Information Technology (IT) System Awareness and Training (AT) Standard

January 31, 2022

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Questions about the policies outlined in this document should be directed to Information Assurance Services (IAS) at **OCIO_IAS@ed.gov**

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2022.02.01 15:59:45 -05'00'

Steven Hernandez
Director, IAS/Chief Information Security Officer (CISO)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Date	Summary of Changes
1.0	12/22/2021	Initial draft of new standard which combines NIST SP 800-53, Revision 5 controls, including ED specific control parameter values, with existing policy standards.
1.1	1/14/2022	Update to incorporate feedback from Information Assurance Services (IAS), Governance, Risk and Policy (GRP) Team.
1.2	1/31/2022	Update to incorporate feedback from IAS; address new security measures required by Executive Order (EO) 14028, including Office of Management and Budget (OMB) regulations and memoranda and updated NIST guidance issued to comply with the EO.

Table of Contents

1 INTRODUCTION

1.1 Purpose

The Federal Information Security Modernization Act (FISMA)[1] and implementing regulation Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*[2], requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, and services that are either fully or partially provided, including agency-hosted, outsourced, and cloud-based solutions. Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*[3], mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, *Security and Privacy Controls for Information Systems and Organizations*[4], as baseline information system controls.

This governance document establishes Department information technology (IT) system awareness and training standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders, Emergency Orders, Binding Operational Directives, and Department Administrative Communications System (ACS) directives and policies. In doing so, these standards supersede any prior governance documentation establishing such standards.

1.2 Scope

These standards apply to all information and information systems that support the operations and assets of the Department, including those provided or managed by another agency, contractor, or other source, as well as services that are either fully or partially provided, including Department-hosted, outsourced, and cloud-based solutions. Principal Offices, employees, contractors, external service providers and system users are required to comply with these awareness and training control standards.

2 STANDARDS

The Department standards for IT system awareness and training controls are organized to follow the order in which controls are presented in the current version of NIST SP 800-53. To define a control baseline for Department information systems, a FIPS 199 categorization level (e.g., Low

[1] Public Law 113-283-Dec. 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
[2] Office of Management and Budget (OMB) Circular A-130, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/circulars/A130/a130revised.pdf
[3] FIPS 200, https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.200.pdf
[4] NIST SP 800-53, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

(L), Moderate (M) and High (H)) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS 199 impact-level. Designators are also used to indicate when NIST SP 800-53 Privacy (P) baseline controls are required. To manage risk to within the Department's risk tolerance and appetite, control overlays are provided when the Department requires implementation of control(s) that are not required by the FIPS 199 impact-level or privacy baseline. In addition to the controls required by this standard, High Value Assets (HVAs) must implement and comply with the current version of the HVA Control Overlay issued and maintained by the Department of Homeland Security, Cybersecurity & Infrastructure Security Agency.

This standard directly supports the Department's integration of the NIST Cyber Security Framework (CSF) in focusing on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to Appendix A for a summary of controls by baseline and corresponding NIST CSF categories and subcategories.

2.1 AT-1 Awareness and Training Policy and Procedures (P, L, M, H)

The Department shall develop, document, and disseminate to all ED employees, contractors, and users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in OCIO: 3-112/ACSD-OCIO-004, *Cybersecurity Policy* a Department-level awareness and training policy (e.g., this document) 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.

(c) authorizes the Department Chief Information Security Officer (CISO) and Department Chief Information Officer (CIO) to issue subordinate standards, procedures, and memos, with the same authority and enforcement as OCIO: 3-112/ACSD-OCIO-004, Cybersecurity Policy.

The Department CISO in conjunction with the Senior Agency Official for Privacy (SAOP) are designated to manage the development, documentation, and dissemination of the Department-level awareness and training policy.

This policy is reviewed and updated annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

The Office of the Chief Information Officer (OCIO), Information Assurance Services (IAS) manage the development, documentation, and dissemination of the Department-level awareness and training standard operating procedures in support of this policy standard. IAS Branch Chiefs shall review these procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

Principal Office Information System Owners (ISO) and Information System Security Officers (ISSOs) are required to manage the development, documentation, and dissemination of system specific procedures to facilitate the implementation of the Department's awareness and training policy and the associated awareness and training controls. The ISO and ISSO shall review awareness and training procedures annually (i.e., each fiscal year) and following the identification of evolving threats, issuance of new or significantly changed existing Federal laws, executive orders, directives, regulations, and ED policies, identification of emerging technology and information technology service delivery models and determination that adjustments are deemed necessary to improve its effectiveness based upon feedback from Principal Office personnel.

2.2 AT-2 Literacy Training and Awareness (P, L, M, H and Control Overlay)

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 annually (i.e., each fiscal year) thereafter; and

    2. When required by system changes or following a determination by the Department CIO, CISO, or Governance, Risk and Policy Branch (GRP) branch chief that additional training is required to manage risk.

b. Employ the following techniques to increase the security and privacy awareness of system users:

    1. Conduct practical exercises that simulate actual cyber-attacks. Practical exercises may include social engineering attempts to collect information, gain unauthorized access, invoke opening malicious email attachments, or web links via spear phishing attacks.

    2. Supplement training providing by using awareness techniques such as posting information on connectED, generating email advisories/notices (e.g., Department-wide or from senior Department officials), conducting information security awareness events, and conducting other awareness activities deemed appropriate.

c. Update literacy training and awareness content annually (i.e., each fiscal year) and following security and privacy incidents or breaches and/or significant changes in the security environment.

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

Control Overlay AT-2 ED-01 (L, M, H): Ensure the Office of the Chief Information Officer (OCIO), Information Assurance Services (IAS):

1. Determines the appropriate training content and awareness techniques used.
2. Identifies users who fail to complete training by the assigned due date and revoke network access until the training requirement is fulfilled.

Control Overlay AT-2 ED-02 (L, M, H): Train all users of Executive Order (EO)-critical software, based on their roles and responsibilities, on how to securely use the software and the EO-critical software platforms.

Control Overlay AT-2 ED-03 (L, M, H): Conduct frequent awareness activities to reinforce the training for all users and administrators of EO-critical software and platforms, and to measure the training's effectiveness for continuous improvement purposes.

2.3 AT-2(2) Literacy Training and Awareness | Insider Threat (L, M, H)

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

2.4 AT-2(3) Literacy Training and Awareness | Social Engineering and Mining (M, H)

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

2.5 AT-3 Role-based Training (P, L, M, H and Control Overlay)

a. Provide role-based security and privacy training to personnel with Significant Security Responsibilities (SSR):

    1. Before authorizing access to the system, information, or performing assigned duties, and annually (i.e., each fiscal year) thereafter; and
    2. When required by system changes.

b. Update role-based training content when new courses or curriculum is made available to the Department through existing, updated, or new contracts or shared services and following security and privacy incidents or breaches and/or significant changes in the security environment.

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

Control Overlay AT-3 ED-01 (L, M, H): Identify and document all employees and contractors in positions with SSR, map their job function to the designated work role and specialty area in accordance with the current version of NIST SP 800-181, *Workforce Framework for Cybersecurity (NICE Framework)*, apply the corresponding Office of Personnel Management (OPM) Cybersecurity Work Role Code, and communicate the resulting mapping monthly to OCIO/IAS to support RBT and FISMA reporting. Note: Individuals are considered to have SSR if their work roles or positions could, upon execution, have the potential to adversely impact the security posture of one or more ED systems and/or the Department.

Control Overlay AT-3 ED-02 (L, M, H): Require all individuals with elevated privileges to complete RBT regardless of the work roles or position assigned.

Control Overlay AT-3 ED-03 (L, M, H): Train all administrators of EO-critical software and EO-critical software platforms, based on their roles and responsibilities, on how to securely administer the software and/or platforms.

2.5.1 AT-3(5) Role-based Training | Processing Personally Identifiable Information (P)

Provide all ED employees, contractors, and other internal users authorized to access to ED information systems, or systems operated or maintained on behalf of ED, or ED information as defined in OCIO: 3-112/ACSD-OCIO-004 *Cybersecurity Policy,* with initial and annual (i.e., each fiscal year) training in the employment and operation of personally identifiable information processing and transparency controls.

2.6 AT-4 Training Records (P, L, M, H and Control Overlay)

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

b. Retain individual training records for a minimum of three (3) years.

Control Overlay AT-4 ED-01 (L, M, H): Document and monitor practical exercises.

Control Overlay AT-4 ED-02 (L, M, H): Maintain training records within the Department's authorized learning management systems or other authorized training record repository. Principal Offices may maintain manual spreadsheets for contractors without Department network accounts which complete mandatory training outside of the Department's authorized learning management systems; these spreadsheets must be maintained by the Principal Office and submitted to the OCIO/IAS Cybersecurity Awareness and Training Program Manager upon request.

3 RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

4 ACRONYMS

ACS	Administrative Communications System
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSF	Cyber Security Framework
DHS	Department of Homeland Security
ED	Department of Education
EO	Executive Order
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
GRP	Governance, Risk and Policy Branch
IAS	Information Assurance Services
ISO	Information System Owner
ISSO	Information Systems Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OPM	Office of Personnel Management
RAF	Risk Acceptance Form
RBT	Role-based Training
SAOP	Senior Agency Official for Privacy
SP	Special Publication
SSR	Significant Security Responsibilities

5 APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below. NIST SP 800-53 controls that are not applicable to any control baseline are shaded in gray.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
AT-1	Policy and Procedures	x	x	x	x		
AT-2	Literacy Training and Awareness	x	x	x	x	PR.AT, GV.AT-P	PR.AT-1, GV.AT-P1
AT-2(1)	Literacy Training and Awareness | Practical Exercises					PR.AT, GV.AT-P	PR.AT-1, GV.AT-P1
AT-2(2)	Literacy Training and Awareness | Insider Threat		x	x	x	PR.AT, GV.AT-P	PR.AT-1, GV.AT-P1
AT-2(3)	Literacy Training and Awareness | Social Engineering and Mining			x	x	PR.AT, GV.AT-P	PR.AT-1, GV.AT-P1
AT-2(4)	Literacy Training and Awareness | Suspicious Communications and Anomalous System Behavior					PR.AT, GV.AT-P	PR.AT-1, GV.AT-P1
AT-2(5)	Literacy Training and Awareness | Advanced Persistent Threat					PR.AT, GV.AT-P	PR.AT-1, GV.AT-P1
AT-2(6)	Literacy Training and Awareness | Cyber Threat Environment					PR.AT, GV.AT-P	PR.AT-1, GV.AT-P1
AT-3	Role-based Training	x	x	x	x	PR.AT, GV.AT-P	PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, GV.AT-P1, GV.AT-P2, GV.AT-P3, GV.AT-P4
AT-3(1)	Role-based Training | Environmental Controls					PR.AT, GV.AT-P	PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, GV.AT-P1, GV.AT-P2, GV.AT-P3, GV.AT-P4
AT-3(2)	Role-based Training | Physical Security Controls					PR.AT, GV.AT-P	PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, GV.AT-P1, GV.AT-P2, GV.AT-P3, GV.AT-P4
AT-3(3)	Role-based Training | Practical Exercises					PR.AT, GV.AT-P	PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, GV.AT-P1, GV.AT-P2, GV.AT-P3, GV.AT-P4

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and Privacy Category	CSF and Privacy Subcategory
AT-3(5)	Role-based Training | Processing Personally Identifiable Information	x				PR.AT, GV.AT-P	PR.AT-2, PR.AT-3, PR.AT-4, PR.AT-5, GV.AT-P1, GV.AT-P2, GV.AT-P3, GV.AT-P4
AT-4	Training Records	x	x	x	x		
AT-6	Training Feedback						