3.2 AWARENESS AND TRAINING

Quick link to Awareness and Training Summary Table

AT-1 POLICY AND PROCEDURES

Control:

a. Develop, document, and disseminate to [*Assignment: organization-defined personnel or roles*]:

   1. [*Selection (one or more): Organization-level; Mission/business process-level; System-level*] awareness and training policy that:

      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and

      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and

   2. Procedures to facilitate the implementation of the awareness and training policy and the associated awareness and training controls;

b. Designate an [*Assignment: organization-defined official*] to manage the development, documentation, and dissemination of the awareness and training policy and procedures; and

c. Review and update the current awareness and training:

   1. Policy [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

   2. Procedures [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Discussion: Awareness and training policy and procedures address the controls in the AT family that are implemented within systems and organizations. The risk management strategy is an important factor in establishing such policies and procedures. Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures. Security and privacy program policies and procedures at the organization level are preferable, in general, and may obviate the need for mission- or system-specific policies and procedures. The policy can be included as part of the general security and privacy policy or be represented by multiple policies that reflect the complex nature of organizations. Procedures can be established for security and privacy programs, for mission or business processes, and for systems, if needed. Procedures describe how the policies or controls are implemented and can be directed at the individual or role that is the object of the procedure. Procedures can be documented in system security and privacy plans or in one or more separate documents. Events that may precipitate an update to awareness and training policy and procedures include assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Simply restating controls does not constitute an organizational policy or procedure.

Related Controls: PM-9, PS-8, SI-12.

Control Enhancements: None.

References: [OMB A-130], [SP 800-12], [SP 800-30], [SP 800-39], [SP 800-50], [SP 800-100].

AT-2 LITERACY TRAINING AND AWARENESS

Control:

a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):

   1. As part of initial training for new users and [*Assignment: organization-defined frequency*] thereafter; and

   2. When required by system changes or following [*Assignment: organization-defined events*];

b. Employ the following techniques to increase the security and privacy awareness of system users [*Assignment: organization-defined awareness techniques*];

c. Update literacy training and awareness content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

d. Incorporate lessons learned from internal or external security incidents or breaches into literacy training and awareness techniques.

Discussion: Organizations provide basic and advanced levels of literacy training to system users, including measures to test the knowledge level of users. Organizations determine the content of literacy training and awareness based on specific organizational requirements, the systems to which personnel have authorized access, and work environments (e.g., telework). The content includes an understanding of the need for security and privacy as well as actions by users to maintain security and personal privacy and to respond to suspected incidents. The content addresses the need for operations security and the handling of personally identifiable information.

Awareness techniques include displaying posters, offering supplies inscribed with security and privacy reminders, displaying logon screen messages, generating email advisories or notices from organizational officials, and conducting awareness events. Literacy training after the initial training described in AT-2a.1 is conducted at a minimum frequency consistent with applicable laws, directives, regulations, and policies. Subsequent literacy training may be satisfied by one or more short ad hoc sessions and include topical information on recent attack schemes, changes to organizational security and privacy policies, revised security and privacy expectations, or a subset of topics from the initial training. Updating literacy training and awareness content on a regular basis helps to ensure that the content remains relevant. Events that may precipitate an update to literacy training and awareness content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-3, AT-4, CP-3, IA-4, IR-2, IR-7, IR-9, PL-4, PM-13, PM-21, PS-7, PT-2, SA-8, SA-16.

Control Enhancements:

(1) LITERACY TRAINING AND AWARENESS | PRACTICAL EXERCISES

Provide practical exercises in literacy training that simulate events and incidents.

Discussion: Practical exercises include no-notice social engineering attempts to collect information, gain unauthorized access, or simulate the adverse impact of opening malicious email attachments or invoking, via spear phishing attacks, malicious web links.

Related Controls: CA-2, CA-7, CP-4, IR-3.

(2) LITERACY TRAINING AND AWARENESS | INSIDER THREAT

Provide literacy training on recognizing and reporting potential indicators of insider threat.

Discussion: Potential indicators and possible precursors of insider threat can include behaviors such as inordinate, long-term job dissatisfaction; attempts to gain access to information not required for job performance; unexplained access to financial resources; bullying or harassment of fellow employees; workplace violence; and other serious violations of policies, procedures, directives, regulations, rules, or practices. Literacy training includes how to communicate the concerns of employees and management regarding potential indicators of insider threat through channels established by the organization and in accordance with established policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role. For example, training for managers may be focused on changes in the behavior of team members, while training for employees may be focused on more general observations.

Related Controls: PM-12.

(3) LITERACY TRAINING AND AWARENESS | SOCIAL ENGINEERING AND MINING

Provide literacy training on recognizing and reporting potential and actual instances of social engineering and social mining.

Discussion: Social engineering is an attempt to trick an individual into revealing information or taking an action that can be used to breach, compromise, or otherwise adversely impact a system. Social engineering includes phishing, pretexting, impersonation, baiting, quid pro quo, thread-jacking, social media exploitation, and tailgating. Social mining is an attempt to gather information about the organization that may be used to support future attacks. Literacy training includes information on how to communicate the concerns of employees and management regarding potential and actual instances of social engineering and data mining through organizational channels based on established policies and procedures.

Related Controls: None.

(4) LITERACY TRAINING AND AWARENESS | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

Provide literacy training on recognizing suspicious communications and anomalous behavior in organizational systems using [*Assignment: organization-defined indicators of malicious code*].

Discussion: A well-trained workforce provides another organizational control that can be employed as part of a defense-in-depth strategy to protect against malicious code coming into organizations via email or the web applications. Personnel are trained to look for indications of potentially suspicious email (e.g., receiving an unexpected email, receiving an email containing strange or poor grammar, or receiving an email from an unfamiliar sender that appears to be from a known sponsor or contractor). Personnel are also trained on how to respond to suspicious email or web communications. For this process to work effectively, personnel are trained and made aware of what constitutes suspicious communications. Training personnel on how to recognize anomalous behaviors in systems can provide organizations with early warning for the presence of malicious code. Recognition of anomalous behavior by organizational personnel can supplement malicious code detection and protection tools and systems employed by organizations.

Related Controls: None.

(5) LITERACY TRAINING AND AWARENESS | ADVANCED PERSISTENT THREAT

Provide literacy training on the advanced persistent threat.

Discussion: An effective way to detect advanced persistent threats (APT) and to preclude successful attacks is to provide specific literacy training for individuals. Threat literacy training includes educating individuals on the various ways that APTs can infiltrate the organization (e.g., through websites, emails, advertisement pop-ups, articles, and social

engineering). Effective training includes techniques for recognizing suspicious emails, use of removable systems in non-secure settings, and the potential targeting of individuals at home.

Related Controls: None.

(6) LITERACY TRAINING AND AWARENESS | CYBER THREAT ENVIRONMENT

(a) Provide literacy training on the cyber threat environment; and

(b) Reflect current cyber threat information in system operations.

Discussion: Since threats continue to change over time, threat literacy training by the organization is dynamic. Moreover, threat literacy training is not performed in isolation from the system operations that support organizational mission and business functions.

Related Controls: RA-3.

References: [OMB A-130], [SP 800-50], [SP 800-160-2], [SP 800-181], [ODNI CTF].

AT-3 ROLE-BASED TRAINING

Control:

a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: [*Assignment: organization-defined roles and responsibilities*]:

   1. Before authorizing access to the system, information, or performing assigned duties, and [*Assignment: organization-defined frequency*] thereafter; and

   2. When required by system changes;

b. Update role-based training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*]; and

c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

Discussion: Organizations determine the content of training based on the assigned roles and responsibilities of individuals as well as the security and privacy requirements of organizations and the systems to which personnel have authorized access, including technical training specifically tailored for assigned duties. Roles that may require role-based training include senior leaders or management officials (e.g., head of agency/chief executive officer, chief information officer, senior accountable official for risk management, senior agency information security officer, senior agency official for privacy), system owners; authorizing officials; system security officers; privacy officers; acquisition and procurement officials; enterprise architects; systems engineers; software developers; systems security engineers; privacy engineers; system, network, and database administrators; auditors; personnel conducting configuration management activities; personnel performing verification and validation activities; personnel with access to system-level software; control assessors; personnel with contingency planning and incident response duties; personnel with privacy management responsibilities; and personnel with access to personally identifiable information.

Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical controls. Role-based training also includes policies, procedures, tools, methods, and artifacts for the security and privacy roles defined. Organizations provide the training necessary for individuals to fulfill their responsibilities related to operations and supply chain risk management within the context of organizational security and privacy programs. Role-based training also applies to contractors who provide services to federal agencies. Types of training include web-based and computer-based training, classroom-style training, and hands-on training (including micro-training). Updating role-based

training on a regular basis helps to ensure that the content remains relevant and effective. Events that may precipitate an update to role-based training content include, but are not limited to, assessment or audit findings, security incidents or breaches, or changes in applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.

Related Controls: AC-3, AC-17, AC-22, AT-2, AT-4, CP-3, IR-2, IR-4, IR-7, IR-9, PL-4, PM-13, PM-23, PS-7, PS-9, SA-3, SA-8, SA-11, SA-16, SR-5, SR-6, SR-11.

Control Enhancements:

(1) ROLE-BASED TRAINING | ENVIRONMENTAL CONTROLS

Provide [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of environmental controls.

Discussion: Environmental controls include fire suppression and detection devices or systems, sprinkler systems, handheld fire extinguishers, fixed fire hoses, smoke detectors, temperature or humidity, heating, ventilation, air conditioning, and power within the facility.

Related Controls: PE-1, PE-11, PE-13, PE-14, PE-15.

(2) ROLE-BASED TRAINING | PHYSICAL SECURITY CONTROLS

Provide [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of physical security controls.

Discussion: Physical security controls include physical access control devices, physical intrusion and detection alarms, operating procedures for facility security guards, and monitoring or surveillance equipment.

Related Controls: PE-2, PE-3, PE-4.

(3) ROLE-BASED TRAINING | PRACTICAL EXERCISES

Provide practical exercises in security and privacy training that reinforce training objectives.

Discussion: Practical exercises for security include training for software developers that addresses simulated attacks that exploit common software vulnerabilities or spear or whale phishing attacks targeted at senior leaders or executives. Practical exercises for privacy include modules with quizzes on identifying and processing personally identifiable information in various scenarios or scenarios on conducting privacy impact assessments.

Related Controls: None.

(4) ROLE-BASED TRAINING | SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

[Withdrawn: Moved to AT-2(4)].

(5) ROLE-BASED TRAINING | PROCESSING PERSONALLY IDENTIFIABLE INFORMATION

Provide [*Assignment: organization-defined personnel or roles*] with initial and [*Assignment: organization-defined frequency*] training in the employment and operation of personally identifiable information processing and transparency controls.

Discussion: Personally identifiable information processing and transparency controls include the organization's authority to process personally identifiable information and personally identifiable information processing purposes. Role-based training for federal agencies addresses the types of information that may constitute personally identifiable information and the risks, considerations, and obligations associated with its processing. Such training also considers the authority to process personally identifiable information documented in privacy policies and notices, system of records notices, computer matching agreements and

notices, privacy impact assessments, [PRIVACT] statements, contracts, information sharing agreements, memoranda of understanding, and/or other documentation.

Related Controls: PT-2, PT-3, PT-5, PT-6.

References: [OMB A-130], [SP 800-50], [SP 800-181].

AT-4 TRAINING RECORDS

Control:

a. Document and monitor information security and privacy training activities, including security and privacy awareness training and specific role-based security and privacy training; and

b. Retain individual training records for [*Assignment: organization-defined time period*].

Discussion: Documentation for specialized training may be maintained by individual supervisors at the discretion of the organization. The National Archives and Records Administration provides guidance on records retention for federal agencies.

Related Controls: AT-2, AT-3, CP-3, IR-2, PM-14, SI-12.

Control Enhancements: None.

References: [OMB A-130].

AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS

[Withdrawn: Incorporated into PM-15.]

AT-6 TRAINING FEEDBACK

Control: Provide feedback on organizational training results to the following personnel [*Assignment: organization-defined frequency*]: [*Assignment: organization-defined personnel*].

Discussion: Training feedback includes awareness training results and role-based training results. Training results, especially failures of personnel in critical roles, can be indicative of a potentially serious problem. Therefore, it is important that senior managers are made aware of such situations so that they can take appropriate response actions. Training feedback supports the evaluation and update of organizational training described in AT-2b and AT-3b.

Related Controls: None.

Control Enhancements: None.

References: None.