

Department of the Interior
Security Control Standard
Awareness and Training

April 2011

Version: 1.1



Signature Approval Page

| Designated Official | |
|---|--------------|
| Bernard J. Mazer, Department of the Interior, Chief Information Officer | |
| Signature: | Date: |

REVISION HISTORY

| Author | Version | Revision Date | Revision Summary |
|--------------------|----------------|----------------------|---|
| Chris Peterson | 0.1 | December 2, 2010 | Initial draft |
| Timothy Brown | 0.2 | December 3, 2010 | Incorporated comments into body text |
| Timothy Brown | 0.21 | January 07, 2011 | Added introductory paragraph |
| Timothy Brown | 0.22 | February 15, 2011 | Checked/added cloud controls to high |
| Chris Peterson | 1.0 | February 18, 2011 | Final review of controls; remove margin notes |
| Lawrence K. Ruffin | 1.1 | April 29, 2011 | Final revisions and version change to 1.1 |
| | | | |
| | | | |
| | | | |
| | | | |

TABLE OF CONTENTS

| | |
|--|----------|
| REVISION HISTORY | 3 |
| TABLE OF CONTENTS | 4 |
| SECURITY CONTROL STANDARD: AWARENESS AND TRAINING | 5 |
| AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES | 5 |
| AT-2 SECURITY AWARENESS | 6 |
| AT-3 SECURITY TRAINING | 6 |
| AT-4 SECURITY TRAINING RECORDS | 7 |

SECURITY CONTROL STANDARD: AWARENESS AND TRAINING

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Awareness and Training (AT) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

AT-1 SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES

Applicability: All Information Systems

Control: The organization develops, disseminates, and reviews/updates annually:

- a. A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the security awareness and training family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational

policies and procedures may make the need for additional specific policies and procedures unnecessary. The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the security awareness and training policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-16, 800-50, 800-100.

Priority and Baseline Allocation:

| | | | |
|-----------|-----------------|-----------------|------------------|
| P1 | LOW AT-1 | MOD AT-1 | HIGH AT-1 |
|-----------|-----------------|-----------------|------------------|

AT-2 SECURITY AWARENESS

Applicability: All Information Systems

Control: The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and annually thereafter.

Supplemental Guidance: The organization determines the appropriate content of security awareness training and security awareness techniques based on the specific requirements of the organization and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security as it relates to the organization's information security program. 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.

Control Enhancements: None mandated.

References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); NIST Special Publication 800-50.

Priority and Baseline Allocation:

| | | | |
|-----------|-----------------|-----------------|------------------|
| P1 | LOW AT-2 | MOD AT-2 | HIGH AT-2 |
|-----------|-----------------|-----------------|------------------|

AT-3 SECURITY TRAINING

Applicability: All Information Systems

Control: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) at least annually thereafter.

Supplemental Guidance: The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides 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. Related controls: AT-2, SA-3.

Control Enhancements: None.

References: C.F.R. Part 5 Subpart C (5 C.F.R 930.301); NIST Special Publications 800-16, 800-50.

Priority and Baseline Allocation:

| | | | |
|-----------|-----------------|-----------------|------------------|
| P1 | LOW AT-3 | MOD AT-3 | HIGH AT-3 |
|-----------|-----------------|-----------------|------------------|

AT-4 SECURITY TRAINING RECORDS

Applicability: All Information Systems

Control: The organization:

- a. Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and
- b. Retains individual training records for at least 3 years.

Supplemental Guidance: While an organization may deem that organizationally mandated individual training programs and the development of individual training plans are necessary, this control does not mandate either. Documentation for specialized training may be maintained by individual supervisors at the option of the organization.

Control Enhancements: None.

References: None.

Priority and Baseline Allocation:

| | | | |
|-----------|-----------------|-----------------|------------------|
| P3 | LOW AT-4 | MOD AT-4 | HIGH AT-4 |
|-----------|-----------------|-----------------|------------------|