Information Technology (IT) System Media Protection (MP) 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 16:03:41 -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
1.1 Purpose 1
1.2 Scope 1
2 STANDARDS 1
2.1 MP-1 Media Protection Policy and Procedures (P, L, M, H) 2
2.2 MP-2 Media Access (L, M, H) 3
2.3 MP-3 Media Marking (M, H) 3
2.4 MP-4 Media Storage (M, H) 3
2.5 MP-5 Media Transport (M, H) 3
2.6 MP-6 Media Sanitization (P, L, M, H) 4
2.7 MP-7 Media Use (L, M, H) 4
3 RISK ACCEPTANCE/POLICY EXCEPTIONS 4
4 ACRONYMS 6
5 APPENDIX A - BASELINE CONTROL PARAMETER SUMMARY 7

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 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, 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 media protection control standards.

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 199 categorization level (e.g., Low (L), Moderate (M) and High (H)) is assigned to each requirement. This designator indicates a

[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

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 (DHS), Cybersecurity & Infrastructure Security Agency (CISA).

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 MP-1 Media Protection 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 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 OCIO: 3-112/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-2 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-digital media to include but not limited to paper documents and microfilm to ED approved personnel and roles.

2.3 MP-3 Media Marking (M, H)

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 from marking if the media remains within ED-authorized and controlled areas in accordance with OCIO: 3-112/ACSD-OCIO-004 *Cybersecurity Policy* and OCIO 3-113/ACSD-OCIO-002 *Controlled Unclassified Information Program* for media storing and/or processing CUI.

2.4 MP-4 Media Storage (M, H)

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-5 Media Transport (M, H)

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.

2.6 MP-6 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-6(1) Media Sanitization | Review, Approve, Track, Document, and Verify (H)

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

2.6.2 MP-6(2) 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-6(3) 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.

2.7 MP-7 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

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

ACS	Administrative Communication System
AO	Authorizing Official
ATO	Authorization to Operate
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CSAM	Cyber Security Assessment and Management tool
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
ED	Department of Education
EO	Executive Order
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Modernization Act
IAS	Information Assurance Services
ISO	Information System Owner
ISSO	Information Systems Security Officer
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PO	Principal Office
RAF	Risk Acceptance Form
SAOP	Senior Agency Official for Privacy
SP	Special Publication

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
MP-1	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-2	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-3	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-4	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-4(2)	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-5	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-5(3)	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-6	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-6(1)	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, PR.DS-P1, PR.DS-P3
MP-6(2)	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

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
MP-6(3)	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-6(7)	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-6(8)	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-7	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-7(2)	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-8	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-8(1)	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
MP-8(2)	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-8(3)	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-8(4)	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