Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Awareness and Training (AT) Procedure

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 (AT) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.*

2. SCOPE

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

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. BACKGROUND

EPA is responsible for ensuring 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 shall meet security requirements by implementing the security controls defined in the NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

This document adopts procedures and standards for the EPA consistent with FIPS Publication 200.

5. AUTHORITY

Additional legal foundations for the Awareness and Training Procedure include:

- Federal Information Security Modernization Act (FISMA) of 2014, Public Law 113-283, to amend chapter 35 of title 44, United States Code (U.S.C.)

- OMB Circular A-130, "Managing Information as a Strategic Resource," Appendix I, "Responsibilities for Protecting and Managing Federal Information Resources," July 2016
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

6. PROCEDURE

SIO, ISO, and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system through a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and SO or their official designees for the systems that they oversee.

The "AT" designator (e.g., AT-2, AT-3) identified for each procedure below corresponds to the NIST- identifier for the Awareness and Training control family, as identified in NIST SP 800-53, Revision 5, Security and Privacy Controls for Federal Information Systems and Organizations.

NIST defines the applicable AT security and privacy baseline controls in NIST 800-53B, Control Baselines for Information Systems and Organizations. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name.

AT-2 – Literacy Training and Awareness

For All Systems and Privacy Control Baseline:

1) Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
   a) As part of initial training for new users and at least annually thereafter; and
   b) When required by system changes or following audit findings, security events, or when deemed appropriate as determined by the Chief Information Security Officer (CISO), Chief Information Officer (CIO), SO or ISO to manage risks.
2) Employ the following techniques to increase the security and privacy awareness of system users: intranet and SharePoint sites, special events, email notices, alerts, and exercises;

3) Update literacy training and awareness content annually and following significant changes/updates in the security/threat environment and/or a significant cybersecurity and privacy incident or breach as needed; and
4) Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

AT-2(2) – Literacy Training and Awareness | Insider Threat

For All Systems:

1) Provide security training on recognizing and reporting potential indicators of insider threat.

AT-2(3) – Literacy Training and Awareness | Social Engineering and Mining

For Moderate and High Systems:

1) Provide security training on recognizing and reporting potential and actual instances of social engineering and social mining.

AT-3 – Role-Based Training

For All Systems and Privacy Control Baseline:

1) Provide role-based security and privacy training to personnel with the following roles and responsibilities:
    - Security Administrators
    - Database Administrators
    - System Administrators
    - Application Developers
    - Service Desk Technicians
    - Network Security Operations Division (NSOD)
    - ISO
    - Information System Security Officers (ISSO)
    - Liaison Privacy Officials (LPO)
    - System Owners
    - System Managers
    - Information Management Officers (IMO)
    - Information Resources Management Branch Chief (IRMBC)
    - Applications Owners
    - SIO
    - Office of Information Security and Privacy (OISP) Staff

a) Before authorizing access to the system, information, or performing assigned duties, and at least annually thereafter; and
b) When required by system changes;

2) Update role-based training content annually and following significant changes/updates in the security/threat environment and/or a significant cybersecurity and privacy incident or breach as needed; and
3) Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

AT-3(5) – Role-Based Security Training | Processing Personally Identifiable Information

For Privacy Control Baseline:

1) Provide personnel or roles listed in AT-3 and other staff who are actively engaged in processing PII with initial and annual training in the employment and operation of personally identifiable information processing and transparency controls.

AT-4 – Training Records

For All Systems and Privacy Control Baseline:

1) Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and
2) Retain individual training records in accordance with the National Records Management Program (NRMP) and EPA Records Schedules requirements.

7. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

8. RELATED INFORMATION

- NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model
- NIST SP 800-50. Building an Information Technology Security Awareness and Training Program
- 5 C.F.R. Part 930.301

9. DEFINITIONS

- **Assessment** – see "Control Assessment."
- **Authorization** – access privileges granted to a user, program or process or the act of granting those privileges.
- **Control Assessment** – the testing or evaluation of the controls in an information system or organization to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security or privacy requirements for the system or the organization.
- **EPA-operated System** – an on-premise system where EPA personnel, including federal employees or contractors, have sole and direct system administrative and management responsibilities or cloud system where EPA personnel, including federal employees or contractors, have management responsibilities. The system may be operated internally or externally to the EPA's intranet boundary.
- **Incident** – an occurrence that actually or imminently 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 violation of security policies, security procedures or acceptable use policies.
- **Information** – any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, electronic or audiovisual forms.
- **Information Security** – the protection of information and 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.
- **Organization** – a federal agency or, as appropriate, any of its operational elements.
- **Personally Identifiable Information (PII)** – any information about an individual maintained by an agency, which can be used to distinguish, trace, or identify an individual's identity, including personal information which is linked or linkable to an individual (e.g., name, date of birth, address).
- **PII Processing** – an operation or set of operations performed on PII that can include, but is not limited to, the collection, retention, logging, generation, transformation, use, disclosure, transfer and disposal of PII.
- **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 (e.g., 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).
- **Significant Change** – a change that is likely to substantively affect the security or privacy posture of a system.
- **System Operated on Behalf of the EPA** – a system where EPA personnel do not have sole or direct system management responsibilities. System administration is directed and performed by service provider personnel. The system may be operated within or externally to EPA's intranet boundary.
- **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** – an individual or (system) process authorized to access an information system.
- **Vulnerability** – a weakness in an information system, system security procedures, internal controls or implementation that could be exploited or triggered by a threat source.
- **Written** (or in writing) – to officially document the action or decision, either manually or electronically, and includes a signature.

10. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

11. MATERIAL SUPERSEDED

Information Directive: CIO 2150-P-02.2, Information Security – Awareness and Training Procedures

12. CONTACTS

For further information, please contact the Office of Information Security and Privacy (OISP), Office of Mission Support (OMS).

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2023.06.12 08:15:03 -04'00'

Vaughn Noga
Chief Information Officer and
Deputy Assistant Administrator for Environmental Information
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS & ABBREVIATIONS

AT	Awareness and Training
C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
IO	Information Owner
NIST	National Institute of Standards and Technology
OISP	Office of Information Security and Privacy
OITO	Office of Information Technology Operations
OMB	Office of Management and Budget
OMS	Office of Mission Support
PII	Personally Identifiable Information
PWS	Performance Work Statement
SA	System and Services Acquisition
SISR	Significant Information Security Responsibilities
SM	Service Manager
SO	System Owner
SOW	Statement of Work
SP	Special Publication
U.S.C.	United States Code