Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19

Information Security – Media Protection (MP) Procedure

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of the security control requirements for the Media Protection (MP) control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.*

2. SCOPE

These procedures address all United States Environmental Protection Agency (EPA) information and information systems to include information and information systems used, managed or operated by a contractor, another agency or other organization on behalf of the EPA.

3. AUDIENCE

Senior Information Officials (SIO), Information Security Officers (ISO) and EPA System Owners (SO) or their official designees, for EPA-operated systems, and Service Managers (SM), for systems operated on behalf of the EPA, EPA employees, contractors and all other users of EPA information and systems.

4. BACKGROUND

EPA is responsible for ensuring all offices within the Agency meet the minimum-security requirements defined in the Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems. All EPA information systems shall meet security requirements by implementing the security controls defined in the NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations.*

This document adopts procedures and standards for the EPA consistent with FIPS Publication 200.

5. AUTHORITY

Additional legal foundations for the Media Protection Procedure include:

- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)

- OMB Circular A-130, “Management of Federal Information Resources”, Appendix III, “Security of Federal Information Resources,” November 2000
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- EPA Information Security Policy
- EPA Roles and Responsibilities Procedures

6. PROCEDURE

SIO, ISO and EPA SO or their official designees for EPA-operated systems; and SM, for systems operated on behalf of the EPA and to the extent made applicable to their management of the system though a contract or other appropriate mechanism, are responsible for implementing the controls in this procedure. EPA is adopting this procedure agency-wide, and expects these officials to develop a plan with timelines for adoption for their system(s). EPA employees, contractors and all other users of EPA information and information systems that support the operations and assets of the EPA should be aware of the content of this procedure and should follow the directions provided by SIO, ISO and EPA SO or their official designees and SM for the systems that they oversee.

The "MP" designator (e.g., MP-2, MP-3) identified for each procedure below corresponds to the NIST- identifier for the Media Protection control family, as identified in NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*.

NIST defines the applicable MP security and privacy baseline controls in NIST 800-53B, *Control Baselines for Information Systems and Organizations*. The applicable security baseline for each impact level (Low, Moderate, High or For All Systems) as well as the Privacy Control Baseline are identified below the control name.

MP-2 – Media Access

For All Systems:

1) Restrict access to authorized EPA digital removable storage media (RSM) including but not limited to disks, magnetic tapes, universal serial bus (USB) thumb/flash drives; external (removable) hard drives or solid-state drives; digital video disks (DVD) compact disks (CD); and non-digital media including, paper and microfilm to only authorized users.

MP-3 – Media Marking

For Moderate and High Systems:

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

2) Exempt media containing publicly releasable or non-sensitive information from markings if the media remains within an EPA-controlled environment.

MP-4 – Media Storage

For Moderate and High Systems:

1) Physically control and securely store all digital and non-digital media within EPA-controlled areas; and
2) Protect system media types defined in MP-4 1) until the media are destroyed or sanitized using approved equipment, techniques, and procedures.[1]

MP-5 – Media Transport

For Moderate and High Systems:

1) Protect and control all digital and non-digital media containing controlled unclassified information (CUI) during transport outside of controlled areas using a locked container or a device that is protected by FIPS 140-2 and when available 140-3 cryptography;
2) Maintain accountability for system media during transport outside of controlled areas;
3) Document activities associated with the transport of system media; and
4) Restrict the activities associated with the transport of system media to authorized personnel.

MP-6 – Media Sanitization

For All Systems and Privacy Control Baseline:

1) Sanitize all system media (both digital and non-digital) prior to disposal, release out of organizational control, or release for reuse using approved sanitization equipment, techniques, and procedures; and
2) Employ sanitization mechanisms with the strength and integrity commensurate with the security category of classification of the information.

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

For High Systems:

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

[1] *Refer to MP-6 Media Sanitization and Disposal*

MP-6(2) – Media Sanitization | Equipment Testing

For High Systems:

1) Test sanitization equipment and procedures at least quarterly to ensure that the intended sanitization is being achieved.

MP-6(3) – Media Sanitization | Nondestructive Techniques

For High Systems:

1) Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: prior to initial use, or when organizations cannot maintain a positive chain of custody for the devices.

MP-7 – Media Use

For All Systems:

1) Prohibit the use of unauthorized and non-FIPS compliant mobile devices and EPA digital RSM including: backup devices/storage media; USB thumb/flash drives; external (removable) hard drives or solid-state drives on EPA information systems using technical controls such as group policy and other network controls; and
2) Prohibit the use of portable storage devices in EPA systems when such devices have no identifiable owner.

7. ROLES AND RESPONSIBILITIES

The Information Security – Roles and Responsibilities procedure provides roles and responsibilities for personnel who have IT security or related governance responsibility for protecting the information and information systems they operate, manage and support.

8. RELATED INFORMATION

- National Security Agency (NSA)/Central Security Services (CSS) Evaluated Products List for High Security Crosscut Paper Shredders, Version AA (Paper Only)
- NSA/CSS Evaluated Products List for Punched Tape Disintegrators, January 2021
- NSA/CSS Evaluated Products List for Optical Media Destruction Devices, January 2021
- NSA/CSS Evaluated Product List for Magnetic Degaussers, July 2021
- NSA/CSS Storage Device Declassification Manual (SDDM), (Storage Devices)
- NSA/CSS Evaluated Products List (EPL) for High-Security Disintegrators, January 2012
- Toxic Substances Control Act (TSCA) CBI Protection Manual, 2004

- NIST Special Publications, 800 series
- FIPS 140-3, Security Requirements for Cryptographic Modules
- Federal Identity, Credential and Access Management (FICAM)
- Information Directive No: CIO 2158.0, Interim Controlled Unclassified Information Policy

9. DEFINITIONS

- **Authentication** – the process of verifying the identity of a user, process or device, often as a prerequisite to allowing access to resources in an information system.
- **Availability** – ensuring timely and reliable access to, and use of, information.
- **Confidentiality** – preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.
- **Controlled Access Area** – any area or space within a facility for which the EPA has confidence that physical and procedural protections provided are sufficient to meet the EPA's authorized access requirements established for protecting the information and/or information system (generally a controlled area is within a facility not owned or managed solely by the EPA). This area may be within a publicly accessible facility or a controlled access facility.
- **Controlled Access Facility** – a facility where access at the facility entrance is physically or procedurally controlled and is limited to individuals authorized to access the facility. This may include government or non-government organizations that inhabit the facility other than the EPA.
- **Controlled Area** – any area or space for which the EPA has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
- **Controlled Limited Access Area** – an area or office space, generally within a controlled access area, that further restricts access to a smaller subset of authorized individuals.
- **E-discovery (electronic discovery)** – any process in which electronic data is sought, located, secured and searched with the intent of using it as evidence in a civil or criminal legal case.
- **Information** – Any communication or representation of knowledge such as facts, data or opinions in any medium or form including text, numeric, graphic, cartographic, narrative, electronic or audiovisual forms.
- **Information Security** – the protection of information and information systems from a link unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability.
- **Information Security Policy** – an aggregate of directives, regulations, rules and practices that prescribe how an organization manages, protects and distributes information.

- **Information System** – a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.
- **Information Technology** – any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by the executive agency.
- **Information Type** – a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy or regulation.
- **Integrity** – guarding against improper information modification or destruction and includes ensuring information nonrepudiation and authenticity.
- **Labeling** – the application or use of security attributes with regard to internal data structures within the information system.
- **Marking** *(see also security marking)* – the means used to associate a set of security attributes with objects in a human-readable form in order to enable organizational, process-based enforcement of information security policies.
- **Media** – physical devices or writing surfaces including magnetic tapes, optical disks, magnetic disks, Large-Scale Integration memory chips and printouts (but excluding display media) onto which information is recorded, stored or printed within a system.
- **Media Sanitization** – actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
- **Organization** – a federal agency or, as appropriate, any of its operational elements.
- **Overwriting [media]** – writing to the entire media storage space with a predetermined pattern of meaningless information, usually 0's, 1's and random or pseudo-random data, effectively rendering any data unrecoverable. Reformatting media is neither sufficient nor equivalent to overwriting.
- **Protection Level Markings** – the EPA has three basic protection level markings related to data or information confidentiality. These protection levels can be augmented in marking to include the content and/or governing statute (examples include "Restricted – PII," "Restricted – Privacy Act," "Restricted – Controlled Unclassified Information" or "Restricted - TSCACBI"). The three protection levels and associated markings are: Unrestricted data, which is accessible to anyone for any reason; Restricted data, which is not accessible to the general public, is accessible to data subjects or data suppliers and is accessible only to authorized users; and Protected data, which is accessible to only authorized users and not the general public.
- **Removable Media** – includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks and digital video disks) and non-digital media (e.g., paper, microfilm).
- **Risk** – a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact or magnitude of harm that would arise if the circumstance or event occurs and (ii) the likelihood of occurrence.

- **Risk Assessment** – the process of identifying risks to organizational operations (including mission, functions, image or reputation), Agency assets and other organizations, individuals or the Nation arising through the operation of the information system. Part of risk management, synonymous with risk analysis, incorporates threat and vulnerability analyses and considers mitigations provided by planned, or in place, security controls.
- **Risk Management** – the program and supporting processes to manage risk to Agency operations (including mission, functions, image, reputation), Agency assets, individuals, other organizations and the Nation, including establishing the context for risk-related activities, assessing risk, responding to risk once determined and monitoring risk over time.
- **Sanitization** – a process to render access to target data on the media infeasible for a given level of effort. Clear, purge and destroy are actions that can be taken to sanitize media.
- **Secured Means of Transport** – secured means of transport is determined by documented risk assessments and varies depending on the media. Secure transport of non-digital media includes, but is not limited to, media contained in marked and addressed envelopes within an "official" commercial carrier container (e.g., United Parcel Service, FedEx, etc.) Secure transport of digital media includes, as a minimum, use of encryption. Transport protections for some small handheld device type media may include, but are not limited to, password protection and electronic deactivation or erasure if control has been compromised.
- **Signature** (of an individual) – a mark or sign made by an individual to signify knowledge, approval, acceptance or obligation (can be accomplished manually, sometimes referred to as a "wet signature," or electronically).
- **User** – individual or (system) process authorized to access a system.
- **Written** (or in writing) – means to officially document, manually or electronically, the action or decision and includes a signature.

10. WAIVERS

Waivers or deviations may be requested through the EPA Risk Determination Process based on a substantive business need and the implementation of compensating controls that provide a suitable alternative to the mandated protection.

Only EPA's Chief Information Officer may authorize Agency-wide waivers or deviations from the standards herein.

11. MATERIAL SUPERSEDED

Information Directive: CIO 2150-P-10.2, Information Security – Media Protection Procedures

12. CONTACTS

For further information, please contact the OMS, Office of Information Security and Privacy (OISP).

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2023.07.18 08:38:09 -04'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information and Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS & ABBREVIATIONS

CBI	Confidential Business Information
CIO	Chief Information Officer
CISO	Chief Information Security Officer
EPA	Environmental Protection Agency
EPL	Evaluated Products List
FICAM	Federal Identity, Credential and Access Management
FIPS	Federal Information Processing Standards
ISSO	Information Systems Security Officer
NIST	National Institute of Standards and Technology
NSA/CSS	National Security Agency/Central Security Service
OMB	Office of Management and Budget
OMS	Office of Mission Support
PII	Personally Identifiable Information
RSM	Removable Storage Media
SDDM	Storage Device Declassification
SP	Special Publication
TSCA	Toxic Substances Control Act
U.S.C.	United States Code