Information Security – Media Protection Procedures			
EPA Classification No.:	CIO 2150-P-10.2	CIO Approval Date:	01/08/2016
CIO Transmittal No.:	16-005	Review Date:	01/08/2019

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

INFORMATION SECURITY – MEDIA PROTECTION PROCEDURES

1. PURPOSE

To implement 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 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

2. SCOPE AND APPLICABILITY

The procedures cover all 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.

The procedures apply to all EPA employees, contractors, and all other users of EPA information and information systems that support the operation and assets of the EPA.

3. AUDIENCE

The audience is all EPA employees, contractors, and all other users of EPA information and information systems that support the operations and assets of the EPA.

4. BACKGROUND

Based on federal requirements and mandates, the 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 the security requirements using the security controls defined in the NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.* This document addresses the procedures and standards set forth by the EPA, and complies with the family of Media Protection controls.

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III, Federal Information Security Management Act (FISMA) as amended
- Federal Information Security Modernization Act of 2014, Public Law 113-283, chapter 35 of title 44, United States Code (U.S.C.)

- Freedom of Information Act (FOIA), 5 U.S.C. § 552, as amended by Public Law 104-231, 110 Stat. 3048, Electronic Freedom of Information Act Amendments of 1996
- Clinger-Cohen Act of 1996, Public Law 104-106
- Paperwork Reduction Act of 1995 (44 USC 3501-3519)
- Privacy Act of 1974 (5 USC § 552a) as amended
- USA PATRIOT Act of 2001, Public Law 107-56
- Code of Federal Regulations (C.F.R), Part 5 Administrative Personnel, Subpart C — Employees Responsible for the Management or Use of Federal Computer Systems, Section 930.301 through 930.305 (5 C.F.R 930.301-305)
- C.F.R, Part 2001 and 2003, “Classified National Security Information,” (32 C.F.R)
- Office of Management and Budget (OMB) Memorandum M-06-16, “Protection of Sensitive Agency Information,” June 2006 Office of Management and Budget (OMB)
- Memorandum M-02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones," October 2001
- OMB Circular A-130, “Management of Federal Information Resources”, Appendix III, “Security of Federal Information Resources,” November 2000
- Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 2001
- FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, February 2004
- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems, March 2006
- FIPS 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
- EPA Information Security Program Plan
- EPA Information Security Policy
- EPA Records Management Policy
- EPA Roles and Responsibilities Procedures
- EPA Information Security Continuous Monitoring Strategic Plan
- CIO Policy Framework and Numbering System

6. PROCEDURES

The "MP" designator identified in each procedure represents the NIST-specified identifier for the Media Protection control family, as identified in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*

Abbreviations including acronyms are summarized in Appendix A.

MP-2 – Media Access

For All Information Systems:

1) System Owners (SO), in coordination with Information Security Officers (ISO), Information Management Officers (IMO), Information Owners (IO), and Information System Security Officers (ISSO), for EPA-operated systems shall; and Service Managers (SMs), in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

    a) Permit only authorized user access to digital and non-digital media.

    b) Perform assessment of risk to guide the selection of media for storage, transport, backup, etc., and the associated information contained on that media requiring restricted access.

    c) Protect unmarked media until determining information type, marking requirements and appropriately marking, then employ appropriate protection measure(s).

    d) Document the processes required to ensure the protection of media and the information on the media of their information system from unauthorized access.

        i) This includes, but is not limited to, backup media such as tapes or disks and non-digital media such as printouts.

    e) Use only approved EPA removable digital media to store EPA data.

        i) The removable media shall be encrypted unless the EPA Deputy Administrator or Chief Information Officer has identified all data on the device as non-sensitive in writing.

        ii) Following insertion into, or connection with a non-EPA information system, security personnel shall check EPA-owned USB removable media for malware using a system that is disconnected from EPA systems and networks.

            (1) The secured system shall be isolated from EPA networks, and other EPA systems, and have system ‘autorun’ capabilities deactivated.

            (2) The secured system shall utilize at least one form of anti-malware software to review the removable media for evidence of malware. The anti-malware software shall be kept up-to-date with the latest malware signature updates in order to detect the latest threats.

            (3) Detected malware shall be safely removed from the digital media and verified by rechecking to ensure that the media is safe for use prior to use on EPA systems and networks.

    f) Use NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* for guidance on mapping security impact levels to types of information and information systems.

    Note: Information system 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 and microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).

MP-2(1) – Media Access | Automated Restricted Access

Incorporated into MP-4(2).

MP-2(2) – Media Access | Cryptographic Protection

Incorporated into SC-28(1).

MP-3 – Media Marking

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:
    a) Validate that Information system personnel mark paper and other output products appropriately in accordance with EPA protection requirements, and Parts 2001 and 2003, *Classified National Security Information*, 32 Code of Federal Regulations (C.F.R).
    b) Ensure the assessment of risk guides the selection of media requiring marking.
        i) NIST SP 800-30, *Guide for Conducting Risk Assessments*, shall be used for guidance on conducting risk assessments of federal information systems and organizations, amplifying the guidance in NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View.*
    c) Direct information system personnel and users to adhere to the following when marking documents that contain confidential, restricted or sensitive information:
        i) Mark documents appropriately in accordance with applicable policies and procedures set forth by the EPA so that it is immediately apparent that the information shall be protected from unauthorized disclosure.
        ii) Apply applicable stamps or marks that detail the highest level of protected information contained in the document to the top and bottom of the front and back cover, and on the first and last page.
            (1) If the last page is not blank, then apply the stamp to the blank back cover.
            (2) Annotate all other pages with the highest level of categorization contained on each page.
            (3) Pages that contain information not requiring protection should be annotated as ‘unrestricted’.
        iii) If a document appears as though it may contain information other than “unrestricted,” treat the document as if it is at least “restricted” until its status can be verified with the authoritative source.[1]

[1] *Refer to the definition of protection level markings in Section 9 of this document.*

iv) As required by the document source or originator, documents containing high confidentiality information may be required to be logged and tracked. These documents shall then be submitted to a designated Document Control Officer (DCO) for logging and tracking purposes.

d) Mark restricted and sensitive information appropriately and clearly in accordance with Parts 2001 and 2003, *Classified National Security Information: Subpart C – Identification and Markings*, 32 C.F.R.

e) Mark digital media and cover sheets with the following:

i) Any applicable security markings. “Unrestricted” information or information of low confidentiality (FIPS 199) does not require marking but may be marked at the discretion of the SO or IO.

ii) Mark media to the most restrictive protection level of the information contained on the media.

f) Adhere to marking requirements and guidelines provided by the SO and the *EPA Records Management Program* for records scheduled for archival.

For FedRAMP[2] Moderate Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Prohibit any types of removable media to be used with EPA-owned information.

MP-4 – Media Storage

For Moderate and High Information Systems:

Note: Information system 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 and microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop/tablet computers, personal digital assistants, smart phones, cellular telephones, digital cameras, and audio recording devices).

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Physically control and securely store all digital and non-digital media within defined controlled areas using defined security measures.[3]

b) Ensure the assessment of risk guides the selection of media and associated information contained on that media requiring physical protection.

[2] *The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.*

[3] *Refer to Appendix B for storage protection guidelines.*

i) NIST SP 800-30, *Guide for Conducting Risk Assessments,* shall be used for guidance on conducting risk assessments of federal information systems and organizations, amplifying the guidance in NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View.*

ii) Protected, classified, sensitive, and restricted information stored by EPA personnel and contractors shall be physically controlled and safeguarded in the manner prescribed for the highest categorization level of the information contained on the media until the media is sanitized or destroyed, in accordance with 32 CFR, parts 2001 and 2003, Executive Order 13526; *Classified National Security Information*, and EPA protection requirements.

c) Encrypt data stored on secondary storage devices (devices that retain copies of data stored on primary data storage devices) as required for the protection of the highest level of information contained therein.

i) The employment of cryptographic mechanisms shall be based upon maintaining the confidentiality and integrity of the information.[4]

ii) The strength of mechanisms shall be commensurate with the categorization and sensitivity of the information.

d) Protect information system media until the media's destruction or sanitization via approved equipment, techniques, and procedures.[5]

e) Maintain a secure, environmentally appropriate facility for archiving digital and non-digital media, identified in the General Records Schedule (GRS), in compliance with National Archives and Records Administration (NARA) regulations on electronic records management.

i) This includes a secure and environmentally correct archival facility for the storage of tapes (e.g., cartridge and reel) or other digital and non-digital media containing data that shall be maintained, but has no immediate processing need.

f) Retain archived data in accordance with EPA Records Management Policy.

i) Upon reaching the end of the timeframe for archived digital and non-digital media (prescribed by the EPA Records Management Policy and/or the specific records schedule, the media is released to the SO for disposition in accordance with record retention schedules related to the information or information system.

(1) Specific EPA records schedules may be located using the EPA records schedule locator at http://www.epa.gov/records/policy/schedule/index.htm.

(2) Information system personnel shall test a statistical sample of archived digital media annually to ensure that the digital media are in good condition and are accessible.

ii) NIST SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* and NIST SP 800-56B, *Recommendation for*

[4] *All cryptography is expected to be implemented using FIPS 140-2 validated modules in FIPS mode.*

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

Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography shall be used for guidance on cryptographic key establishment.

iii) NIST SP 800-57, *Recommendation for Key Management* shall be used for guidance on cryptographic key management.

iv) NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices* shall be used for guidance on storage encryption technologies.

MP-4(1) – Media Storage | Cryptographic Protection

Incorporated into SC-28(1).

MP-4(2) – Media Storage | Automated Restricted Access

Not selected as part of the control baseline.

MP-5 – Media Transport

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:
   a) Guarantee the protection and control of all digital and non-digital media during transport outside of controlled areas using defined security measures (e.g., locked container, cryptography) that are agency-approved, FIPS 140-2 validated or compliant encryption technologies.
   b) Maintain accountability for information system media during transport outside of controlled areas using defined security measures (e.g., locked container, cryptography) that are agency-approved, FIPS 140-2 validated or compliant encryption technologies.
   c) Restrict activities associated with transport of information system media to authorized personnel.
   d) Use the assessment of risk to guide the selection of media and associated information contained on that media requiring physical protection:
      i) NIST SP 800-30, *Guide for Conducting Risk Assessments*, shall be used for guidance on conducting risk assessments of federal information systems and organizations, amplifying the guidance in NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.
      ii) The selection of media and associated information contained on that media requiring protection during transport.
      iii) The selection and use of storage containers for transporting non-digital media outside controlled areas within the EPA.
   e) Guarantee physical and technical security measures for the protection of digital and non-digital media are approved by the ISO, commensurate with the categorization or sensitivity of the information residing on the media and consistent with any federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

f) Document, using defined documentation methods, activities associated with the transport of media containing “protected” or “restricted” information outside controlled areas within the EPA.

  i) The logging or tracking requirements for activities associated with the transport of media shall be based on the SO documented assessment of risk to include the flexibility to define different record-keeping methods for different types of media transport as part of an overall system of transport-related records.

  ii) NIST SP 800-30, *Guide for Conducting Risk Assessments* shall be used for guidance on conducting risk assessments of federal information systems and organizations, amplifying the guidance in NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*.

  iii) Any log or tracking mechanism shall include, at a minimum:

    (1) Description of information being transported.

    (2) Type of “protected” or “restricted” information (e.g., PII, CBI) contained on the media.

    (3) Method(s) of transport.

    (4) Protection measures employed.

    (5) Name(s) of individual(s) transporting the information (if appropriate).

    (6) Authorized recipient(s).

    (7) Dates sent and received.

g) Obtain official management approval and document this approval in instances where it is necessary to remove or transport sensitive document(s) or media containing “protected” or “restricted” information outside of controlled areas of the EPA.

  i) Management shall be satisfied that the organization’s requirements for securing sensitive information are being met.

h) Ensure that before transporting, delivering or mailing media containing “protected” or “restricted” information, individuals shall:

  i) Notify the entity authorized to receive the information.

  ii) Document the following information:

    (1) An identifying document number, if used.

    (2) Description of the information.

    (3) Name and signature of the sender.

    (4) Date sent.

  iii) Double wrap the media.

  iv) Mark the inner wrapping with the recipient’s name and the statement “Protected” (or “Restricted”) – “To Be Opened by Addressee Only.”

    (1) Other appropriate descriptors may be appended to the protection labels.

  v) Mark the outer wrapper with the name and address of the recipient and a return address.

vi) Ensure there is no indication on the outer wrapper that the package contains "protected" or "restricted" information.[6]

vii) Use an acknowledgement of receipt on media transported by a common carrier.

i) Ensure personnel store media marked as "protected" or "restricted" information in a locked trunk while in route by car.

  i) If a trunk is not available in the vehicle, the media shall be hidden from sight.

j) Prohibit personnel from leaving media containing "protected" or "restricted" information in a vehicle overnight.

k) Ensure if media containing "protected" or "restricted" information is being transported and delivered by hand, then it will be given directly to the recipient or another authorized individual.

  i) Acknowledgement of receipt shall be used.

l) Ensure if "protected" or "restricted" information is faxed, an authorized individual will attend both the sending and receiving fax machines.

  i) The fax transmission-confirmation receipt of the faxed document containing "protected" or "restricted" information shall be attached or stored with the document.

  ii) The document shall be placed in the official document file, if applicable.

m) Adhere to the following when in receipt of media containing "protected" or "restricted" information:

  i) Sign for acceptance of contents.

  ii) Return the original receipt, if used, to the sender within five business days.

  iii) Maintain a copy of the receipt for their files.

    (1) This may require printing out tracking data for delivery confirmation mechanisms.

MP-5(1) – Media Transport | Protection Outside of Controlled Areas

Incorporated into MP-5.

MP-5(2) – Media Transport | Documentation of Activities

Incorporated into MP-5.

MP-5(3) – Media Transport | Custodians

Not selected as part of the control baseline.

MP-5(4) – Media Transport | Cryptographic Protection

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

[6] *Refer to the definition of secured means of transport in Section 9 of this document.*

a) Use cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas[7].

Note: This requirement also applies to mobile devices including portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones).

MP-6 – Media Sanitization

For All Information Systems:

Note: This control applies to all media subject to disposal or reuse, whether or not considered removable.

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Sanitize all information system media (both digital and non-digital) using approved equipment, techniques, and procedures prior to disposal, release out of organizational control or release for reuse.

i) Employ sanitization mechanisms with the strength and integrity commensurate with the categorization or sensitivity of the information.

ii) Use sanitization techniques, including degaussing and overwriting memory locations and physical destruction, to ensure that the information on media is not disclosed to unauthorized individuals when such media is reused or released for disposal.

(1) All Agency records shall be properly identified, retrieved from the media, if necessary, and processed in accordance with the *EPA Records Management Policy*.

(2) The media and information shall not be sanitized, disposed of, or destroyed if they are subject to ongoing e-discovery litigation or other legal requirement.

(3) Media shall be sanitized using approved equipment and techniques.

(4) When large numbers of media are being sanitized, a representative sample shall be tested to ensure proper sanitization.

(a) Take and test samples at random intervals if sanitization will be performed over a long period of time.

(5) Verification of samples shall be documented such that the media can be identified if necessary.

iii) Remove all electronic information and licensed software when disposing of computers with hard drives and clean IT resources and digital storage of all information.

iv) For sanitizing media:

[7] *Refer to Information EPA Security – System and Communications Protection Procedures for guidance on the use of cryptography*

(1) At a minimum, a triple-pass overwrite method shall be used, where data is overwritten with, for example, 0’s, then 1’s, and then with pseudo-random data.

(2) Any system containing a hard drive or digital media that has information categorized as high confidentiality shall be overwritten at least seven times in this manner.

Note: After overwriting, the hard drive is still physically functional and can accept formatting. Therefore, the media can be reissued and used within the Agency.

b) Consult, when handling sensitive information, with EPA offices on the appropriate IT and programmatic-related records management schedules to determine if and when the information should be destroyed.

c) Validate that media sanitization equipment, techniques and procedures comply with NIST SP 800-36, *Guide to Selecting Information Technology Security Products*.

d) Refer to media types and the requirements on sanitization of such media contained in NIST SP 800-88, *Guidelines for Media Sanitization*, Appendix A, *Minimum Sanitization Recommendation for Media Containing Data*; and Appendix C, *Tools and Resources,* for additional information.

e) Ensure the product selected for sanitizing, destroying or disposing of media containing sensitive or classified information are listed on the National Security Agency’s Evaluated Products Lists which covers: crosscut paper shredders, optical media, degaussers, storage devices and disintegrators.[8]

f) Ensure media destruction and disposal are:

i) Performed in an environmentally approved manner.

ii) Undertaken when the information is no longer needed in accordance with requirements set forth by the Agency, SO and IO.

iii) Accomplished in a safe and effective manner, especially when physically destroying nonmagnetic (i.e., optical) media (e.g., CDs, DVDs).

iv) Addressed in the System Security Plan (SSP).

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

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Track, document, and verify media sanitization and disposal actions.

b) Create and retain a log for all media destroyed.

c) Work in coordination with the SAISO to develop EPA Standard Operating Procedure (SOP) for media sanitization.

i) Train users on these SOP(s).

[8] *For media destruction guidance, please see:* http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml.

ii) The SOP(s) for media sanitization shall include steps to document the following information:

(1) Report date.

(2) Sanitization completion date.

(3) Media being sanitized (including serial number or other uniquely identifiable characteristic, if applicable).

(4) Party performing sanitization.

(5) Sanitation method employed.

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

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Test media sanitization equipment and procedures for effectiveness at least quarterly.

For FedRAMP Moderate Information Systems:

1) SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Test sanitization equipment and procedures at least annually using approved equipment and techniques.

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

For High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Sanitize portable removable storage devices (e.g., thumb drives, flash drives, and external storage devices) prior to connecting such devices to the information system under the following circumstances: refer to NIST SP 800-88, *Guidelines for Media Sanitization* for additional guidelines.

Note: Portable, removable storage devices can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown sources and may contain various types of malicious code that can be readily transferred to the information system through USB ports or other entry portals. While scanning such devices is always recommended, sanitization provides additional assurance that the device is free of all malicious code to include code capable of initiating zero-day attacks.

b) Consider the sanitization of portable, removable storage devices shall when:

i) Such devices are first purchased from the manufacturer or vendor prior to initial use; or,

ii) The organization loses a positive chain of custody for the device.

c) Use an assessment of risk to guide the specific circumstances for employing the sanitization process.

i) NIST SP 800-30, *Guide for Conducting Risk Assessments* shall be used for guidance on conducting risk assessments of federal information systems and organizations, amplifying the guidance in NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View.*

MP-6(4) – Media Sanitization | Controlled Unclassified Information

Incorporated into MP-6.

MP-6(5) – Media Sanitization | Classified information

Incorporated into MP-6.

MP-6(6) – Media Sanitization | Media Destruction

Incorporated into MP-6.

MP-6(7) – Media Sanitization | Dual Authorization

Not selected as part of the control baseline.

MP-6(8) – Media Sanitization | Remote Purging / Wiping of Information

Not selected as part of the control baseline.

MP-7 – Media Use

For All Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems shall; and SM, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Prohibit or restrict the use of non-approved media on EPA information systems.

i) Media types to be used for all EPA-owned information are contingent upon SAISO approval.

MP-7(1) – Media Use

For Moderate and High Information Systems:

1) SOs, in coordination with ISOs, IMOs, IOs, and ISSOs, for EPA-operated systems shall; and SMs, in coordination with IOs, ISOs, IMOs, and ISSOs, for systems operated on behalf of the EPA, shall ensure service providers:

a) Prohibit using portable storage devices on EPA information when such devices have no identifiable owner.

MP-7(2) – Media Use | Prohibit Use of Sanitization-Resistant Media

Not selected as part of the control baseline.

MP-8 – Media Downgrading

Not selected as part of the control baseline.

MP-8(1) – Media Downgrading | Documentation of Process

Not selected as part of the control baseline.

MP-8(2) – Media Downgrading | Equipment Testing

Not selected as part of the control baseline.

MP-8(3) – Media Downgrading | Controlled Unclassified Information

Not selected as part of the control baseline.

MP-8(4) – Media Downgrading | Classified Information

Not selected as part of the control baseline.

7. RELATED DOCUMENTS

- 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 Destruction Devices, Version C, (Punched Tape)
- NSA/CSS Evaluated Products List for Optical Media Destruction Devices, Version H, (Optical Media)
- NSA/CSS Evaluated Product List - Degausser (Magnetic Media Sanitization) 30 March 2009
- NSA/CSS Storage Device Declassification Manual (SDDM), (Storage Devices)
- NSA/CSS Evaluated Products List (EPL) for High-Security Disintegrators, Version O, 25 September 2009 (High Security Disintegrators)
- NIST SP 800-36, Guide to Selecting Information Technology Security Products
- Toxic Substances Control Act (TSCA) CBI Protection Manual, 2004
- NIST Special Publications, 800 series
- Federal Identity, Credential and Access Management (FICAM)

8. ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO), Office of Environmental Information (OEI)

1) The CIO has the following responsibilities with respect to media protection:
   a) Review waiver requests for sufficiency, and approve waivers in the best interests of the Agency.

Senior Agency Information Security Officer (SAISO)

1) The SAISO has the following responsibilities with respect to media protection:
   a) Coordinate to maintain a central repository of all media protection-related waivers.
   b) Document in policy and procedures the specific measures taken to protect media based on requirements of the information it holds.
   c) Document in policy and procedures the media requiring protection during transport and the specific measures taken to protect such transported media.
   d) Develop SOPs for media sanitization.

System Owner (SO)

1) The SO has the following responsibilities with respect to media protection:
   a) Ensure that an assessment of risk guides the selection of media and associated information contained on that media requiring protection and restricted access.
   b) Protect unmarked media at the highest FIPS 199 security category for the information system until the media are reviewed and appropriately marked.
   c) Document the processes required to ensure the protection of media and the information on the media of their information system from unauthorized access.
   d) Ensure EPA data can be stored only on approved EPA removable digital media.
   e) Physically control and securely store information system media within controlled areas.
   f) Protect information system media until the destruction or sanitization of the media using approved equipment, techniques, and procedures.
   g) Consider the employment of cryptography to protect information at rest.
   h) Maintain a secure, environmentally appropriate facility for archiving digital and non-digital media.
   i) Employ cryptographic mechanisms to protect information stored on digital media during transport outside of controlled areas.
   j) Restrict activities associated with transport of information system media to authorized personnel.
   k) Base the selection and use of appropriate storage containers for transporting media on the assessed risk.

l) Approve physical and technical security measures for protecting non-digital media during transportation.

m) Document activities associated with the transport of media containing “protected” or “restricted” information outside controlled areas within EPA and ensure that the logging or tracking requirements are based on the assessed risk.

n) Employ an identified custodian throughout the transport of information system media.

o) Consult with appropriate IT and programmatic-related records management schedules to determine when information should be destroyed.

p) Ensure that all Agency records are properly identified, retrieved from the media, and processed in accordance with *Records Management Policy* prior to sanitization of media.

q) Prior to sanitizing, disposing of, or destroying media, ensure that the media and information are not subject to e-discovery litigation or other legal requirement.

r) Track, document, and verify media sanitization and disposal actions.

s) Create and retain a log of all media destroyed.

t) Ensure that users are trained regarding media sanitation SOPs.

u) Ensure the testing of sanitization equipment and procedures for high information systems, to verify correct performance.

v) Employ cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Information Management Officer (IMO)

1) IMOs have the following responsibilities with respect to media protection:

a) Coordinate with the SAISO in responding to media protection audit requests and reporting.

b) Complete information security awareness training and media protection training prior to initial access to EPA systems and information and at least annually thereafter.

c) Respond to media protection-related security notifications. Such notifications shall be complied with immediately.

d) Coordinate and implement media-protection-related policies, procedures, control techniques, and processes as identified by the SAISO in the Agency information security program.

e) Support the SIO in implementing the SIO’s information technology and information management functions, and responsibilities related to media protection and media sanitation.

Information Owners (IO)

1) IOs have the following responsibilities with respect to media protection:

a) Coordinate with System Owners to ensure resident information is properly disposed of and actions are included in the decommissioning strategy.

b) Develop and implement system decommissioning and information disposal strategies.

c) Ensure information and systems are properly categorized.

d) Conduct impact analyses for proposed or actual changes to systems or their operational environments.

Information Security Officer (ISO)

1) ISOs have the following responsibilities with respect to media protection:

a) Comply with all EPA Information Security Program requirements.

Information System Security Officers (ISSO)

1) ISSOs have the following responsibilities with respect to media protection

a) Ensure the day-to-day security operations of information system sanitization equipment, including verifying that sanitization equipment is functioning as intended.

b) Maintain current and accurate information regarding the equipment.

c) Implement policies, procedures, and control techniques identified in the Agency information security program.

Service Managers (SM)

1) SMs have the following responsibilities with respect to media protection:

a) Permit only authorized users’ access to digital and non-digital media.

b) Perform assessment of risk to guide the selection of media for storage, transport, backup, etc., and the associated information contained on that media requiring restricted access.

c) Protect unmarked media until the media are reviewed and appropriately marked, at which time the commensurate media protection measure(s) will be employed.

d) Document the processes required to ensure the protection of media and the information on the media of their information system from unauthorized access.

i) This includes, but is not limited to, backup media such as tapes or disks and non-digital media such as printouts.

e) Ensure Service Providers use only approved EPA removable digital media to store EPA data.

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 EPA has confidence that the physical and procedural protections provided are sufficient to meet 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 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 EPA.
- *Controlled Area* – any area or space for which 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* – an instance of an information type.
- *Information Security* – the protection of information and information systems from 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* – the application or use of human-readable security attributes.
- *Media* – physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, printouts (but not including display media) onto which information is recorded, stored, or printed within an information system. Digital media include diskettes, tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks; examples of non-digital media are

paper or microfilm. This term also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).

- *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 or nor equivalent to overwriting.
- *Protection Level Markings* – 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: "Restricted – PII," "Restricted – Privacy Act," "Restricted – Controlled Unclassified Information," or "Restricted - TSCA CBI." 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 not accessible to the general public but is accessible only to authorized users.
- *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* – the level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, other organizations, individuals, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
- *Risk Assessment* – the process of identifying risks to Agency operations (including mission, functions, image, or reputation), Agency assets, 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 process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, other organizations, individuals, or the Nation resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for the continuous monitoring of the security state of the information system.
- *Sanitization* – the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed.
- *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 an information system.
- *Written* (or in writing) – means to officially document, manually or electronically, the action or decision and includes a signature.

10. WAIVERS

Waivers may be requested from the CIO by submitting a justification based on:

- Substantive business case need(s)
- Demonstration of, or a proposal for, establishment of adequate compensating controls that provide a suitable alternative to the mandated protection

The CIO may grant a waiver for sufficient reasons exercising judgment in the best interests of the Agency.

The SAISO and Director, OTOP shall coordinate to maintain a central repository of all waivers.

11. RELATED POLICY, PROCEDURES, STANDARDS AND GUIDELINES

Related policy and procedures are available on OEI’s Policy Resources website.

http://intranet.epa.gov/oei/imitpolicy/policies.htm

Related standards and guidelines are available on OEI’s website.

12. MATERIAL SUPERSEDED

- EPA Information Directive – Information Security - Interim Media Protection Procedures, CIO 2150-P-10.1, July 18, 2012.

13. ADDITIONAL INFORMATION

N/A

Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A: ACRONYMS & ABBREVIATIONS

CBI	Confidential Business Information
CD	Compact Disk
CIO	Chief Information Officer
DCO	Document Control Officer
DVD	Digital Video Disk
EPA	Environmental Protection Agency
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GRS	General Records Schedule
IO	Information Owner
ISO	Information Security Officer
ISSO	Information Systems Security Officer
IT	Information Technology
LSI	Large-Scale Integration
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA CSS	National Security Agency Central Security Service
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SM	Service Manager
SO	System Owner
SAISO	Senior Agency Information Security Officer
SOP	Standard Operating Procedures
SP	Special Publication
SSP	System Security Plan
TSCA	Toxic Substances Control Act
USC	United States Code
USB	Universal Serial Bus

APPENDIX B: STORAGE PROTECTION GUIDELINES

INFORMATION CATEGORY **CONFIDENTIALITY LEVEL / PROTECTION LEVEL**	**MEDIA STORAGE PROTECTED ENVIRONMENT GUIDELINES (SELECTION OF “ACCEPTABLE” OR “OPTIMUM” MAY BE RISK DEPENDENT)**		
	UNACCEPTABLE	**ACCEPTABLE**	**OPTIMUM**
High **“Restricted” or “Protected”**	Anywhere in a public space	• In a controlled access facility • In a controlled limited access area • In padlocked and labeled file cabinet or labeled and encrypted (digital media)	• In a controlled access facility • In a controlled limited access area • In a safe or labeled and encrypted (digital media)
Moderate **“Restricted” or “Protected”**		• In a controlled access facility • In locked office space • In a labeled file cabinet or encrypted (digital media) (user ID and password access may be acceptable for some moderate confidentiality information other than sensitive PII)	• In a controlled access facility • In a controlled access area • In locked, labeled file cabinet or encrypted (digital media)
Low **No marking, “Unrestricted” or “Restricted”**		• Anywhere in a controlled access facility	• In a controlled access facility • In locked office space or user ID and password access required.
Public **No marking or “Unrestricted”**	N/A	No Limits	No Limits