Information Technology (IT) Media Protection (MP) Standard

December 22, 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: 2023.12.20 17:40:56 -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 National Institute of Standards and Technology (NIST) Special Publication (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. Update broken link. Add High Value Asset (HVA) control footnote.
5.4	12/22/2023	Aligned document major version number to align with NIST 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 MP-01 and MP-03. Added controls MP-05(03) and MP-06(08). 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) media protection 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 media protection 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 media protection 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 information (FTI) 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, media protection controls identified in the current version of NIST SP 800-53B that support only the confidentiality security objective may be downgraded to the corresponding media protection 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 Privacy Framework 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] CISA HVA Overlay 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 MP-01 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 ACSD-OCIO-004[8], *Cybersecurity Policy* a Department-level IT system media protection 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 ACSD-OCIO-004, *Cybersecurity Policy*.

The Department Chief Information Security Officer (CISO) in conjunction with the Senior Agency Official for Privacy (SAOP) are designated to manage the development, documentation, and dissemination of the Department-level IT system media protection policy.

This policy shall be 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 IT system media protection policy and the associated media protection controls. The ISO and ISSO shall review media protection 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 MP-02 Media Access (L, M, H)

Restrict access to digital media to include but not limited to diskettes; magnetic tapes; external/removable hard disk drives; flash drives' compact disks; and digital video disks and non-

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

digital media to include but not limited to paper documents and microfilm to ED approved personnel and roles.

2.3 MP-03 Media Marking (M, H)[9]

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and

b. Exempt all digital and non-digital information system media or hardware components of lower classification than controlled unclassified information (CUI) from marking if the media remains within ED-authorized and controlled areas in accordance with ACSD-OCIO-004[10] *Cybersecurity Policy* and ACSD-OCIO-002[11] *Controlled Unclassified Information Program* for media storing and/or processing controlled unclassified information (CUI).

2.4 MP-04 Media Storage (M, H)[9]

a. Physically control and securely store digital media to include but not limited to diskettes; magnetic tapes; external/removable hard disk drives; flash drives' compact disks; and digital video disks and non-digital media to include but not limited to: paper documents and microfilm within ED secure/controlled facilities; and

b. Protect system media types defined in MP-4a until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

2.5 MP-05 Media Transport (M, H)[9]

a. Protect and control digital media to include but not limited to diskettes; magnetic tapes; external/removable hard disk drives; flash drives' compact disks; and digital video disks and non-digital media to include but not limited to paper documents and microfilm during transport outside of controlled areas using a FIPS 140-2 validated encryption module/mechanism for digital assets and locked containers for physical assets;

b. Maintain accountability for system media during transport outside of controlled areas;

c. Document activities associated with the transport of system media; and

d. Restrict the activities associated with the transport of system media to authorized personnel.

[9] MP-03, MP-04, and MP-05 have 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.

[10] Also known as OCIO 3-112.

[11] Also known as OCIO 3-113.

2.5.1 MP-05(03) Media Transport | Custodians

Employ an identified custodian during transport of system media outside of controlled areas.

2.6 MP-06 Media Sanitization (P, L, M, H)

a. Sanitize all digital and non-digital information system media prior to disposal, release out of organizational control, or release for reuse using the current version of NIST SP 800-88, *Guidelines for Media Sanitization*, techniques and procedures to include, but not limited to: clearing; purging; cryptographic erase; de-identification of personally identifiable information; and destruction; and

b. Employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

2.6.1 MP-06(01) Media Sanitization | Review, Approve, Track, Document, and Verify (H)[12]

Review, approve, track, document, and verify media sanitization and disposal actions.

2.6.2 MP-06(02) Media Sanitization | Equipment Testing (H)

Test sanitization equipment and procedures at least annually (i.e., each fiscal year) to ensure that the intended sanitization is being achieved.

2.6.3 MP-06(03) Media Sanitization | Nondestructive Techniques (H)

Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances:

a. Devices are purchased from manufacturers or vendors prior to initial use;

b. Unable to maintain a positive chain of custody for the devices.

2.6.4 MP-06(08) Media Sanitization | Remote Purging or Wiping of Information

Provide the capability to purge or wipe information from the information system remotely; under the following conditions: the system or its component has been obtained by unauthorized individuals.

2.7 MP-07 Media Use (L, M, H)

a. Restrict the use of non-FIPS 140-2 compliant digital storage devices, to include but not limited to backup media, removable media, and mobile devices on all ED information systems using technical and nontechnical controls; and

[12] MP-06(01) 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. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

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 Directives
BOD	Binding Operational Directive
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CSF	Cybersecurity Framework
CT.DM-P	Data Processing Management
CT.PO-P	Data Processing Policies, Processes, and Procedures
CT-P	Control-P
CUI	Controlled Unclassified Information
DE	Detect
DE.DP	Detection Processes
Department	U.S. Department of Education
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
FTI	Federal Tax 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
IRS	Internal Revenue Service
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
L	Low
M	Moderate
MP	Media Protection 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
PO	Principal Office
PR	Protect
PR.DS	Data Security
PR.DS-P	Data Security
PR.IP	Information Protection Processes and Procedures

Acronym	Definition
PR.PT	Protective Technology
PR.PT-P	Protective Technology
PR-P	Protect-P
PUB	Publication
RAF	Risk Acceptance Form
SAOP	Senior Agency Official for Privacy
SP	Special Publication

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
MP-01	Policy and Procedures	X	X	X	X	PR.PT, DE.DP, GV.PO-P, GV.MT-P, PR.PT-P	PR.PT-2, DE.DP-2, GV.PO-P1, GV.PO-P3, GV.PO-P5, GV.MT-P2, GV.MT-P6, PR.PT-P1
MP-02	Media Access		X	X	X	PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1
MP-03	Media Marking			X	X	PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1
MP-04	Media Storage			X	X	PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1
MP-04(02)	Media Storage | Automated Restricted Access					PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1
MP-05	Media Transport			X	X	PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1
MP-05(03)	Media Transport | Custodians					PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1
MP-06	Media Sanitization	X	X	X	X	PR.DS, PR.IP, CT.PO-P, CT.DM-P, PR.DS-P	PR.DS-1, PR.DS-3, PR.IP-6, CT.PO-P2, CT.DM-P5, PR.DS-P1, PR.DS-P3
MP-06(01)	Media Sanitization | Review, Approve, Track, Document, and Verify				X	PR.DS, PR.IP, CT.PO-P, CT.DM-P, PR.DS-P	PR.DS-1, PR.DS-3, PR.IP-6, CT.PO-P2, CT.DM-P5,

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
							PR.DS-P1, PR.DS-P3
MP-06(02)	Media Sanitization | Equipment Testing				X	PR.DS, PR.IP, CT.PO-P, CT.DM-P, PR.DS-P	PR.DS-1, PR.DS-3, PR.IP-6, CT.PO-P2, CT.DM-P5, PR.DS-P1, PR.DS-P3
MP-06(03)	Media Sanitization | Nondestructive Techniques				X	PR.DS, PR.IP, CT.PO-P, CT.DM-P, PR.DS-P	PR.DS-1, PR.DS-3, PR.IP-6, CT.PO-P2, CT.DM-P5, PR.DS-P1, PR.DS-P3
MP-06(07)	Media Sanitization | Dual Authorization					PR.DS, PR.IP, CT.PO-P, CT.DM-P, PR.DS-P	PR.DS-1, PR.DS-3, PR.IP-6, CT.PO-P2, CT.DM-P5, PR.DS-P1, PR.DS-P3
MP-06(08)	Media Sanitization | Remote Purging or Wiping of Information					PR.DS, PR.IP, CT.PO-P, CT.DM-P, PR.DS-P	PR.DS-1, PR.DS-3, PR.IP-6, CT.PO-P2, CT.DM-P5, PR.DS-P1, PR.DS-P3
MP-07	Media Use		X	X	X	PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1
MP-07(02)	Media Use | Prohibit Use of Sanitization-resistant Media					PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1
MP-08	Media Downgrading					PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1
MP-08(01)	Media Downgrading | Documentation of Process					PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1

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
MP-08(02)	Media Downgrading | Equipment Testing					PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1
MP-08(03)	Media Downgrading | Controlled Unclassified Information					PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1
MP-08(04)	Media Downgrading | Classified Information					PR.DS, PR.PT, PR.DS-P, PR.PT-P	PR.DS-1, PR.PT-2, PR.DS-P1, PR.PT-P1