Information Technology (IT) Maintenance (MA) Standard

December 15, 2023

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 **IAS_Governance@ed.gov**.

APPROVAL

STEVEN HERNANDEZ

Digitally signed by STEVEN HERNANDEZ
Date: 2023.12.15 14:32:53 -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.
1.3	1/27/2023	Annual review; no updates required.
5.4	12/15/2023	Aligned document major version number to align with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision number. Clean up formatting and numbering throughout and update broken links. Section 2, Standards was updated to include the description of incorporating organizationally defined parameters (ODP) for controls that may be necessary from external control overlays (e.g., High Value Assets [HVA]). Inserted references to NIST SP 800-53B tailoring guidance. Updated Section 4, Acronyms as appropriate. Updated language in controls MA-01, MA-03(03), and MA-05(01). Added controls MA-03(04), MA-03(05), MA-04(01), MA-04(04), MA-04(06), MA-04(07), and MA-05(05). Added “leading zeros” to control identifiers in alignment with patch release of NIST SP 800-53 (Release 5.1.1) to applicable controls, enhancements, and overlays.

Table of Contents

1 INTRODUCTION

This governance document establishes U.S. Department of Education (ED or Department) information technology (IT) maintenance controls standards necessary to improve the efficiency of operation or security of Department information systems and comply with Federal laws, regulations, Executive Orders (EO), Emergency Orders, Binding Operational Directives (BOD), and Department Administrative Communications System Directives (ACSD) and Handbooks. In doing so, these standards supersede any prior governance documentation establishing such standards.

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 (PUB) 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 amended, as baseline information system controls.

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 maintenance control standards.

[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/wp-content/uploads/legacy_drupal_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

2 STANDARDS

The Department standards for IT system maintenance 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 PUB 199 categorization level (e.g., Low [L], Moderate [M] and High [H]) is assigned to each requirement. This designator indicates a requirement applies to information systems categorized at that FIPS PUB 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 PUB 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[5] issued and maintained by the U.S. Department of Homeland Security (DHS), Cybersecurity & Infrastructure Security Agency (CISA). Systems that process federal tax return information (FTRI) must implement and comply with the Internal Revenue Service (IRS) Publication 1075[6], *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information.* Systems that are Federal Risk and Authorization Management Program (FedRAMP) authorized must implement and comply with the FedRAMP identified baselines[7].

Throughout the standard, there are controls captured that have not been scoped to any specific security or privacy baseline. This is intentional as all controls for identified external overlays and baselines (e.g., FedRAMP, IRS, HVA), that may apply to systems within the Department, have been incorporated into the standard. This ensures the organization defined parameters (ODPs) for controls within the Department have been clearly defined in a consistent manner.

Based upon an assessment of risk and determination that the level of protection for the security-relevant information within a system is not adversely impacted, maintenance controls identified in the current version of NIST SP 800-53B that support only the availability or confidentiality security objective may be downgraded to the corresponding maintenance control in a lower baseline (or modified or eliminated if not defined in a lower baseline).

This standard directly supports the Department's integration of the NIST Cybersecurity Framework (CSF) and NIST Privacy Framework (PF) by using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the Department's risk management processes. Refer to *APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY* for a summary of controls by baseline and corresponding NIST CSF and NIST PF categories and subcategories.

[5] https://www.cisa.gov/publication/high-value-asset-control-overlay
[6] IRS Publication 1075 https://www.irs.gov/pub/irs-pdf/p1075.pdf
[7] FedRAMP baselines https://www.fedramp.gov/baselines/

2.1 MA-01 Policy and Procedures (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 ACSD-OCIO-004[8], *Cybersecurity Policy* a Department-level IT system maintenance 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.

The Department Chief Information Security Officer (CISO) is designated to manage the development, documentation, and dissemination of the Department-level maintenance 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.

Principal Office (PO) 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 maintenance policy and the associated maintenance controls. The ISO and ISSO shall review maintenance 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 MA-02 Controlled Maintenance (L, M, H)

a. Schedule, document, and review records of maintenance, repair, and replacement on system components in accordance with manufacturer or vendor specifications and/or organizational requirements.

b. Approve and monitor all maintenance activities, whether performed on site or remotely and whether the system or system components are serviced on site or removed to another location.

[8] Also known as OCIO: 3-112.

c. Require ISO, ISSO, or designated alternate to explicitly approve the removal of the system or system components from organizational facilities for off-site maintenance, repair, or replacement.

d. Sanitize equipment to remove the following information from associated media prior to removal from organizational facilities for off-site maintenance, repair, or replacement: information the Department deems as sensitive, including but not limited to Personally Identifiable Information (PII), Sensitive PII, and Controlled Unclassified Information.

e. Check all potentially impacted controls to verify that the controls are still functioning properly following maintenance, repair, or replacement actions.

f. Include the following information in organizational maintenance records:

    1. the date and time of maintenance
    2. a description of the maintenance performed
    3. names of the individuals or group performing the maintenance
    4. name of the escort
    5. system components or equipment that are removed or replaced

2.2.1 MA-02(02) Controlled Maintenance | Automated Maintenance Activities (H)

Schedule, conduct, and document maintenance, repair, and replacement actions for the system using ED approved automated mechanisms. Produce up-to date, accurate, and complete records of all maintenance, repair, and replacement actions requested, scheduled, in process, and completed.

2.3 MA-03 Maintenance Tools (M, H)

Approve, control, and monitor the use of system maintenance tools. Review previously approved system maintenance tools at least annually (i.e., each fiscal year).

2.3.1 MA-03(01) Maintenance Tools | Inspect Tools (M, H)

Inspect the maintenance tools used by maintenance personnel for improper or unauthorized modifications.

2.3.2 MA-03(02) Maintenance Tools | Inspect Media (M, H)

Check media containing diagnostic and test programs for malicious code before the media are used in the system.

2.3.3 MA-03(03) Maintenance Tools | Prevent Unauthorized Removal (M, H)[9]

Prevent the removal of maintenance equipment containing organizational information by:

a. Verifying that there is no organizational information contained on the equipment.

b. Sanitizing or destroying the equipment

c. Retaining the equipment within the facility; or

d. Obtaining an exemption from the ISO, ISSO, or designated alternate explicitly authorizing removal of the equipment from the facility.

2.3.4 MA-03(04) Maintenance Tools | Restricted Tool Use

Restrict the use of maintenance tools to authorized personnel only.

2.3.5 MA-03(05) Maintenance Tools | Execution with Privilege

Monitor the use of maintenance tools that execute with increased privilege.

2.4 MA-04 Nonlocal Maintenance (L, M, H)

a. Approve and monitor nonlocal maintenance and diagnostic activities;

b. Allow the use of nonlocal maintenance and diagnostic tools only as consistent with organizational policy and documented in the security plan for the system;

c. Employ strong authentication in the establishment of nonlocal maintenance and diagnostic sessions;

d. Maintain records for nonlocal maintenance and diagnostic activities; and

e. Terminate session and network connections when nonlocal maintenance is completed.

2.4.1 MA-04(01) Nonlocal Maintenance | Logging and Review

a. Log events defined in AU-2a for nonlocal maintenance and diagnostic sessions; and

b. Review the audit records of the maintenance and diagnostic sessions to detect anomalous behavior.

2.4.2 MA-04(03) Nonlocal Maintenance | Comparable Security and Sanitization (H)

a. Require that nonlocal maintenance and diagnostic services be performed from a system that implements a security capability comparable to the capability implemented on the system being serviced; or

[9] MA-3(3) has been identified by NIST SP 800-53B as supporting only confidentiality and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

b. Remove the component to be serviced from the system prior to nonlocal maintenance or diagnostic services; sanitize the component (for organizational information); and after the service is performed, inspect and sanitize the component (for potentially malicious software) before reconnecting the component to the system.

2.4.3 MA-04(04) Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions

Protect nonlocal maintenance sessions by:

a. Employing multifactor authentication consistent with NIST SP 800-63 Digital Identity Guidelines requirements; and

b. Separating the maintenance sessions from other network sessions with the system by either:

    1. Physically separated communications paths; or

    2. Logically separated communications paths.

2.4.4 MA-04(06) Nonlocal Maintenance | Cryptographic Protection

Implement the following cryptographic mechanisms to protect the integrity and confidentiality of nonlocal maintenance and diagnostic communications: virtual private network (VPN) connection.

2.4.5 MA-04(07) Nonlocal Maintenance | Disconnect Verification

Verify session and network connection termination after the completion of nonlocal maintenance and diagnostic sessions.

2.5 MA-05 Maintenance Personnel (L, M, H)

a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel;

b. Verify that non-escorted personnel performing maintenance on the system possess the required access authorizations; and

c. Designate organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

2.5.1 MA-05(01) Maintenance Personnel | Individuals Without Appropriate Access (H)

a. Implement procedures for the use of maintenance personnel that lack appropriate security clearances or are not U.S. citizens, that include the following requirements:

    1. Maintenance personnel who do not have needed access authorizations, clearances, or formal access approvals are escorted and supervised during the performance of maintenance and diagnostic activities on the system by approved organizational

personnel who are fully cleared, have appropriate access authorizations, and are technically qualified; and

2. Prior to initiating maintenance or diagnostic activities by personnel who do not have needed access authorizations, clearances or formal access approvals, all volatile information storage components within the system are sanitized and all nonvolatile storage media are removed or physically disconnected from the system and secured; and

b. Develop and implement alternate security safeguards and/or Authorizing Official (AO) approved alternate controls defined in the security plan in the event a system component cannot be sanitized, removed, or disconnected from the system.

2.5.2 MA-5(5) Maintenance Personnel | Non-System Maintenance

Ensure that non-escorted personnel performing maintenance activities not directly associated with the system but in the physical proximity of the system, have required access authorizations.

2.6 MA-06 Timely Maintenance (M, H)[10]

Obtain maintenance support and/or spare parts for security critical information system components and/or essential information technology components within system-level specified timeframes, defined in the System Security Plan (SSP), Information System Contingency Plan (ISCP) and Business Impact Analysis (BIA), of a failure.

[10] MA-6 has been identified by NIST SP 800-53B as supporting only availability and may be downgraded to the corresponding control in a lower baseline (or modified or eliminated if defined in a lower baseline) only if the downgrading action reflects the security category for the supported availability security objective defined impact level.

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

Acronym	Definition
ACSD	Administrative Communications System Directive
AO	Authorizing Official
AU	Audit and Accountability Family
BIA	Business Impact Analysis
BOD	Binding Operational Directive
CISA	Cybersecurity & Infrastructure Security Agency
CISO	Chief Information Security Officer
CSF	Cybersecurity Framework
DE	Detect
DE.DP	Detection Processes
Department	U.S. Department of Education
DHS	U.S. Department of Homeland Security
ED	U.S. Department of Education
EO	Executive Order
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
FTRI	Federal Tax Return Information
GRP	Governance, Risk and Policy
GV.MT-P	Monitoring and Review
GV.PO-P	Governance Policies, Processes, and Procedures
GV-P	Govern-P
H	High
HVA	High Value Asset
IAS	Information Assurance Services
ISCP	Information System Contingency Plan
ISO	Information System Officer
ISSO	Information System Security Officer
IT	Information Technology
L	Low
M	Moderate
MA	Maintenance Family
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
ODP	Organizationally Defined Parameters
OMB	Office of Management and Budget
P	Privacy
PF	Privacy Framework
PII	Personally Identifiable Information
PO	Principal Office
PR	Protect
PR.MA	Maintenance
PR.MA-P	Maintenance

Acronym	Definition
PR-P	Protect-P
PUB	Publication
RAF	Risk Acceptance Form
SP	Special Publication
SSP	System Security Plan
VPN	Virtual Private Network

APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY

The applicability for each baseline control parameter is shown below.

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
MA-01	Policy and Procedures		X	X	X	PR.MA, DE.DP, GV.PO-P, GV.MT-P, PR.MA-P	PR.MA-1, DE.DP-2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.MA-P1
MA-02	Controlled Maintenance		X	X	X	PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-02(02)	Controlled Maintenance | Automated Maintenance Activities				X	PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-03	Maintenance Tools			X	X	PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-03(01)	Maintenance Tools | Inspect Tools			X	X	PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-03(02)	Maintenance Tools | Inspect Media			X	X	PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-03(03)	Maintenance Tools | Prevent Unauthorized Removal			X	X	PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-03(04)	Maintenance Tools | Restricted Tool Use					PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-03(05)	Maintenance Tools | Execution with Privilege					PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-03(06)	Maintenance Tools | Software Updates and Patches					PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-04	Nonlocal Maintenance		X	X	X	PR.MA, PR.MA-P	PR.MA-2, PR.MA-P2
MA-04(01)	Nonlocal Maintenance | Logging and Review					PR.MA, PR.MA-P	PR.MA-2, PR.MA-P2
MA-04(03)	Nonlocal Maintenance | Comparable Security and Sanitization				X	PR.MA, PR.MA-P	PR.MA-2, PR.MA-P2
MA-04(04)	Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions					PR.MA, PR.MA-P	PR.MA-2, PR.MA-P2
MA-04(05)	Nonlocal Maintenance | Approvals and Notifications					PR.MA, PR.MA-P	PR.MA-2, PR.MA-P2

Control Identifier	Control/Control Enhancement) Name	Privacy Baseline	Security Control Baseline Low	Security Control Baseline Moderate	Security Control Baseline High	CSF and PF Category	CSF and PF Subcategory
MA-04(06)	Nonlocal Maintenance | Cryptographic Protection					PR.MA, PR.MA-P	PR.MA-2, PR.MA-P2
MA-04(07)	Nonlocal Maintenance | Disconnect Verification					PR.MA, PR.MA-P	PR.MA-2, PR.MA-P2
MA-05	Maintenance Personnel		X	X	X	PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-05(01)	Maintenance Personnel | Individuals Without Appropriate Access				X	PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-05(02)	Maintenance Personnel | Security Clearances for Classified Systems					PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-05(03)	Maintenance Personnel | Citizenship Requirements for Classified Systems					PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-05(04)	Maintenance Personnel | Foreign Nationals					PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-05(05)	Maintenance Personnel | Non-system Maintenance					PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-06	Timely Maintenance			X	X	PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-06(01)	Timely Maintenance | Preventive Maintenance					PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-06(02)	Timely Maintenance | Predictive Maintenance					PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-06(03)	Timely Maintenance | Automated Support for Predictive Maintenance					PR.MA, PR.MA-P	PR.MA-1, PR.MA-P1
MA-07	Field Maintenance						