
EPA Classification No.:	CIO-2150.3-P-02.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

*Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005*

**INFORMATION SECURITY –
INTERIM AWARENESS AND TRAINING PROCEDURES**

V3.1

JULY 18, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Awareness and Training control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*.

2. SCOPE AND APPLICABILITY

These procedures cover all EPA information and information systems to include those used, managed, or operated by a contractor, another agency, or other organization on behalf of the Agency.

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operation and assets of EPA.

3. AUDIENCE

These procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of EPA.

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that all Offices within the Agency meet the minimum security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*. All EPA information systems must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the awareness and training family of controls found in NIST SP 800-53, Revision 3.

EPA Classification No.: CIO-2150.3-P-02.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III, *Federal Information Security Management Act (FISMA)* as amended
 - Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
 - Clinger-Cohen Act of 1996, Public Law 104-106
 - Paperwork Reduction Act of 1995 (44 USC 3501-3519)
 - Privacy Act of 1974 (5 USC § 552a) as amended
 - USA PATRIOT Act of 2001, Public Law 107-56
 - Code of Federal Regulations, Part 5 Administrative Personnel, Subpart C—*Employees Responsible for the Management or Use of Federal Computer Systems*, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
 - Office of Management and Budget (OMB) Circular A-130, “*Management of Federal Information Resources*”, Appendix III, “*Security of Federal Information Resources*”, November 2000
 - Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
 - FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 2006
 - EPA Information Security Program Plan
 - EPA Information Security Policy
-

6. PROCEDURES

AT-2 – Security Awareness

- a. All users, including managers, senior executives, and contractors shall complete basic information system security awareness training as part of initial training for new users, when required by system changes, and annually thereafter.
- b. EPA shall determine the appropriate content of the basic information system security awareness training materials and security awareness techniques based on specific requirements of the organization, federal regulations, and the information systems to which personnel have authorized access.
 - i. Awareness level training must be a minimum of 15 minutes annually.

Note: Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.

EPA Classification No.: CIO-2150.3-P-02.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- c. The content of EPA's security awareness program must include:
 - i. A basic understanding of the need for information security.
 - ii. User actions to maintain security.
 - iii. User actions to respond to suspected security incidents.
 - Refer to *Information Security – Incident Response Procedures* for requirements on responding to security incidents.
 - iv. Awareness of the need for operations security as it relates to EPA's information security program.
- d. Each program office, Region, and Lab shall augment security awareness training by mechanisms (e.g., "message of the day," posters, special events, email notices) it deems necessary to address local or programmatic information security issues, incidents, policies, and procedures.

AT-3 – Security Training

- a. All users shall complete role-based security-related training:
 - i. Before they are permitted access to an information system or performing assigned duties.
 - ii. When required by system changes.
 - iii. Annually thereafter.
- b. EPA shall determine the appropriate content of the security training based on assigned roles and responsibilities and the specific requirements of the information systems to which personnel have authorized access.
- c. All users who have already completed information system security training and who are appointed to a new position that requires additional role-based security-related training shall complete the relevant training within 60 days of appointment.
- d. EPA shall provide adequate security-related technical training to the following individuals in order for them to perform their assigned duties:
 - i. Information system managers.
 - ii. System and network administrators.
 - iii. Personnel performing independent verification and validation (IV&V) activities.
 - iv. Security control assessors.
 - v. Other personnel having access to system-level software.
- e. All users shall, on an annual basis, complete the training hours as specified below for each of the subject areas required for their role (identified as "Audience" in *Appendix E*).
 - i. Awareness level training must be a minimum of 15 minutes annually.
 - ii. Policy level training must be a minimum of 1 hour.
 - iii. Broad Level training must be a minimum of 1 hour in each subject area.
 - iv. Management level training must be a minimum of 1 hour in each subject area.

EPA Classification No.: CIO-2150.3-P-02.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- v. Implementation level training must be a minimum of 1 hour in each subject area.
- f. Refer to *Appendix D* of this document for more information on training levels, and *Appendix E* for more information on subject areas.
- g. Security training must address management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures.
- h. EPA shall provide the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization's information security program.
- i. Security training must be consistent with requirements contained in 5 C.F.R. Part 930.301, NIST SP 800-16 and 800-50, and *Appendices B, C, D, and E* of this document.
- j. EPA shall develop Agency-specific certification courses for the administrative functions for each technology platform (e.g., Oracle, UNIX, Windows) as necessary, to administer the technology in accordance with unique Agency requirements. These certification courses must not duplicate or replace commercial training certifications or courses designed to provide certification or instruction on vendor or industry operational or administrative practices for technology.
- k. EPA platform administrators shall satisfactorily complete EPA-required platform certification courses prior to assuming unsupervised administrator duties.
- l. Security awareness and training content must be obtained from the most economical and relevant sources. Some relevant sources include, but are not limited to, the following:
 - i. A security and awareness training provider in accordance with the Information Systems Security Line of Business.
 - ii. Content that is developed or provided in-house.
 - iii. Another governmental agency.
 - iv. Commercial vendors.
- m. Security and awareness training must be no more than one critical element in all of an employee's performance standards, which may be found in the Performance Appraisal and Recognition System (PARS).
- n. EPA personnel, contractors, or others working on behalf of EPA with significant security responsibilities (e.g., ISSOs, system administrators) shall receive initial specialized training, and annual refresher training thereafter, specific to their security responsibilities.
- o. All personnel involved in COOP efforts shall be identified and trained in the procedures and logistics of COOP development and implementation.

AT-4 – Security Training Records

- a. EPA shall identify all individuals requiring role-based security-related training as part of the Agency's personnel management function.
- b. Individual training records shall be retrained for a period of seven (7) years in accordance with agency retention policy and procedure.

EPA Classification No.: CIO-2150.3-P-02.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- c. All EPA employees shall include security awareness training, including any role-based security-related training, in their Individual Development Plans (IDPs) annually.
- d. EPA shall maintain a record of awareness and training for each individual as required in accordance with federal regulations and EPA's policies and procedures. Records must consist of certificates of completion signed by the training provider, the trainee's supervisor, the ISO, or ISSO or other similar mechanism.
- e. EPA shall track the status of awareness and training progress and completion at least every 30 days, then no less than weekly within 60 days of the deadline for the annual FISMA report.
 - i. Reports of the status of all users' training must be made available to supervisors, System Owners (SO), and Senior Information Officials (SIOs) as needed but at least weekly prior to the deadline for the annual FISMA report.
- f. Each program office and Region shall report on the status of employees' training activities at the end of the fiscal year to the Senior Agency Information Security Officer (SAISO) of EPA, as required by the annual FISMA reporting requirement.
- g. EPA shall retain training and awareness records in accordance with *EPA Records Schedule 571*.
- h. EPA personnel, contractors, or others working on behalf of EPA accessing EPA systems shall receive initial training and annual refresher training, in security awareness and accepted security practices. Personnel shall complete security awareness within twenty-four (24) hours of being granted a user account. If the user fails to comply, user access shall be suspended.

AT-5 – Contacts with Security Groups and Associations

- a. EPA shall establish and institutionalize contact with selected groups and associations within the security community to:
 - i. Stay up-to-date with the latest recommended security practices, techniques, and technologies.
 - ii. Facilitate ongoing security education and training for organizational personnel.
 - iii. Share current security-related information including threats, vulnerabilities, and incidents.

Note: Ongoing contact with security groups and associations is of paramount importance in an environment of rapid technology changes and dynamic threats. Security groups and associations can include, for example, special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations.

- b. The groups and associations selected must be consistent with the organization's mission/business requirements.

EPA Classification No.: CIO-2150.3-P-02.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- i. At a minimum, EPA shall maintain such contacts and relationships as:
 - NIST
 - United States Computer Emergency Response Team (US-CERT)
 - c. Information-sharing activities regarding threats, vulnerabilities, and incidents related to information systems must be consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
 - d. Establishes and institutionalizes contact with selected groups and associations within the security community:
 - I. To facilitate ongoing security education and training for organizational personnel;
 - II. To stay up to date with the latest recommended security practices, techniques, and technologies; and
 - III. To share current security-related information including threats, vulnerabilities, and incidents.
-

7. RELATED DOCUMENTS

- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998
 - NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003
 - NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009
-

8. ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO)

- a. The CIO has the following responsibilities with respect to awareness and training:
 - i. Establish overall strategy for the IT security awareness and training program.
 - ii. Ensure that the Agency head, senior managers, system and data owners, and others understand the concepts and strategy of the security awareness and training program, and are informed of the progress of the program's implementation.
 - iii. Ensure that an Agency-wide IT security program is implemented, is well-supported by resources and budget, and is effective.
 - iv. Ensure that the Agency has enough personnel with significant security responsibilities and that they are sufficiently trained to protect its IT resources.
 - v. Ensure the role-based security-related training of Agency personnel.
 - vi. Ensure that all users are sufficiently trained in their security responsibilities.
 - vii. Ensure that effective tracking and reporting mechanisms are in place.
-

EPA Classification No.: CIO-2150.3-P-02.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

System Owner (SO)

- a. The SO has the following responsibilities with respect to awareness and training:
 - i. In coordination with the Information Owner (IO), the SO is also responsible for deciding who has access to the system (and with what types of privileges or access rights) and ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior).

Information Technology Security Program Manager

- a. The Information Technology Security Program Manager has the following responsibilities with respect to awareness and training:
 - i. Ensure that awareness and training material developed is appropriate and timely for the intended audiences.
 - ii. Ensure that awareness and training material is effectively deployed to reach the intended audience.
 - iii. Ensure that users and managers have an effective way to provide feedback on the awareness and training material and its presentation.
 - iv. Ensure that awareness and training material is reviewed periodically and updated when necessary.
 - v. Assist in establishing a tracking and reporting strategy.

Managers and Supervisors

- a. Managers and supervisors have the following responsibilities with respect to awareness and training:
 - i. Work with the CIO and IT security program manager to meet shared responsibilities.
 - ii. Serve in the role of SO and IO, where applicable:
 - Augment awareness and training as necessary for the specific security issues of the information or information system.
 - Ensure users and operational personnel receive role-based security-related training and awareness.
 - iii. Ensure IDPs include required training and awareness, especially for users in roles with significant security responsibilities.
 - iv. Promote the professional development and certification of the IT security program staff, full-time or part-time security officers, and others with significant security responsibilities.
 - v. Ensure that all users (including contractors, grantees, etc.) of their systems (i.e., general support systems and major applications) are role-based security-related trained in how to fulfill their security responsibilities before allowing them access to information systems.
 - vi. Ensure that users (including contractors, grantees, etc.) understand specific rules of each system and application they use.
 - vii. Work to reduce errors and omissions by users due to lack of awareness

EPA Classification No.: CIO-2150.3-P-02.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

and/or training.

EPA Administrators

- a. Administrators have the following responsibilities with respect to awareness and training:
 - i. Ensure that an Agency-wide IT security program is implemented, is well-supported by resources and budget, and is effective.
 - ii. Ensure that the Agency has enough sufficiently trained personnel to protect its IT resources.

Users / Individuals

- a. Users/individuals have the following responsibilities with respect to awareness and training:
 - i. Complete basic information system security awareness materials as part of initial training for new users, when required by system changes, and annually thereafter.
 - ii. Complete the specified training hours annually for the subject areas found in *Appendix E* of this document.
 - iii. Complete role-based security-related training within 60 days of appointment to a new position that requires additional role-specific training.
 - iv. Include security awareness training, including any role-specific training, in their IDPs annually.

9. DEFINITIONS

- General Support System – an interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. A general support system, for example, can be a: (i) LAN including smart terminals that support a branch office; (ii) backbone (e.g., Agency-wide); (iii) communications network; (iv) Agency data processing center including its operating system and utilities; (v) tactical radio network; or (vi) shared information processing service facility. A general support system can have a FIPS 199 impact level of low, moderate, or high in its security categorization depending on the criticality or sensitivity of the system and any major applications the general support system is supporting. A general support system is considered a major information system when special management attention is required, there is high development, operating, or maintenance costs; and the system/information has a significant role in the administration of Agency programs. When the general support system is a major information system, the system's FIPS 199 impact level is either moderate or high.
- Incident – an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of

EPA Classification No.: CIO-2150.3-P-02.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

violation of security policies, security procedures, or acceptable use policies.

- Information – an instance of an information type.
- Information Security – the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- Information Security Policy – an aggregate of directives, regulations, rules, and practices that prescribe how an organization manages, protects, and distributes information.
- Information System – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- Major Application – an application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.
- Organization – a federal agency or, as appropriate, any of its operational elements.
- Records – the recordings of evidence of activities performed or results achieved (e.g., forms, reports, test results) which serve as the basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
- Signature (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance, or obligation. Can be accomplished manually, sometimes referred to as a “wet signature,” or electronically.
- Threat – Any circumstance or event with the potential to adversely impact Agency operations (including mission, functions, image, or reputation), Agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- User – individual or (system) process authorized to access an information system.
- Vulnerability – weakness in an information system, system security procedures, internal controls, or implementation that could be exploited.
- Written – or “in writing” means to officially document the action or decision and includes a signature. The documentation can be accomplished manually or electronically.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- substantive business case need(s)
-

EPA Classification No.: CIO-2150.3-P-02.1	CIO Approval Date: 08/06/2012
CIO Transmittal No.: 12-003	Review Date: 08/06/2015

- demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

The SAISO and Director, OTOP shall coordinate to maintain central repository of all waivers.

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

Related policy and procedures are available on OEI's Policy Resources website.

<http://intranet.epa.gov/oei/imitpolicy/policies.htm>

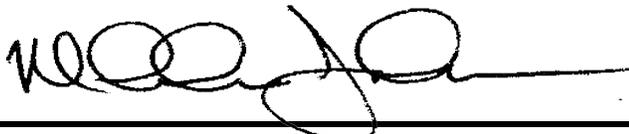
Related standards and guidelines are available on OEI's website.

12. MATERIAL SUPERSEDED

EPA Information Security Manual, Directive 2195A1, 1999 Edition, Section 13 and Appendix A

13. ADDITIONAL INFORMATION

NA



Malcolm D. Jackson
Assistant Administrator and Chief Information Officer
Office of Environmental Information

APPENDIX A: ACRONYMS

CIO	Chief Information Officer
COR	Contracting Office Representative
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
IDP	Individual Development Plan
IO	Information Owner
IRM	Information Resources Management
ISO	Information Security Officer
ISSO	Information Systems Security Officer
IT	Information Technology
IV&V	Independent Verification and Validation
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OTOP	Office of Technology and Operations Planning
PARS	Performance Appraisal and Recognition System
PO	Project Officer
SAISO	Senior Agency Information Security Officer
SIO	Senior Information Official
SO	System Owner
SP	Special Publication
TISS	Technology and Information Security Staff
USC	United States Code
US-CERT	United States Computer Emergency Response Team

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.4	9/15/2008	Initial draft	Heather Flager	Procedures-AT-Draft_TO62_020_1
1.0	10/27/2008	Incorporated EPA feedback	Heather Flager	Procedures-AT-Final_TO62_020_2
1.1	10/30/2008	Amended Appendix B, C, D, E	William Gill	Procedures-AT-Final_TO62_020_2
2.0	4/21/2009	Added to Responsibilities Incorporated EPA feedback	Heather Flager	Procedures-AT-Final_TO62_020_3
2.1	9/18/2009	Incorporated review comments	William Gill	Procedures_AT_Final_2.1
2.8	7/29/2010	Updated per NIST SP 800-53 Revision 3	Heather Flager	Procedures_AT_Draft.T O-062_050_1.0
2.8	7/20/2010	TISS comments and changes	Charleen Johnson	Procedures_AT_Draft.T O-062_050_1.0
3.0	5/1/2012	SAISO Final Review	Jabran Malik	Procedures_AT_Draft.T O-062_050_1.0
3.1	7/18/2012	Document Review	LaToya Gordon	Procedures_AT_Draft.T O-062_050_1.0