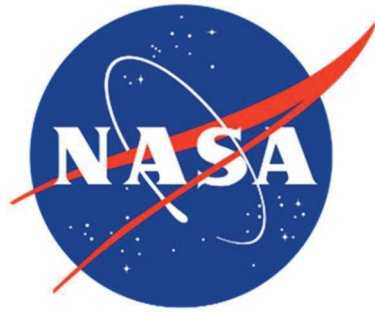




Information Technology Security Handbook

Cybersecurity and Privacy Awareness, Training, and Education

September 2022

Version 4

OFFICE OF THE CHIEF INFORMATION OFFICER

CYBERSECURITY AND PRIVACY DIVISION

Document Properties

- **Maintained by:** OCIO CSPD Team
- **Filename:** ITS-HBK-2810.06-2B
- **Supersedes:**
 - Version 3.0

Table 1: Revision History

Version	Date	Change Description
1.0	05/20/2019	Update and consolidation of Awareness and Training handbooks; addition of supplemental phishing training and Individual development training.
2.0	05/21/2020	Update with the requirement to use SATERN as the authoritative system of record for tracking Annual Cybersecurity and Sensitive Unclassified Information Awareness Training.
3.0	8/24/2020	Update with new requirements prohibiting substitute training to satisfy the mandatory awareness training requirement.
4.0	09/20/2022	Clarified introduction; updated references

Table of Contents

1.	INTRODUCTION	1
2.	PURPOSE	2
2.1	Scope	2
3.	POINT(S) OF CONTACT FOR HANDBOOK	3
4.	APPLICABILITY	3
5.	APPLICABLE DOCUMENTS	3
6.	SECURITY CONTROLS AND CORRESPONDING ROLES AND RESPONSIBILITIES	4
6.1	Security Awareness Training (AT-2)	4
6.2	Role-Based Security Training (AT-3)	5
6.3	Training Records (AT-4)	8
6.4	Reporting	8
6.5	Phishing Supplemental Training Requirement	8
7.	SATERN	10
7.1	Accessing SATERN	10
APPENDIX A: External Role-Based Training Validation Form		11
APPENDIX B: Acronyms		12
APPENDIX C: GLOSSARY		14

This page intentionally left blank.

Distribution:
NODIS



Associate Chief Information Officer for
Cybersecurity & Privacy

1. INTRODUCTION

The *Cybersecurity and Privacy Awareness, Training and Education* handbook describes the requirements for the National Aeronautics and Space Administration's (NASA) Cybersecurity Training Program for all Agency employees and contractors, including individuals with significant security responsibilities (SSR). The handbook also establishes role-based training standards.

Cybersecurity and privacy awareness training is required for all personnel with access to NASA information and information systems. The handbook describes the cybersecurity training requirements for all Agency employees and contractors specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* (See Applicable Document section). The handbook also satisfies the requirements for security and awareness training in the Federal Information Security Modernization Act of 2014, and Title 5, Administrative Personnel, of the Code of Federal Regulations § 930. Additionally, all NASA authorized holders shall complete initial Controlled Unclassified Information (CUI) awareness training subject to education and training requirements set out in NASA Procedural Requirements (NPR) 2810.7, Controlled Unclassified Information (CUI).

NPR 2810.1A, Security of Information Technology, designates the Cybersecurity and Privacy Awareness, Training and Education handbook as a guide for NASA's Awareness and Training (AT) information security controls. The handbook supports the implementation of requirements in NPR 2810.1, and NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy. The content of this document, in conjunction with NPD/R 2810.1, defines NASA policy and procedures to address AT-1. It also augments NIST guidance with NASA-specific requirements, procedures, and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance unless explicitly stated. The Agency's organizationally defined values are integrated into the control requirements within the Risk Information Security Compliance System (RISCS), the Agency system of records.

Individuals with significant security responsibilities require additional training under the NIST Awareness and Training 3 (AT-3) Security Training control in NIST SP 800-53. Individuals with Agency or Center-assigned roles who may significantly impact cybersecurity are designated as SSRs. SSR role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. SSRs are also users with privileged network user accounts and/or managerial, administration, or operational responsibilities that enable them to affect a system or information security.

This handbook also addresses supplemental phishing training required for IT users who have been identified as being susceptible to phishing threats. This supplemental training expands upon the phishing threat training provided in the new employee and annual cybersecurity awareness training required for all NASA employees and contractors.

The Security Awareness and Training control family relates to the information security knowledge requirements for all users of Agency information and information systems, and the development and delivery of courses and other training resources to enable and validate satisfaction of those requirements.

NASA users are responsible for meeting Agency security training requirements to gain and maintain access to any NASA information system resource.

Organization-defined values (ODVs) are managed by the Cybersecurity Standards and Engineering Team (CSET). They are published at <https://cset.nasa.gov> under the specification name NASA-SPEC-2661. Where any ODVs in this handbook are different than the ODVs published by CSET, the CSET ODVs shall take precedence.

2. PURPOSE

Learning is a continuum. It starts with awareness, builds to training, and evolves into education. An effective cybersecurity and privacy awareness and training program provides best practices and explains proper rules of behavior for the use of agency IT systems and information. The program communicates IT security policies and procedures that need to be followed. This must precede and lay the basis for any sanctions imposed due to noncompliance. Users first should be informed of the expectations. Accountability must be derived from a fully informed, well-trained, and aware workforce.

This document provides guidelines for maintaining a comprehensive awareness and training program, as part of NASA's cybersecurity program. Federal agencies and organizations cannot protect the confidentiality, integrity, and availability of information in today's highly networked systems environment without ensuring that all people involved in using and managing IT understand their roles and responsibilities related to the organizational mission, understand the organization's IT security policy, procedures, and practices, and have at least adequate knowledge of the various management, operational, and technical controls required and available to protect the IT resources for which they are responsible. Initial and annual cybersecurity and privacy awareness training will help reinforce these requirements so that personnel understand their IT security responsibilities, organizational policies, and how to properly use, maintain privacy while online and protect the IT resources entrusted to them.

Regarding role-based training, to protect NASA's information, IT and other information resources, NASA must ensure that individuals with Significant Security Responsibilities (SSR) are equipped with the necessary knowledge to accomplish their tasks. SSR applies to any individual who is assigned a role within the Agency that may have a significant impact on security. This IT security handbook, defines and documents the groups of individuals NASA identifies as having SSR. Additionally, this handbook defines the initial and continuing education training requirements for individuals with SSR.

2.1 Scope

The requirements in this handbook apply to all users who access NASA IT resources (e.g., workstations, laptops, and mobile devices) and access, process, store, receive, or transmit NASA information. Failure to complete mandatory awareness and training requirements within the specified timeframe will adversely impact access to, and use of, NASA-owned or NASA-controlled systems, networks, and information.

Although NASA handbooks may contain "shall" (requirements) statements, they are not intended to be requirements documents. Pursuant to NPR 1400.1K, portions of NASA handbooks containing procedural, or process guidance may be cited in contract, program, and other Agency documents, and may become requirements when a NASA directive specifies their use by citing the document title, revision letter/number, and date; or, when a NASA manager with authority over a NASA program, project, or other activity, identifies it as a requirement.

A documented rationale and/or justification shall accompany any non-concurrence, disapproval, denial, or request

for deviation from the policy guidance or procedural requirements set forth in this handbook to support such decision. The documented rational/justification shall be provided to the NASA Cybersecurity and Privacy Division (CSPD) and the point of contact for this handbook, in coordination with Center Information Security Officers (CISO), to review and validate for the record.

3. POINT(S) OF CONTACT FOR HANDBOOK

For any questions or comments regarding the contents of this Handbook contact:

- hq-dl-cspd-policy@mail.nasa.gov

Any questions or concerns regarding perceived gaps in policy or implementation guidance, conflicting procedural requirements, lack of clarity pertaining to specified roles and responsibilities, or issues associated with interpretation shall be elevated to the NASA CSPD, in coordination with the CISO, and directed to the attention of the point of contact for this particular handbook to address and resolve.

4. APPLICABILITY

This handbook is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. The language applies to the Jet Propulsion Laboratory (JPL), a Federally Funded Research and Development Center (FFRDC), other contractors, authorized users, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

5. APPLICABLE DOCUMENTS

Federal Law

- The Computer Security Act of 1987
- Federal Information Security Modernization Act of 2014 (FISMA)

Office of Personnel Management (OPM) and Office of Management and Budget (OMB)

- OPM Title 5 Code of Federal Regulations (CFR) § 930.301
 - Information systems security awareness training program
 - Subpart C, Information Security Responsibilities for Employees who Manage or Use Federal Information Systems
- OMB Circular A-130, Management of Federal Automated Information Resources, Appendix III, Security of Federal Automated Information Resources § 3(a)(2)(b)

Federal Information Processing Standards (FIPS)

- FIPS 199, Standards for Security Categorization for Federal Information and Information Systems
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems

National Institute of Standards and Technology (NIST)

- NIST Special Publication (SP) 800-16, Information Training Security Requirements; A Role- and Performance-Based Model or replacement

- NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
- NIST SP 800-50, Building an Information Technology Security Awareness and Training Program
- NIST SP 800-53, Rev. 5, Recommended Security Controls for Federal Information Systems and Organizations

National Aeronautics and Space Administration (NASA)

- NPD 1382.17J, NASA Privacy Policy
 - NPR 2800.1, Managing Information Technology
 - NPD 2810.1F, NASA Information Security Policy
 - NPR 2810.7, Controlled Unclassified Information
 - NPR 1382.1, NASA Privacy Procedural Requirements
 - NPR 1441.1, NASA Records Management Program Requirements
 - NPR 2810.1F, Security of Information and Information Systems
 - NPD 2810.1, NASA Information Security Policy
 - ITS-HBK-2810-002.1, Format and Procedures for IT Security Policies and Handbooks
 - ITS-HBK-2810.15-02, Access Control and Elevated Privileges
 - ITS-HBK 1382.08-01, *Privacy Training*
-
- Standard Form (SF)-182, Request, Authorization, Agreement and Certification of Training
-
- External Role-Based Training Validation Form

Cancellations, Updates, Consolidations

- ITS-HBK-2810.06.-2B, IT Security Awareness, Training, and Education

6. SECURITY CONTROLS AND CORRESPONDING ROLES AND RESPONSIBILITIES

6.1 Security Awareness Training (AT-2)

- ***The Senior Agency Information Security Officer (SAISO):***
 - Ensures the availability of annual cybersecurity and CUI awareness training for the Agency.
 - Ensures documentation of training completion to specify where a user can complete the training at any point during the calendar year or whether the training should be completed on a rolling annual basis.
- ***The IT Security Awareness and Training Center (ITSATC): Lead***
 - Authors and maintains security awareness training for use across the Agency.
 - Uses the NASA SATERN (System for Administration, Training, and Education Resources) and NAMS platforms as a mechanism to upload, manage, track, and record security awareness training.
 - Monitors the training status to ensure NPR 2810.1, Security of Information and Information Systems, is implemented and effective across the Agency and ensures that annual trainings are completed.
- ***The Center CISO:***
 - Maintains oversight of information security awareness training completion by Center personnel through SATERN.

- Designates Cybersecurity Training Managers (CTMs) for IT Security Training.
- Ensures the delivery of training to personnel through alternative means for all NASA badged users with physical access only, when necessary and approved by CSPD.
- ***The Center Cybersecurity Training Managers:***
 - Supports the Center CISO in ensuring compliance with the FISMA metrics for annual awareness training and role-based IT Security training.
 - Serves as Center POC for questions and issues regarding the requirements of this Handbook.
 - Serves as liaison between the ITSATC, Center CISO, and the individuals who are required to take all mandatory annual training and role-based training.
- ***The ISSO:***
 - Maintains oversight of information security awareness training completion by personnel with access to information systems under their control or purview.
- ***The ISO:***
 - Prior to authorizing access, and annually thereafter, ensures 100 percent of users with login access to information systems or applications under their purview complete annual Cybersecurity and Privacy Awareness Course.
 - Ensures that user access to NASA information systems or applications under their purview is terminated, including the administrative and/or privileged access, if the required annual or other specified information security-related training is not completed.
- ***The NASA User:***
 - Completes the Cybersecurity and Privacy Awareness Course before accessing NASA information systems and applications. The course is an annual requirement for NASA users.
 - Onboarding/New Hires. All introductory training requirements should be satisfied before new NASA personnel gain logical and/or physical access to NASA IT systems or NASA facilities. Otherwise, new NASA personnel shall complete training requirements within ten (10) days of obtaining a PIV card. For all NASA badged users with logical access, complete the training in SATERN. For all NASA badged users with physical access only, complete the annual awareness training and record it in IDMAX. Astronauts assigned to space travel must complete training before flight.

6.2 Role-Based Security Training (AT-3)

The IT security training requirements for each of the roles outlined in this document are summarized on the ITSATC website. For additional information on NASA training reference for Role-Based Training URL at <https://nasa.sharepoint.com/sites/itsatc/SitePages/Role-Based-Training.aspx>.

- The following roles are assigned based on an individual's job description and title:
 - NASA CIO and Deputies
 - Center CIOs and Deputies

- SAISO and Deputy SAISO
 - Center CISOs and Deputies
 - [Center] Agency Privacy Managers (C/APM)
 - [Center] Cybersecurity Risk Managers (C/CRM)
 - Incident Responders
 - Agency and Center Incident Response Managers (IRM)
- The following roles are assigned based on an individual's role with respect to a System Security Plan (SSP) recorded in RISCs:
 - Authorizing Official (AO)
 - Information System Owner (ISO)
 - Information Owner (IO)
 - Information System Security Engineer (ISSE)
 - Information System Security Officer (ISSO)
 - Security Control Assessor (SCA)
- The following NASA roles are designated as having SSR:
 - AO
 - Center CIO and Deputy
 - Center CISO and Deputy
 - CPMs
 - IO
 - Incident Responder
 - IRM
 - ISO
 - ISSE
 - ISSO
 - NASA CIO and Deputies
 - SAISO
 - SCA
- The ITSATC Lead:
 - Identifies and document those roles that have significant information security responsibilities that require initial and annual role-based information security training in accordance with NIST SP 800-16, Information Training Security Requirements; A Role- and Performance-Based Model.
 - Identifies training that will satisfy the role-based IT Security training requirements and reviews it annually to incorporate updates or lessons learned when appropriate.
 - Maintains a list of valid SSR training offerings that satisfy the requirements in this handbook on the ITSATC website.
 - Creates and acquires courses within SATERN that are assigned to the roles identified in this handbook.
 - Provides reports to CTMs regarding the completion training requirements.
 - Compiles performance metrics on training requirements for Center verification and reporting to FISMA.
 - Provides ad-hoc status reports on the completion of the requirements of this handbook to Centers and Agency IT security personnel to show the progress of

- efforts to comply with training requirements.
- Provides monthly reports to the Center CISOs and the Agency CSPD on the number of individuals (at each Center and within the Agency) with SSR for each role and if they have met annual training requirements.
 - Reporting for SSR shall be derived from SATERN for all roles except elevated privileges (EP). EP is reported through the NASA Account Management System (NAMS): refer to ITS-HBK-2810.15-02, Access Control and Elevated Privileges for details on EP.
- **The Center CIO:**
 - Maintains oversight of the completion of role-based information security training to ensure initial and annual refresher training is completed by Center personnel approved for administrative and/or privileged access to NASA information, information systems and/or IT resources, in accordance with procedures outlined by ITS-HBK-2810.15-02, Access Control and Elevated Privileges.
- **The Center CISO:**
 - Provides initial list to the ITSATC and notify the ITSATC when changes are made to the list.
 - Ensures that Center individuals with SSR comply with the requirements outlined within this handbook.
 - Verifies Center FISMA training metrics are properly reported.
- **The ISSO:**
 - Maintains oversight of the completion of role-based information security training to ensure initial and annual refresher training is completed by organizational personnel approved for administrative and/or privileged access to NASA information, information systems and/or IT resources, in accordance with procedures outlined by ITS-HBK-2810.15-02, Access Control and Elevated Privileges.
- **The ISO:**
 - Ensures roles with SSR and/or EP are documented in the SSP.
 - Ensures the individuals with SSR and/or EP:
 - Complete required role-based training and capable of performing assigned roles and responsibilities.
 - Complete annual refresher training as required.
- **The NASA User with SSR:**
 - Completes appropriate role-based information security-related training, as outlined in ITS-HBK-2810.15-02, Access Control; Managed Elevated Privileges, that addresses the procedures and processes necessary to meet the security requirements of the role before being authorized privileged access to the information, information system and/or IT resources and complete the training annually thereafter.
 - If the user completes appropriate training other than that recommended by ITSATC, they should complete the External Role-Based Training Validation form per Appendix, and submit it to ITSATC with either Center CISO or

- Training POC approval. The following information shall be documented in SATERN for each training item completed:
 - Training name
 - Location
 - Training type
 - Description of content
 - Date(s) of training
 - Number of hours
 - Vendor (or instructor if internal)
- Reports role changes to the Center CISOs and the Center CTM.

6.3 Training Records (AT-4)

- **The SAISO:**
 - Provides oversight of Information Security Awareness Training and role-based information security training is tracked using the SATERN Learning Management System (LMS) and training records destroyed 5-years after separation of employee or when no longer needed in accordance with NPR 1441.1E, *NASA Records Management Program Requirements*.
- **The ITSATC Lead:**
 - Maintains and tracks all NASA information security awareness training and role-based training documentation and modules.
 - Uses SATERN to:
 - Assign and monitor progress of Information Security Awareness training compliance.
 - Track employee role-based information security training requirements and completion status.
 - Maintain a central repository for all NASA information security-related training documentation.
- **The NASA User:**
 - Ensures their training records are up to date and reflect completion of all mandatory, role-based, and individual development training requirements.

6.4 Reporting

The ITSATC shall provide monthly reports to the Center CISOs and the Agency CSPD on the status of all mandatory annual IT security training and role-based training requirements for NASA personnel.

- Reporting for SSR shall be derived from SATERN for all roles except EP. This reporting will identify, on a Center and Agency basis, the number of individuals with SSR for each role and if they have met the annual training requirements.
- Reporting for individuals with EP shall be completed using the process associated with the NASA Account Management System (NAMS), as NAMS processes validate the training requirements prior to granting EP.

6.5 Phishing Supplemental Training Requirement

Supplemental phishing training is not a NIST SP 800-53 control, but it is an important requirement with

associated roles and responsibilities.

Phishing is the act of soliciting personal or sensitive information or tricking IT users into running malicious software through e-mail or websites while posing as a legitimate associate or business. Phishing is recognized throughout the government and the private sector to be one of the most prevalent methods for malicious actors to gain unauthorized access to IT systems, networks, and data. To mitigate this threat, NASA has included phishing awareness information in the annual *Cybersecurity and Privacy Awareness Course* that is already mandated for all NASA IT users.

The NASA OCIO conducts periodic phishing exercises to measure the effectiveness of training and further increase awareness. As part of these periodic exercises, the OCIO identifies users who appear to need increased awareness of the threat that phishing poses to NASA when IT users improperly respond to real phishing e-mails. NASA OCIO has defined a “recurring clicker” as a NASA IT user who clicks on a link or provides data in response to a test e-mail sent during an OCIO phishing exercise at least twice within three consecutive exercises.

Supplemental training about phishing is required for select NASA IT users who have been identified as susceptible to phishing threats. This training expands upon the phishing threat training provided in the new employee and annual Cybersecurity Awareness Training required for all NASA employees.

As with any mandatory annual training requirement, failure to complete this training requirement within the specified timeframe will adversely impact access to, and use of, NASA-owned or NASA-controlled systems, networks, and information.

- **The *NASA CIO*:**
 - Promulgates policies, procedures, and processes related to phishing training requirements.
- **The *SAISO*:**
 - Oversees implementation of mandatory training requirement focused on those NASA IT users that are susceptible to phishing threats and serves as the point of contact for questions.
- **The *ITSATC Lead*:**
 - Works with CSPD to ensure that training associated with phishing exercises coincide with ITSATC provided mandatory training.
 - Distributes supplemental phishing training materials to the Center CISOs to support instructor-led anti-phishing training when requested.
 - Supplies the NASA Shared Services Center (NSSC) with anti-phishing training materials to be put into SATERN for self-paced computer-based training when requested.
 - Tracks completion of supplemental training requirements when requested.
- **The *Center CISO*:**
 - Oversees the implementation/enforcement of the anti-phishing training requirement and ensures that training is completed within 60 days of employee

- notification.
 - Grants employee extensions to the 60-day completion requirement upon receipt of adequate justification from the employee (e.g., extended leave, medical reasons).
 - Ensures that user access to NASA information systems or applications under their purview is suspended, including the administrative and/or privileged access, for those employees who fail to successfully complete anti-phishing training and anti-phishing exercises, as appropriate.
- **The NASA User:**
 - Completes the mandatory training requirement within the specified timeframe and ensure their records in SATERN reflect completion of the training.
 - Note: Failure to complete these training requirements promptly will result in loss of IT privileges such as access to, and use of, NASA-owned or NASA-controlled systems, networks, and information.

7. SATERN

SATERN provides web-based access to training and career development resources. A full list of recommended training is located at <https://nasa.sharepoint.com/sites/itsatc/>. SATERN is the designated system used to track and record training completions for NASA-badged employees and contractors with logical IT access. No exceptions, or substitute trainings will be permitted to meet the requirement for mandatory annual awareness training.

7.1 Accessing SATERN

To access SATERN, launch your Internet browser and go to <https://satern.nasa.gov>. For help, visit the SATERN Informational Web site at <https://saterninfo.nasa.gov>. Navigate to “Resources > Guides & Aids” and click “How do I log into SATERN?” job aid for step-by-step instructions. For assistance with SATERN, contact the NSSC Contact Center at 877-677-2123 or nssc-contact@nasa.gov.

APPENDIX A: EXTERNAL ROLE-BASED TRAINING VALIDATION FORM

The *SF-182 Request, Authorization, Agreement, and Certification of Training* is the official form for all external specialized and role-based training requests. Eligible NASA civil servants may submit a request for external training (e.g., conferences, academic courses, and other external events) via the SF-182 form. NASA employees submit electronic requests for external training online and have them automatically approved, tracked, and recorded in SATERN.

After employees attend/complete training, they will receive an e-mail notification to complete the mandatory SATERN online verification. If they attended an academic course, they are required to submit their final grade to their Center training office. Employees must complete the verification and submit their final grade to receive credit on their Learning History. Individuals with SSR designations may complete courses other than those recommended with the approval of their Center CISO or ITS Training POCs. The External Role-Based Training Validation Form must be completed and signed by either the Center CISO or the Center CTM.

Individuals with Significant Security Responsibilities (SSR) are required to complete mandatory training annually according to the NASA Role-Based Training Handbook (HBK) 2810. To support this requirement, for each role, courses have been selected from the internal IT Security library (NASA ITS) and vendor-constructed courses (Skillsoft and ITPro TV). But, as an incumbent in the role, the users are permitted to elect an external course that is approved as a substitute to the NASA recommended internal training courses. The External Role-Based Training Validation Form is available at <https://nasa.sharepoint.com/sites/itsatc/SitePages/RBT-Validation-Form.aspx>.



National Aeronautics and
Space Administration



EXTERNAL ROLE-BASED TRAINING VALIDATION FORM

Individuals with Significant Security Responsibilities (SSR) are required to complete mandatory training annually according to the NASA Role Based Training Handbook (HBK) 2810. To support this requirement, for each role, courses have been selected from the internal IT Security library (NASA ITS) and vendor-constructed courses (Skillsoft and ITPro TV). However, as an incumbent in the role, you are permitted to elect an external course that is approved as a substitute to the NASA recommended internal training courses.

Upon electing an external course, this form must be completed to document and validate your completion of the training requirement.

1. Identify a course and receive approval from the CISO or ITSEC POC.
2. Complete the course and fill in the information detailing the training in the table below.
3. Sign and date the form.
4. Email or print out a copy and obtain a signature from an IT Security Professional at your center as a validation of the appropriateness of the completed training to your assigned role that has significant security responsibilities.
5. Send the signed form and a scanned copy of training completion certificates for each item listed below and mail to:
Agency-DL-External-RBT-Validation@mail.nasa.gov.

Duration (Hours)	Title of the Training Event	Completion Date	Location (City, State)

Print Learner Name

Print CISO (or IT Sec POC) Name

Learner's Digital Signature

CISO (or IT Sec POC) Digital Signature

Date

Date

APPENDIX B: ACRONYMS

AO	Authorizing Official
ACES	Agency Consolidated End-User Services
AT	Awareness and Training
CAP	Certified Authorization Professional
CSPD	Cybersecurity and Privacy Division
CIO	Chief Information Officer
CISM	Certified Information Security Manager
CISO	[Center] Chief Information Security Officer
CISSP	Certified Information Systems Security Professional
CPM	Center Privacy Manager
CSSLP	Certified Secure Software Lifecycle Professional
CTM	Cybersecurity Training Manager
EP	Elevated Privilege
CUI	Controlled Unclassified Information
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HBK	Handbook
IDP	Individual Development Plan
IO	Information Owner
IRM	Incident Response Manager
ISO	Information System Owner
ISSE	Information System Security Engineer
ISSO	Information System Security Officer
IT	Information Technology
ITS	Information Technology Security
ITSATC	Information Technology Security Awareness and Training Center

LMS	Learning Management System
NAMS	NASA Account Management System
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
NSSC	NASA Shared Services Center
OCIO	Office of the Chief Information Officer
OHCM	Office of Human Capital Management
OPM	Office of Personnel Management
OS	Operating System
PM	Program Manager
SA	System Administrator
SAISO	Senior Agency Information Security Officer
SATERN	System for Administration, Training, and Education Resources for NASA
SCA	Security Control Assessment
SOC	Security Operations Center
SP	Special Publication
SR	Service Request
SSR	Significant Security Responsibilities
SSP	System Security Plan

APPENDIX C: GLOSSARY

Awareness	The ability of the user to recognize or avoid behaviors that would compromise cybersecurity; the practice of good behaviors that will maintain cybersecurity; and act wisely and cautiously, where judgment is needed, to support organizational cybersecurity. Awareness is not training, although training can promote awareness. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly.
Education	Knowledge or skill obtained or developed by a learning process. Education integrates all the security skills and competencies of the various functional specialties into a common body of knowledge, with the goal of producing IT security specialists and professionals capable of vision and pro-active response.
Role	The responsibility and functions that a person is performing within their agency; established by individual Federal organization or agency through position descriptions, hierarchy charts, responsibilities, etc.
Training	The action provided to a user in the acquisition of knowledge, skills, and competencies. The training level of the learning continuum strived to produce relevant and needed security skills and competencies by practitioners of functional specialties in addition to IT security (e.g., management, systems design, and development, acquisition, auditing).