controls and one control enhancement from the NIST SP 800-53, Revision 4, Awareness and Training (AT) Control Family listed below are allocated and documented in GSA CIO-IT Security-18-90, "*Information Security Program Plan*", as follows. Specific details regarding inheritance and system responsibilities are in CIO-IT Security-18-90.

Note: Even though a control is marked as Common, a system may decide to augment the control implementation for their system if there is a determination that additional training is required beyond the training provided by the common training.

Table C-1: Inheritable AT Controls

Control ID	Control Name	Federal (Internal) System Control Type	Vendor/Contractor System Control Type
AT-1	Security Awareness and Training Policy and Procedures	Common	Hybrid
AT-2	Security Awareness Training	Common	System Specific
AT-2 (2)	Security Awareness Training | Insider Threat	Common	System Specific
AT-3	Role-based Security Training	Common	Hybrid
AT-4	Security Training Records	Common	Hybrid

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

Appendix D: Supplemental Artifacts Supporting OCISO Training Program

Artifacts describing or supporting the operation of the OCISO training program are posted to the OCISO Wiki throughout the year. Artifacts may include but are not limited to organizational charts for the IS Training organization, procedures for tracking phishing, and report metrics.

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

Appendix E: 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 training on those responsibilities. Therefore, a mapping between these roles and the GSA Information Security program is needed. The table below meets that need. This table aligns positions outlined in OPM 5 CFR Part 930.301 to roles defined in CIO 2100.1.

Table E-1: CFR to GSA Role Mapping

OPM 5 CFR Part 930.301 Role	GSA Role Identified
"Executives"	Authorizing Official/Chief Information Security Officer (CISO)
"Program and functional managers"	System Owner
"Chief Information Officers (CIOs), IT security program managers, auditors, and other security-oriented personnel (e.g., system and network administrators, and system/application security officers)"	Chief Information Security Officer (CISO) Information System Security Manager (ISSM) Information System Security Officer (ISSO) Privileged User
"IT function management and operations personnel"	Privileged User

DocuSign Envelope ID: 12D0E0CB-B0F8-4ECF-BD36-24AB61FCDCA5

Appendix F: Training Program Metrics

This appendix lists 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 manual, some automated. Sources include GSA's Online University, Sailpoint, and Splunk (CDM). Reports from Cofense Phishme will also be used for phishing campaigns. Splunk and Google Sheets are often used to perform calculations and correlations on these data sets.

Some metrics may be added, modified, or removed in between updates to this guide. Check the OCISO Wiki for the latest metrics being captured.

Security Awareness and Training Metrics

Baseline - Count - Number of personnel assigned a module/course at the exact time of launch.

Completers/Non-Completers - % and Count, unadjusted - Number of people from baseline that have completed or not completed the training ***MINUS*** people on the baseline who's Active Directory account has been disabled.

Average Duration To Completion, per Course Module - How long did it take a person to finish each module on the course. Used to determine if estimated duration for course completion is accurate and in-line with time actually spent by people taking the course.

Days from campaign closure to account disablement, count - How long did it take to disable accounts after the training campaign ended? The campaign end date is the due date for the course as specified in the LMS. Used to determine if the enforcement process is improving.

Role-Based Training Metrics

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-ran 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 we don't have the ability to track who goes to what training sessions outside for the organization.

Phishing Metrics

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

VIP Victims - % and Count - Executives (pay grades of E*) or Privileged Users that fell victim (i.e., clicked) to phishing scenario

High Risk VIPs - Count - Executives/Privileged Users that fell victim (i.e., clicked) to more than 3 phishing scenarios over 365 day period.

User Contact (Count) - Number of times a single user is phished over a pre-defined time period.