EPA INFORMATION PROCEDURES

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.:	CIO-2150.3-P-10.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

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

INFORMATION SECURITY –
INTERIM MEDIA PROTECTION PROCEDURES
V4.1
JULY 18, 2012

1. PURPOSE

The purpose of this procedure is to facilitate the implementation of Environmental Protection Agency (EPA) security control requirements for the Media Protection control family, as identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 3 *Recommended Security Controls for Federal Information Systems and Organizations*.

2. SCOPE AND APPLICABILITY

These procedures cover all EPA information and information systems to include those used, managed, or operated by a contractor, another agency, or other organization on behalf of the Agency.

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

3. AUDIENCE

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

4. BACKGROUND

Based on federal requirements and mandates, the EPA is responsible for ensuring that 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 must meet the security requirements through the use of the security controls defined in the NIST SP 800-53, *Revision 3 Recommended Security Controls for Federal Information Systems and Organizations*. This chapter addresses the procedures and standards set forth by EPA, and in compliance with, the media protection family of controls found in NIST SP 800-53, Revision 3.

EPA Classification No.:	CIO-2150.3-P-10.1	CIO Approval Date:	08/06/2012
CIO Transmittal No.:	12-003	Review Date:	08/06/2015

5. AUTHORITY

- E-Government Act of 2002, Public Law 107-347, Title III*, Federal Information Security Management Act (FISMA)* as amended
- 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, 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)
- Office of Management and Budget (OMB) Memorandum M-06-16, "Protection of Sensitive Agency Information", June 2006
- 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
- EPA Information Security Program Plan
- EPA Information Security Policy

6. PROCEDURES

MP-2 – Media Access

a. Only authorized users are permitted access to digital and non-digital media.

Note: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, 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).

b. Assessment of risk must guide the selection of media for storage, transport, backup, etc., and the associated information contained on that media requiring restricted access.

c. Unmarked media must be protected until the media are reviewed and appropriately

marked, at which time the commensurate measure will be employed.

d. System Owners (SOs) must document the processes required to ensure media and the information on the media of their information system are protected 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. Only approved EPA removable digital media must be used to store EPA data.
    i. The removable digital media must be encrypted if it contains sensitive Personally Identifiable Information (PII) or Confidential Business Information (CBI).
    ii. EPA-owned USB removable media shall not be connected to any non-EPA information system.

For moderate and high information systems

Note: This control enhancement is primarily applicable to media storage areas within an organization where a significant volume of media is stored and is not applicable to every location where some media is stored (e.g., in individual offices).

f. Automated mechanisms must be employed in order to ensure that there is only authorized access to media storage areas and to audit access attempts and access granted, unless guard stations control access to media storage areas.

MP-3 – Media Marking

For moderate and high information systems

a. Information system personnel shall mark human-readable output appropriately in accordance with protection level markings set forth by EPA.
    i. Refer to the definition of protection level markings in Section 9 of this document.
b. A defined list of removable media types may be exempt from marking as long as the exempted items remain within defined controlled areas.
c. The assessment of risk must guide the selection of media requiring marking.
d. Information system personnel and users shall adhere to the following when marking documents that contain confidentially sensitive information:
    i. Mark documents appropriately in accordance with applicable policies and procedures set forth by EPA so that it is immediately apparent that the confidentially sensitive information must be protected from unauthorized disclosure.
        - Identify FIPS 199 sensitivity and protection level indicators in the header or footer of printouts.
    ii. Upon creating, handling, or receiving a document containing information requiring marking, the applicable stamp or watermark detailing the highest level of protection level contained in the document must be applied to the top

and bottom of the front and back cover and on the first and last page.

- If the last page is not blank, then the stamp must be applied to the blank back cover.
- All other pages must be annotated with the highest level of classification contained on each page.
- Pages that contain information not requiring marking should be annotated as "unrestricted".

iii. If a document appears as though it may contain information other than "unrestricted," then the document must be treated as if it is at least "restricted" until its status can be verified with the authoritative source.

- Refer to the definition of protection level markings in Section 9 of this document.

iv. At a minimum, documents containing high confidentiality information must be logged and tracked by the originator. These documents must then be submitted to a designated Document Control Officer (DCO).

e. Information system personnel shall affix printed output with cover sheets (developed by the applicable system personnel) if the printed output is not otherwise appropriately marked.

f. Information system personnel and users shall mark digital media and cover sheets with the following:

i. Distribution limitations.

ii. Handling caveats of the information.

iii. Applicable security markings, if applicable.

- Refer to the definition of protection level markings in Section 9 of this document.

iv. "Unrestricted" information or information of low confidentiality (FIPS 199) does not require marking but may be marked at the discretion of the SO or Information Owner (IO).

- Refer to the definition of protection level markings in Section 9 of this document.

g. Media must be marked to the most restrictive protection level of the information contained on the media.

h. All marking requirements and guidelines provided by the SO and the Records Management Program must be followed for records scheduled for archival.

i. Once a portable computer (i.e., laptop, handheld device) has been approved for high confidentiality information use, it must be marked as a "protected" computer with distinctive markings that are not visible when the computer is not in use.

i. Refer to the definition of protection level markings in Section 9 of this document.

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, digital video disks) and non-digital media (e.g., paper, 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).

a. All digital and non-digital media must be physically controlled and securely stored within defined controlled areas using defined security measures.
    i. Refer to Appendix B for storage protection guidelines.
b. The assessment of risk must guide the selection of media and associated information contained on that media requiring physical protection.
c. "Restricted" and "protected" information stored by EPA personnel and contractors must be physically controlled, and safeguarded in the manner prescribed for the highest classification level of the information contained on the media until the media is sanitized or destroyed.
d. Encrypting information at rest on selected secondary storage devices must be considered.
    i. The employment of cryptography is at the discretion of the IO.
    ii. The selection of cryptographic mechanisms used must be based upon maintaining the confidentiality and integrity of the information.
    iii. The strength of mechanisms must be commensurate with the classification and sensitivity of the information.
e. Information system media must be protected until the media are destroyed or sanitized using approved equipment, techniques, and procedures.
    i. Refer to MP-6 Media Sanitization and Disposal.
f. A secure, environmentally appropriate facility for archiving digital and non-digital media, identified in the General Records Schedule (GRS), must be maintained 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, reel) or other digital and non-digital media containing data that must be maintained but has no immediate processing need.
g. Archived data must be retained for a minimum of two years, but may be retained for up to seven years.
    i. Upon reaching the seven-year timeframe for archived digital and non-digital media, the media is automatically released to the SO for disposition in accordance with record retention schedules related to the information or information system.
h. Annually, information system personnel must test a statistical sample of archived digital media, to ensure that the digital media are in good condition and are readable.

i. NIST SP 800-56 must be used for guidance on cryptographic key establishment.
j. NIST SP 800-57 must be used for guidance on cryptographic key management.
k. NIST SP 800-111 must be used for guidance on storage encryption technologies.

MP-5 – Media Transport

For moderate and high information systems

a. All digital and non-digital media must be protected and controlled during transport outside of controlled areas using defined security measures (i.e., locked container, cryptography).
b. Accountability for information system media must be maintained during transport outside of controlled areas using defined security measures (i.e., locked container, cryptography) that are agency-approved, FIPS 140-2 validated or compliant encryption technologies.
c. Activities associated with transport of information system media must be restricted to authorized personnel.
d. The assessment of risk must guide:
    i. The selection of media and associated information contained on that media requiring protection during transport.
    ii. The selection and use of storage containers for transporting non-digital media outside controlled areas within EPA.
e. Physical and technical security measures for the protection of digital and non-digital media must be approved by the SO, commensurate with the classification or sensitivity of the information residing on the media and consistent with any federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
f. The SO shall document, using defined documentation methods, activities associated with the transport of media containing “protected” or “restricted” information outside controlled areas within EPA.
    i. The logging or tracking requirements for activities associated with the transport of media must be based on the SO’s 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. At a minimum, any log or tracking mechanism must include:
        - Description of information being transported.
        - Type of “protected” or “restricted” information (e.g., PII, CBI) contained on the media.
        - Method(s) of transport.
        - Protection measures employed.
        - Name(s) of individual(s) transporting the information (if appropriate).
        - Authorized recipient(s).
        - Dates sent and received.
g. In instances where it is necessary to remove or transport confidentially sensitive

document(s) or media containing "protected" or "restricted" information outside of controlled areas of EPA, official management approval must be obtained and documented.

i. Management must be satisfied that the organization's requirements for securing confidentially sensitive information are being met.

h. 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:

- An identifying document number, if used.
- Description of the information.
- Name and signature of the sender.
- 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".

- 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.

Note: Refer to the definition of secured means of transport in Section 9 of this document.

i. Media transported by a common carrier must use an acknowledgement of receipt.

j. Personnel transporting "protected" or "restricted" information by car shall store the media in a locked trunk while en route.

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

k. Personnel are prohibited from leaving media containing "protected" or "restricted" information in a vehicle overnight.

l. If media containing "protected" or "restricted" information is being transported and delivered by hand, then it must be given directly to the recipient or another authorized individual.

i. Acknowledgement of receipt must be used.

m. If "protected" or "restricted" information is faxed, both the sending and receiving fax machines must be attended by an authorized individual.

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

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

n. Individuals shall 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.
        - This may require printing out tracking data for delivery confirmation mechanisms.

o. Cryptographic mechanisms must be employed to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
    i. Refer to *Information Security – Interim System and Communications Protection Procedures* for guidance on the use of cryptography.

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).

For high information systems

p. The SO shall employ an identified custodian throughout the transport of information system media.

Note: Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.

MP-6 – Media Sanitization

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

a. All information system media (both digital and non-digital) must be sanitized by using approved equipment, techniques, and procedures prior to disposal, release out of organizational control, or release for reuse.
    i. All electronic information and licensed software must be removed when disposing of computers with hard drives. IT resources and digital storage media must be cleaned of all information.

b. Sanitization mechanisms with the strength and integrity commensurate with the classification or sensitivity of the information must be employed.

c. When handling confidentially sensitive information, EPA offices shall consult the appropriate IT and programmatic-related records management schedules to determine if and when the information should be destroyed.

Note: Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed.

d. Sanitization techniques, including degaussing and overwriting memory locations and physical destruction must ensure that the information on media is not disclosed to unauthorized individuals when such media is reused or released for disposal.
    i. All Agency records must be properly identified, retrieved from the media, if necessary, and processed in accordance with *Records Management Policy*.
    ii. The media and information must not be sanitized, disposed of, or destroyed if they are subject to ongoing e-discovery litigation or other legal requirement.
    iii. Media must be sanitized using approved equipment and techniques.
    iv. When large numbers of media are being sanitized, a representative sample must be tested to ensure proper sanitization.
    v. If sanitization must be performed over a long period of time, samples must be taken and tested at random intervals.
    vi. Verification of samples must be documented such that the media can be identified if necessary.
e. Media sanitization equipment, techniques, and procedures must comply with NIST SP 800-36, *Guide to Selecting Information Technology Security Products*.
f. 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, for additional information.
g. The product selected for sanitizing, destroying, or disposing of media must be part of the National Security Agency's approved list found at http://www.nsa.gov/ia/guidance/media_destruction_guidance/index.shtml.
    i. For sanitizing media:
        - At a minimum, a triple-pass overwrite method must be used, where data is overwritten with, for example, 0's, then 1's, and then with pseudo-random data.
        - Any system containing a hard drive or digital media that has information categorized as high confidentiality must 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.

h. Media destruction and disposal must be:
    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).

For high information systems

i. Media sanitization and disposal actions must be tracked, documented, and verified.

j. A log must be created and retained for all media destroyed.

k. Standard Operating Procedures (SOPs) for media sanitization must be developed.
    i. Users must be trained on these SOPs.

l. The SOP for media sanitization must include steps to document the following information:
    i. Report date.
    ii. Sanitization completion date.
    iii. Media being sanitized (including serial number or other uniquely identifiable characteristic, if applicable).
    iv. Party performing sanitization.
    v. Sanitation method employed.

m. Sanitization equipment and procedures must be tested quarterly to verify correct performance.

n. Portable, removable storage devices (e.g., thumb drives, flash drives, external storage devices) must be sanitized prior to connecting such devices to the information system under the following circumstances: refer to NIST 800-88 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.

o. The sanitization of portable, removable storage devices must be considered 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.

p. An assessment of risk must guide the specific circumstances for employing the sanitization process.

7. RELATED DOCUMENTS

- National Security Agency (NSA)/Central Security Services (CSS) *Evaluated Products List for High Security Crosscut Paper Shredders*, Version AA, 31 March 2010 (Paper Only)
- NSA/CSS *Evaluated Products List for Punched Tape Destruction Devices*, Version C,

29 July 2005 (Punched Tape)

- NSA/CSS *Evaluated Products List for Optical Media Destruction Devices*, Version H, 25 September 2009 (Optical Media)
- NSA/CSS *Evaluated Product List* - Degausser (Magnetic Media Sanitization) 30 March 2009
- NSA/CSS *Storage Device Declassification Manual (SDDM)*, December 2007 (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*, October 2003
- Toxic Substances Control Act (TSCA) *CBI Protection Manual*, 2004
- NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009
- NIST SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, March 2007
- NIST SP 800-56B, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, August 2009
- NIST SP 800-57, *Recommendation for Key Management*, March 2007
- NIST SP 800-60, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008
- NIST SP 800-88, Revision 1, *Guidelines for Media Sanitization*, September 2006
- NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, November 2007

8. ROLES AND RESPONSIBILITIES

System Owner (SO)

a. The SO has the following responsibilities with respect to media protection:

i. Ensure that an assessment of risk guides the selection of media and associated information contained on that media requiring protection and restricted access.

ii. Protect unmarked media at the highest FIPS 199 security category for the information system until the media are reviewed and appropriately marked.

iii. Document the processes required to ensure media and the information on the media of their information system are protected from unauthorized access.

iv. Ensure EPA data can be stored only on approved EPA removable digital media.

v. Physically control and securely store information system media within controlled areas.

vi. Document in policy and procedures the specific measures taken to protect media based on requirements of the information it holds.

vii. Protect information system media until the media are destroyed or sanitized

using approved equipment, techniques, and procedures.

viii. Consider the employment of cryptography to protect information at rest.

ix. Maintain a secure, environmentally appropriate facility for archiving digital and non-digital media.

x. Document in policy and procedures the media requiring protection during transport and the specific measures taken to protect such transported media.

xi. Employ cryptographic mechanisms to protect information stored on digital media during transport outside of controlled areas.

xii. Restrict activities associated with transport of information system media to authorized personnel.

xiii. Base the selection and use of appropriate storage containers for transporting media on the assessed risk.

xiv. Approve physical and technical security measures for protecting non-digital media that are transported.

xv. 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.

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

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

xviii. Prior to sanitization of media, ensure that all Agency records are properly identified, retrieved from the media, and processed in accordance with *Records Management Policy*.

xix. 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.

xx. Track, document, and verify media sanitization and disposal actions.

xxi. Create and retain a log of all media destroyed.

xxii. Develop SOPs for media sanitization.

xxiii. Ensure that users are trained on these SOPs.

xxiv. Ensure that sanitization equipment and procedures for high information systems are tested to verify correct performance.

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

Information System Personnel

a. Information system personnel have the following responsibilities with respect to media protection:

i. Protect unmarked media at the highest FIPS 199 security category for the

information system until the media are reviewed and appropriately labeled.

ii. Mark human-readable output appropriately in accordance with applicable policies and procedures set forth by EPA.

iii. Affix printed output with cover sheets (developed by the applicable system personnel) if the printed output is not otherwise appropriately marked.

iv. Mark digital media and cover sheets with the information designated within these procedures.

v. Follow all marking requirements and guidelines provided by the SO and the records management program for records scheduled for archival.

vi. Follow any and all marking guidelines provided by the SO and the Records Management Program for records scheduled for archival.

vii. Adhere to the procedures in this document when marking documents that contain confidentially sensitive information.

viii. Mark as "protected" portable computers or handheld devices approved for high confidentiality information use, employing distinctive markings that are not visible when the computer is not in use.

ix. Release archived digital media that have reached the seven-year timeframe to the SO for disposal.

x. Annually test a statistical sample to ensure that archived digital media are in good condition and are readable.

xi. Protect and control media during transport outside of controlled areas.

xii. Restrict activities associated with transport of media to authorized personnel.

xiii. Obtain and document management approval to remove or transport media containing "protected" or "restricted" information outside of controlled areas of EPA.

xiv. Follow the requirements documented in these procedures before transporting delivering, or mailing media containing "protected" or "restricted" information.

xv. Sanitize all media prior to disposal, release for reuse, or removal for maintenance activities.

xvi. Use approved equipment, techniques, and procedures for sanitizing and disposing of media; these must be in compliances with NIST SP 800-36, NIST SP 800-88, and the National Security Agency's approved list of products.

xvii. Abide by documented procedures and standards for media sanitization and disposal.

xviii. Test sanitization equipment and procedures for high information systems to verify correct performance.

Users / Individuals

a. Users/individuals have the following responsibilities with respect to media protection:

i. Protect unmarked media at the highest FIPS 199 security category for the information system until the media are reviewed and appropriately labeled.

ii. Mark digital media and cover sheets with the information designated within these procedures.

iii. Adhere to the procedures in this document when marking documents that contain confidentially sensitive information.

iv. Follow the requirements documented in these procedures before transporting delivering, or mailing media containing "protected" or "restricted" information.

v. Protect and control media during transport outside of controlled areas.

vi. Store media containing "protected" or "restricted" information in a locked vehicle trunk while en route; if there is no trunk, hide the media from sight.

vii. Do not leave media containing "protected" or "restricted" information in a vehicle overnight.

viii. Follow the requirements documented in these procedures regarding media containing "protected" or "restricted" information when:

- Using a common carrier for delivery.
- Transporting by car or other vehicle.
- Delivering by hand.
- Faxing.
- Receiving.

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 is physically or procedurally controlled at the facility entrance 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 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 as follows:
    i. Unrestricted:

1. Unrestricted data is accessible to anyone for any reason.

ii. Restricted:

1. Restricted data is not accessible to the general public.
2. Restricted data is accessible to data subjects or data suppliers.
3. Restricted data is accessible only to authorized users.

iii. Protected:

1. Protected data is not accessible to the general public.
2. Protected data 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, 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 the action or decision and

includes a signature. The documentation can be accomplished manually or electronically.

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 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

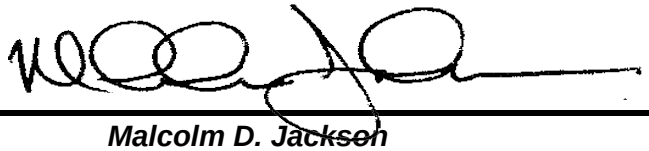
Related standards and guidelines are available on OEI's website.

12. MATERIAL SUPERSEDED

Procedures for Disk Sanitization - http://intranet.epa.gov/otop/policies/DiskSanitization.pdf

13. ADDITIONAL INFORMATION

NA



Malcolm D. Jackson
Assistant Administrator and Chief Information Officer
Office of Environmental Information

APPENDIX A: ACRONYMS

CBI	Confidential Business Information
CD	Compact Disk
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
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
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	MEDIA STORAGE PROTECTED ENVIRONMENT GUIDELINES (SELECTION OF "ACCEPTABLE" OR "OPTIMUM" MAY BE RISK DEPENDENT)		
CONFIDENTIALITY LEVEL / PROTECTION LEVEL	**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"**	NA	No Limits	No Limits

DOCUMENT CHANGE HISTORY

Version	Release Date	Summary of Changes	Author of Changes	DCN
0.7	11/12/2008	Initial draft	Heather Flager	Procedures_MP_Draft_TO62_020_1
2.0	3/26/2009	Incorporated EPA comments, incorporated metrics	Heather Flager	Procedures_MP_Final_TO62_020_2
3.0	4/20/2009	Incorporated EPA comments Final	Heather Flager	Procedures_MP_Final_TO62_020_3
3.8	7/15/2010	Updated per NIST SP 800-53 Rev 3	Heather Flager	Procedures_MP_Draft.TO-062_050_1.0
3.9	12/27/2010	TISS Final Draft Review	Charleen Johnson	Procedures_MP_Draft.TO-062_050_1.0
4.0	5/4/2012	SAISO Final Review	Abe Getchell	Procedures_MP_Draft.TO-062_050_1.0
4.1	7/18/2012	Document Review	LaToya Gordon	Procedures_MP_Draft.TO-062_050_1.0