IT Security Procedural Guide:

Media Protection (MP)

CIO-IT Security-06-32

Revision 5

April 3, 2020

Office of the Chief Information Security Officer

VERSION HISTORY/CHANGE RECORD

Change Number	Person Posting Change	Change	Reason for Change	Page Number of Change
Revision 1 - November 02, 2010				
1	Heard	Changes throughout the document to correspond with updated GSA Policy and procedural requirements	Inclusion of hardcopy references. Policy Reference Updates. Stronger controls for leased copiers. Inclusion of Hardcopy Devices into Sanitization Form.	Various
2	Berlas/ Cook	Changes throughout the document to correspond with update of the current version of GSA CIO P 2100 and NIST 800-53 rev3.	The most current version of GSA CIO P 2100 and more detailed guidance on implementing policy.	Various
Revision 2 - March 15, 2012				
1	Booz Allen Hamilton	Updated/clearly defined the role of System Owner and System Custodian.	Per ISSM Direction	P5, P8, P21, Appendix B
Revision 3 - April 15, 2012				
1	Blanche Heard	Updated/revised with stakeholders comments/audit recommendations	Agency audit process	Various
Revision 4 - May 23, 2016				
1	Sitcharing/ Klemens/ Wilson	Changes made throughout the document to reflect NIST and GSA requirements as a result of the consolidation	Updated to reflect NIST 800-53 Rev4 and GSA requirements.	Various
Revision 5 - April 3, 2020				
1	Feliksa/ Klemens	Updated format and NIST SP 800-53 control parameters, added a section on SCRM, included EO 13800 and NIST Cybersecurity Framework.	Biennial update.	Throughout

Approval

IT Security Procedural Guide: Media Protection (MP), CIO-IT Security-06-32, Revision 5 is hereby approved for distribution.

X

Bo Berlas
GSA Cheif Information Security Officer

Contact: GSA Office of the Chief Information Security Officer (OCISO), Policy and Compliance Division, at ispcompliance@gsa.gov.

Table of Contents

Table of Figures and Tables

1 Introduction

General Services Administration (GSA) information systems capture, process, and store information using a wide variety of media. This information is not only located on the intended storage media but also on devices used to create, process, or transmit this information. These media require special disposition in order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality. The media protection (MP) principles and practices described in this guide are based on guidance from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4*, "Security and Privacy Controls for Federal Information Systems and Organizations*" and NIST SP 800-88, Revision 1, "*Guidelines for Media Sanitization.*"

Every GSA Information Technology (IT) system must follow the MP practices identified in this guide. Any deviations from the security requirements established in GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*" must be coordinated by the Information Systems Security Officer (ISSO) through the appropriate Information Systems Security Manager (ISSM) and authorized by the Authorizing Official (AO). Any deviations, exceptions, or other conditions not following GSA policies and standards must be submitted using the Security Deviation Request Google Form. Deviations must also be documented using the Acceptance of Risk (AoR) process defined in GSA CIO-IT Security-06-30, "*Managing Enterprise Risk"*, including a date of resolution to comply.

Executive Order (EO) 13800, "*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"* requires all agencies to use "*The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology (NIST) or any successor document to manage the agency's cybersecurity risk.*" This NIST document is commonly referred to as the Cybersecurity Framework (CSF).

The CSF focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes. The core of the CSF consists of five concurrent and continuous Functions—Identify (ID), Protect (PR), Detect (DE), Respond (RS), Recover (RC). The CSF complements, and does not replace, an organization's risk management process and cybersecurity program. GSA uses NIST's Risk Management Framework from NIST SP 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach.*" Table 1-1 provides a mapping of the NIST SP 800-53 MP controls to CSF Category Unique Identifiers. The following CSF categories are aligned with NIST's MP controls.

- Identify-Governance (ID.GV)
- Protect-Data Security (PR.DS)
- Protect-Information Protection Processes and Procedures (PR.IP)
- Protect-Protective Technology (PR.PT)

Table 1-1: NIST SP 800-53 Control to CSF Mapping

NIST SP 800-53 Control	CSF Category Unique Identifier Codes
MP-1	ID.GV-1, ID.GV-3
MP-2	PR.PT-2
MP-3	PR.PT-2
MP-4	PR.PT-2
MP-5	PR.PT-2
MP-6	PR.DS-3, PR.IP-6
MP-7	PR.PT-2

1.1 Purpose

The purpose of this guide is to provide guidance for the MP security controls identified in NIST SP 800-53 and media protection requirements specified in CIO 2100.1. This procedural guide provides GSA Federal employees and contractors with significant security responsibilities, as identified in CIO 2100.1, and other IT personnel involved in media protection, sanitization, and disposal the specific procedures and processes they are to follow for GSA information systems under their purview.

1.2 Scope

The requirements outlined within this guide apply to and must be followed by all GSA Federal employees and contractors who are involved in the media protection of GSA information systems and data.

1.3 Policy

CIO 2100.1 Chapter 4, Policy on Operational Controls, states:

k. Media Protection.

(1) All GSA data from information system media, both digital and non-digital, must be sanitized IAW methods described in IT Security Procedural Guide: Media Protection Guide, OCIO-IT Security-06-32, before disposal or transfer outside of GSA.
(2) Restrict access to information system media (e.g., disk drives, diskettes, internal and external hard drives, and portable devices), including backup media, removable media, and media containing sensitive information to authorized individuals.
(3) Physically control and securely store information system media within controlled areas.
(4) Protect digital media during transport outside of controlled areas using a certified FIPS 140-2 encryption module; non-digital media shall follow GSA personnel security procedures.

1.4 References

Note: GSA updates its IT security policies and procedural guides on independent biennial cycles which may introduce conflicting guidance until revised guides are developed. In addition, many of the references listed are updated by external organizations which can lead to inconsistencies with GSA policies and guides. When conflicts or inconsistencies are noticed, please contact ispcompliance@gsa.gov for guidance.

Federal Laws and Regulations:

- EO 13800, "*Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*"

Federal Guidance:

- CSF, Version 1.1, "*Framework for Improving Critical Infrastructure Cybersecurity*"
- Federal Information Processing Standards (FIPS) Publication (PUB) 140-2, "*Security Requirements for Cryptographic Modules*"
- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- NIST SP 800-37, Revision 1, "*Guide for Applying the Risk Management Framework to Federal Information Systems*"
- NIST SP 800-53, Revision 4, "*Security and Privacy Controls for Federal Information Systems and Organizations*"
- NIST SP 800-88, Revision 1, "*Guidelines for Media Sanitization*"
- NIST SP 800-161, "*Supply Chain Risk Management Practices for Federal Information Systems and Organizations*"

GSA Guidance:

- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*"
- GSA Order OAS 1820.1, "*GSA Records Management Program*"
- GSA Order CIO 3490.2, "*Document Security for Sensitive But Unclassified Building Information*"

The guidance documents below are available on the GSA IT Security Procedural Guides InSite page.

- CIO-IT Security-01-02, "*Incident Response (IR)*"
- CIO-IT Security-06-30, "*Managing Enterprise Risk*"
- CIO-IT Security-07-38, "*Hardcopy Device Security*"
- CIO-IT Security-09-48, "*Security and Privacy Requirements for IT Acquisition Efforts*"
- CIO-IT Security-18-90, "*Information Security Program Plan*"

2 Roles and Responsibilities

There are many roles associated with implementing effective media protection policies and procedures. The roles and responsibilities provided in this section have been extracted or paraphrased from CIO 2100.1 or summarized from GSA and Federal guidance. The responsibilities listed in this guide are focused on media protection, a complete set of GSA security roles and responsibilities can be found in CIO 2100.1. Throughout this guide, specific processes and procedures for implementing NIST's MP controls are described.

2.1 Authorizing Official (AO)

Responsibilities include the following:

- Ensuring IT systems under their purview meet the security requirements of IT information security laws and regulations, including compliance with NIST SP 800-53 media protection controls.
- Providing support to the ISSM and ISSO of record for each information system under their purview.

2.2 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Verifying systems under their purview have appropriately addressed NIST SP 800-53 media protection controls.
- Coordinating with the AO, System Owner, ISSOs, and OCISO Directors, as necessary, regarding security control compliance and data and system security.

2.3 Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Ensuring the system is operated, used, maintained, and disposed of in accordance with documented security policies and procedures.
- Ensuring media protection procedures are followed.

2.4 System Owners

Responsibilities include the following:

- Ensuring their systems and the data each system processes has necessary NIST SP 800-53 MP security controls in place and operating as intended.
- Coordinating with IT security personnel including the ISSM and ISSO and Data Owners to ensure implementation of system and data security requirements.
- Coordinating with Data Owners and Custodians to ensure system media is properly stored, maintained, and protected.
- Ensuring system media is properly marked, transported, and sanitized when required.

2.5 Data Owners

Responsibilities include the following:

- Coordinating with System Owners and Custodians to ensure the data each system processes has necessary NIST SP 800-53 MP security controls in place and operating as intended.
- Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of system and data security requirements.
- Coordinating with System Owners and Custodians to ensure system media is properly stored, maintained, and protected.
- Ensuring system media is properly marked, transported, and sanitized when required.

2.6 Contracting Officers (CO)/Contracting Officers Representative (COR)

Responsibilities include the following:

- Ensuring that all IT acquisitions include the appropriate security requirements in each contract and task order.
- Coordinating with the CISO or other appropriate official as required to ensure that all agency contracts and procurements are compliant with the agency's information security policy.
- Ensuring new solicitations for all GSA IT systems includes the security contract language from CIO-IT Security-09-48, "*Security and Privacy Requirements for IT Acquisition Efforts.*"

2.7 Custodians

Responsibilities include the following:

- Coordinating with Data Owners and System Owners to ensure system media is properly stored, maintained, and protected.
- Ensuring system media is properly marked, transported, and sanitized when required.

2.8 Authorized Users of IT Resources

Responsibilities include the following:

- Ensuring PII and/or sensitive data stored on any workstations or mobile devices including, but not limited to, laptop computers, notebook computers, external hard drives, USB drives, CD-ROMs/DVDs, and personal digital assistants is encrypted with GSA provided encryption.
- Ensuring any media used as part of their duties is protected IAW the NIST SP 800-53 media protection controls and the procedures in this guide.

2.9 System/Network Administrators

System/Network administrators are responsible for:

- Ensuring any media used as part of their duties is protected IAW the NIST SP 800-53 media protection controls and the procedures in this guide.
- Working with Custodians, Data Owners, and System Owners to ensure Ensuring system media is properly marked, transported, and sanitized when required.

3 Media Protection Overview

Media protection involves three key elements:

- Protection of digital and hardcopy information;
- Controlling access to information system media to authorized users; and
- Ensuring information system media is sanitized prior to disposal or reuse.

Information stored on digital or hardcopy media must be physically protected within controlled areas. In terms of media access, organizations must ensure that access to media is restricted to authorized individuals and that media is properly marked as per the latest GSA policy detailed in Section 4.3. Any media containing PII must be encrypted using a FIPS 140-2, "*Security Requirements for Cryptographic Modules*" certified encryption module. Media that is transported outside of controlled areas must be protected in accordance with the most current GSA guidelines defined in Section 4.5. Sanitization refers to the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and/or reconstructed. Equipment that is transferred, becomes obsolete, or are no longer usable or required by an information system must be sanitized based on the FIPS 199 Security Categorization of the system. Improper sanitization techniques may leave residual data on storage media that could allow unauthorized individuals to reconstruct data and thereby gain access to sensitive agency information. Hardcopy devices such as fax and copier machines must also be sanitized prior to being removed from GSA facilities IAW CIO-IT Security-07-38, "*Hardcopy Device Security.*"

3.1 Sanitization Methods

FIPS 199 system security categorization along with a number of other factors, drive decisions on how to deal with media sanitization. Other factors defined by NIST SP 800-88 include:

- What types (e.g., optical non-rewritable, magnetic) and size (e.g., megabyte, gigabyte, and terabyte) of media storage does the organization require to be sanitized?
- What is the confidentiality requirement for the data stored on the media?
- Will the media be processed in a controlled area?
- Should the sanitization process be conducted within the organization or outsourced?
- What is the anticipated volume of media to be sanitized by type of media?
- What is the availability of sanitization equipment and tools?
- What is the level of training of personnel with sanitization equipment/tools?

- How long will sanitization take?
- What is the cost of sanitization when considering tools, training, verification, and reentering media into the supply stream?

There are different types of sanitization for each type of media. NIST has divided media sanitization into three categories: clear, purge, and destroy. Table 3-1 (Table 5-1 in NIST SP 800-88) below presents the different methods that can be used to sanitize media.

Table 3-1: Sanitization Methods

Type	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite user addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user addressable locations. The security goal of the overwriting process is to replace Target Data with non-sensitive data. Overwriting cannot be used for media that are damaged or not rewriteable, and may not address all areas of the device where sensitive data may be retained. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear levelling, making it infeasible for a user to sanitize all previous data using this approach because the device may not support directly addressing all areas where sensitive data has been stored using the native read and write interface. The Clear operation may vary contextually for media other than dedicated storage devices, where the device (such as a basic cell phone or a piece of office equipment) only provides the ability to return the device to factory state (typically by simply deleting the file pointers) and does not directly support the ability to rewrite or apply media-specific techniques to the non-volatile storage contents. Where rewriting is not supported, manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device and associated media. These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared data.
Purge	Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands. Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures (such as using a firearm to shoot a hole through a storage device) may only damage the media as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques. Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity. Coercivity may be difficult to determine based only on information provided on the label. Therefore, refer to the device manufacturer for coercivity details. Degaussing should never be solely relied upon for flash memory-based storage devices or for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique).

Type	Description
Destroy	There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques. • Disintegrate, Pulverize, Melt, and Incinerate. These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal Destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. • Shred. Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. To make reconstructing the data even more difficult, the shredded material can be mixed with non-sensitive material of the same type (e.g., shredded paper or shredded flexible media). The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the verification of Clear or Purge methods fails (for known or unknown reasons).

3.2 Five Step Media Sanitization Process

The GSA media sanitization process is based on the NIST Sanitization and Disposition Decision Flow and the Minimum Sanitization Recommendations contained in NIST SP 800-88. This guide describes key steps in media sanitization. It is designed to assist agency personnel with security responsibilities in implementing the process. The steps and corresponding diagram outline this process.

3.2.1 Step 1 - Sanitization and Disposition Decision

Refer to Figure 3-1, the Sanitization and Disposition Decision Flow (NIST SP 800-88, Figure 4-1), to select the appropriate sanitization method and disposition for media. The decision process is based on the confidentiality (FIPS 199 categorization) of the information, whether the media will be reused, and whether it will leave GSA control.

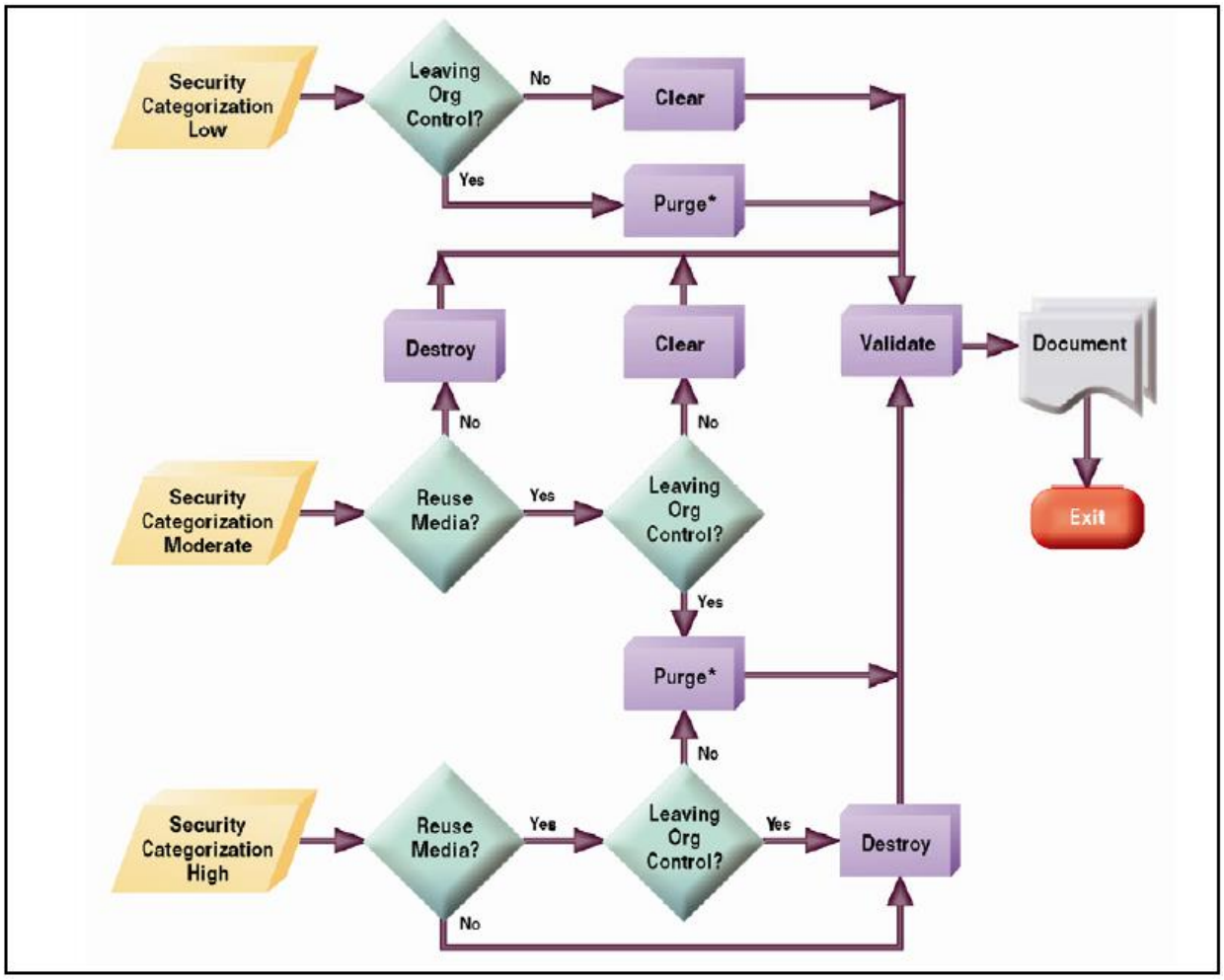

Figure 3-1: Sanitization and Disposition Decision Flow

3.2.2 Step 2 – NIST Sanitization Recommendations for Media Containing Data

Upon selection of a sanitization method (Clear, Purge, Destroy) using the decision flow in Step 1 and factoring relevant organizational environmental factors (if any), refer to NIST SP 800-88, Appendix A to determine the recommended sanitization technique for specific media.

3.2.3 Step 3 – Sanitize Media

Sanitization is intended to permanently delete data, ensure recovery of the data is not required before initiating sanitization. Upon determining sanitization is appropriate, implement the latest sanitization recommendations from Step 2, using tools and resources identified in NIST SP 800-88, Appendix C. In general, NIST recommends using tools from the following resources.

- National Security Agency (NSA) Media Destruction Guidance. Tools at this site can be used for logical and physical sanitization and destruction of paper, media, and devices.
- Open Source Tools. There are a variety of open source tools available that support leveraging sanitization commands based on standardized interfaces. Carnegie Mellon

University (CMU) has a listing of open source (and commercial) data sanitization and disposal tools; CMU data sanitization website.

- Outsourcing Media Sanitization and Destruction. Outsourcing media sanitization and destruction may be used if the Service/Staff Office and ISSM/ISSO decide this would be the most reasonable option to maintain confidentiality while optimizing available resources.

Any tool the System Owner and/or Data Owner proposes for use in the sanitization of media, commercial or open source, must be approved by the AO, ISSM, and ISSO prior to use. The OCISO Information Security Engineering (ISE) Division will provide assistance, as needed.

If outsourcing of sanitization or destruction is chosen for use, "*due diligence*" must be used before issuing a contract. NIST SP 800-88, Appendix C.4, states:

> *Due diligence for this case is accepted as outlined in 16 CFR 682 which states "due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule [guide], obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.*

3.2.4 Step 4 – Sanitization Verification

The end result of the sanitization must be verified following the use of the chosen sanitization tool. Verification includes validating the proper functioning of any equipment used, the competency of people or organizations performing sanitization, and verifying the sanitization completed successfully by examining the media, where feasible. NIST SP 800-88, Section 4.7, describes verification methods. If assistance is needed on how to conduct sanitization verification, contact your ISSO/ISSM for assistance.

3.2.5 Step 5 – Document Media Sanitization Activity

Upon completion of sanitization activities, it is important to document and validate what occurred. The responsibility for this documentation rests with the System Owner, Data Owner, and Custodian. The System Owner is responsible for maintaining the documentation to record that the system's media was properly sanitized.

A GSA Sanitization Information Form is available on the IT Security Forms InSite page. While it is recommended this form be used for sanitization tracking purposes, other means of documenting the sanitization process (e.g., IT Service Desk ticket, sanitization log) are acceptable as long as they provide the following information:

- Organization
- System Name

- Item Make/Model
- Item Serial Number(s)
- Item Disposition (Clear, Purge, Destroy)
- Date Conducted
- Conducted By
- Validated By
- Final Disposition of Media (Disposed, Reused Internally, Reused Externally, Returned to Manufacturer).

The completed document should be maintained by the System Owner for record keeping purposes and proof of proper sanitization.

Records covered by the Privacy Act are considered sensitive and offices must certify that they have been properly destroyed. Per GSA Order 1820.1, large-scale destruction of records, regardless of media, such as those requiring assistance of outside companies, should not be done without the knowledge and sign-off by the appropriate GSA Records Management Coordinator. If an employee or contractor knows of any actual or potential threat to records (e.g., unlawful removal, alteration, or destruction), follow the instructions below which have been extracted from CIO-IT Security-01-02, "*Incident Response (IR)*."

> *Confirmed and/or suspected incidents involving the potential loss or compromise of PII in electronic or physical form must be reported IMMEDIATELY to the OCISO via the GSA IT Service Desk. The OCISO will determine when it is appropriate to report incidents to the GSA SAOP. The OCISO will also determine external reporting to the US-CERT, OIG, and U.S. Congress. Reporting will be completed IAW this guide and the US-CERT Federal Incident Notification Guidelines.*

4 Implementation Guidance for MP Controls

The GSA-defined parameter settings included in the control requirements are offset by brackets in the control text. As stated in Section 1.2, Scope, the requirements in this guide apply to GSA Federal employees and contractors who are involved in the media protection of GSA information systems and data. The GSA implementation guidance stated for each control applies to personnel and/or the systems operated on behalf of GSA. Any additional instructions/requirements for contractor systems will be included in the "Additional Contractor System Considerations" portion of each control section.

MP-1, Media Protection Policy and Procedures, has been identified as a Common Control for all GSA/internally operated systems and as a Hybrid Control for contractor systems. The MP-2 to MP-7 controls, when included in a system's control set, either are provided as a Common Control by a Major Information System, a system specific control by the system, or as a Hybrid Control with shared responsibilities for control implementation. CIO-IT Security-18-90, "*Information Security Program Plan*" describes the GSA enterprise-wide inheritable common and hybrid controls and outlines the responsible party for implementing each of them.

4.1 MP-1 Media Protection Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to [*Information System Security Managers, Information System Security Officers, System Owners, Program Managers, Project Managers, Acquisitions/Contracting Officers, Custodians*]:
    1. A media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
    2. Procedures to facilitate the implementation of the media protection policy and associated media protection controls; and
b. Reviews and updates the current:
    1. Media protection policy [*biennially*]; and
    2. Media protection procedures [*biennially*].

GSA Implementation Guidance: Control MP-1 is applicable at all FIPS 199 levels.

Media protection policy and procedures is a common control provided by the GSA OCISO Policy and Compliance Division (ISP). Media protection policy is included in GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*." The policy states, "*All GSA data from information system media, both digital and non-digital, must be sanitized IAW methods described in GSA CIO-IT Security-06-32: Media Protection before disposal or transfer outside of GSA.*"

Agency-wide media protection procedures are provided in this guide. GSA's security policy and procedural guides are disseminated via the IT Security webpage. GSA Order CIO 2100.1 and GSA IT Security Procedural Guide 01-05 are reviewed and updated at least biennially.

Additional Contractor System Considerations:

Vendors/contractors may defer to the GSA policy and guide or implement their own media protection policies and procedures which comply with GSA's requirements with the approval of the AO.

4.2 MP-2 Media Access

Control: The organization restricts access to [*S/SO or Contractor recommended and AO approved types of digital and/or non-digital media*] to [*S/SO or Contractor recommended and AO approved personnel or roles*].

GSA Implementation Guidance: Control MP-2 is applicable at all FIPS 199 levels.

Access to digital and non-digital media associated with the information system must be restricted to authorized individuals only. Consideration must be given to the type of information (e.g., medical data, design/engineering data, proprietary, contract) as well as the media type (hard copy, electronic, etc.) when determining the personnel who require access by

their position or role in the organization or system. The concept of least privilege must be used to ensure only personnel with a business 'need-to-know' are allowed access to media.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above and the AO must approve contractor recommended parameters.*

4.3 MP-3 Media Marking

Control: The organization:

a. Marks information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempts [*no media (i.e., all media must be marked)*] from marking as long as the media remain within [*all environments, including controlled areas*].

GSA Implementation Guidance: Control MP-3 is applicable at the FIPS 199 Moderate and High levels.

All FIPS 199 Moderate and High systems must mark all media associated with the information system. GSA policy does not exempt any form of media and requires marking in all environments, including controlled areas. Media includes all types of disks, tapes, internal/external hard drives, flash/thumb drives, and hard copy output.

GSA Order CIO 2103.1, "*Controlled Unclassified Information (CUI) Policy*" and GSA Order CIO 3490.2, "*Document Security for Sensitive But Unclassified Building Information*" require all media containing Controlled Unclassified Information (CUI) to be marked.

Media marking is required to visually identify media that may require special handling or storage instructions per data sensitivity, as well as to ensure information such as serial or control numbers on backup tapes is physically affixed to the media to support logging and retrieval of backups.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.4 MP-4 Media Storage

Control: The organization:

a. Physically controls and securely stores [*digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, and disks of any type and non-digital media*] within [*locked cabinets or safes in secure/controlled facilities within the authorization boundary*]; and
b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

GSA Implementation Guidance: Control MP-4 is applicable at the FIPS 199 Moderate and High levels.

FIPS 199 Moderate and High systems must ensure all digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, disks of any type, and non-digital media shall be securely stored in locked cabinets or safes in secure/controlled facilities within the authorization boundary. Control must also be maintained when not locked up, for example tracking media through check-out and check-in procedures to maintain accountability. These protections must be maintained until the media is sanitized or destroyed.

Note: Encryption requirements for data residing on media is addressed under control MP-5 when transporting media. GSA's basic requirement for encrypting data at rest (NIST control SC-28(1)) is to use FIPS 140-2 validated encryption modules/mechanisms to encrypt PII, PCI, and business sensitive data.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.5 MP-5 Media Transport

Control: The organization:

a. Protects and controls [*digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, and disks of any type*] during transport outside of controlled areas using [*a FIPS 140-2 validated encryption module/mechanism*];
b. Maintains accountability for information system media during transport outside of controlled areas;
c. Documents activities associated with the transport of information system media; and
d. Restricts the activities associated with the transport of information system media to authorized personnel.

Control Enhancements:

(4) Media Transport | Cryptographic Protection. The information system implements cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

GSA Implementation Guidance: Control MP-5 and enhancement MP-5(4) are applicable at the FIPS 199 Moderate and High levels.

FIPS 199 Moderate and High systems must ensure all transported digital and non-digital media is protected against unauthorized access and modification during transport outside of any controlled area. Digital media that is transported outside of controlled areas must be encrypted using a validated FIPS 140-2 encryption module/mechanism; non-digital media including but not limited to hard copy output, micro films, etc., must be secured using the same policies and procedures as paper documents as prescribed by the Office of Administrative Services policies.

Media that is transported outside of controlled areas must ensure accountability. This can be accomplished using GSA's evidentiary Chain of Custody Record template found on the IT Security Forms page. When used for media protection purposes only, Case Name and Case Number may be left blank on the form.

For enhancement MP-5(4), FIPS 199 Moderate and High systems must ensure agency data that resides on mobile/portable devices (e.g., USB flash drives, external hard drives, and SD cards) is encrypted using a FIPS 140-2 validated encryption module. All data residing on GSA furnished laptop computing devices must be protected with GSA approved encryption.

If it is a business requirement to store PII in digital form, the requirement pertains (i.e., encrypted using a FIPS 140-2 validated encryption module). An employee or contractor shall not physically take out PII from GSA facilities (including GSA managed programs housed at contractor facilities under contract), or access remotely (i.e., from locations other than GSA facilities), without written permission from the employee's supervisor, the data owner, and the IT system authorizing official. Approvals shall be filed with the employee's supervisor. This applies to electronic media (e.g. laptops, USB drives), paper, and any other media (e.g., tapes, disks) that may contain PII. COOP contact lists kept on an electronic device that is password protected (Government approved Smart Phone devices, laptop, USB drive) do not require written permission or encryption.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.6 MP-6 Media Sanitization

Control: The organization:

a. Sanitizes [*all information system media, both digital and non-digital,*] prior to disposal, release out of organizational control, or release for reuse using [*S/SO or Contractor recommended and AO approved sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and
b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Control Enhancements:

(1) Media Sanitization | Review / Approve / Track / Document / Verify. The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.
(2) Media Sanitization | Equipment Testing. The organization tests sanitization equipment and procedures [*annually*] to verify that the intended sanitization is being achieved.
(3) Media Sanitization | Nondestructive Techniques. The organization applies nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the information system under the following circumstances: [(1) P*ositive chain of custody for a device is lost. (2) First purchase from manufacturer/vendor*].

GSA Implementation Guidance: Control MP-6 is applicable at all FIPS 199 levels. Enhancements MP-6(1), MP-6(2), and MP-6(3) are applicable at the FIPS 199 High level.

The focus of this control is to ensure that both digital and non-digital media are sanitized prior to release for disposal, reuse, or release from organizational control. GSA's media sanitization process/procedures are documented in Section 3.2, Five Step Media Sanitization Process, specifics steps are dependent upon the type of media, type of data, and tools used.

For MP-6 enhancements (1) and (2), FIPS 199 High impact systems must ensure media sanitization activities are tracked, documented and verified upon completion, and that any sanitization equipment used is tested annually to ensure they are performing as required.

For MP-6 enhancement (3), FIPS 199 High impact systems must also ensure all portable storage devices are sanitized whenever a positive chain of custody for the device is lost and when a device is first purchased from a manufacturer/vendor.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

4.7 MP-7 Media Use

Control: The organization [*restricts*] the use of [*digital storage devices, including backup media, removable media, and mobile devices*] on [*GSA information systems*] using [*S/SO recommended and AO approved security safeguards*].

Control Enhancements:

(1) Media Use | Prohibit Use Without Owner. The organization prohibits the use of portable storage devices in organizational information systems when such devices have no identifiable owner.

GSA Implementation Guidance: Control MP-7 is applicable at all FIPS 199 levels. Enhancement MP-7(1) is applicable at the FIPS 199 Moderate and High levels.

All FIPS 199 systems shall only use device(s) provided by GSA or provided by organizations approved by GSA. The use of unapproved digital storage devices, including backup media, removable media, and mobile devices on GSA information systems is prohibited.

For enhancement MP-7(1), FIPS 199 Moderate and High systems shall prohibit the use of portable storage devices when such devices have no identifiable owner.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

5 Media Protection and Supply Chain Risk Management

NIST SP 800-161 recommends Information and Communication Technology (ICT) Supply Chain Risk Management (SCRM) practices be used for FIPS 199 High systems. ICT SCRM processes increase the costs, both financial and time expended in supporting them, not just for GSA, but also for system integrators, suppliers, and service providers. ICT SCRM should be considered in the context of the system's missions, operational environments, and risks. Due to the increased costs involved in incorporating SCRM in media protection processes the System Owner, IST Division Director, ISSM, and ISSO must carefully consider these costs prior to incorporating system specific SCRM processes involving media protection. Any questions regarding SCRM should be sent to ispcompliance@gsa.gov.

NIST SP 800-161 states: "*Media itself can be a component traversing the ICT supply chain or containing information about the organization's ICT supply chain. This includes both physical and logical media including, for example, system documentation on paper or in electronic files, shipping and delivery documentation with acquirer information, memory sticks with software code, or complete routers or servers that include permanent media. The information contained on the media may be sensitive or proprietary information. Additionally, the media is used throughout the SDLC, from concept to disposal. Organizations should ensure that the Media Protection controls are applied to both an organization's media and the media received from system integrators, suppliers, and external service providers throughout the SDLC.*"

The MP controls addressed in NIST SP 800-161, limited to those controls for FIPS 199 High systems, are provided in the following sections along with NIST SP 800-161 supplemental guidance on the controls and GSA's implementation guidance.

5.1 MP-1 Media Protection Policy and Procedures (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: A number of documents and information on a variety of physical and electronic media is disseminated throughout the ICT supply chain. This information may contain a variety of sensitive information and intellectual property from the acquirer, system integrator, supplier, and external service provider and should be appropriately protected. Media protection policies and procedures should address ICT supply chain concerns including media in the organization's ICT supply chain infrastructure.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must adequately address media risks associated with the ICT supply chain infrastructure. Protection commensurate with these risks must be implemented. For example, contract clauses may be used to require media to be sanitized and the sanitization verified when media traverses the supply chain, especially when the media will be leaving GSA control or a vendor's control supporting a GSA system.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

5.2 MP-5 Media Transport (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: The organization should consider ICT supply chain risks when transporting media, either by organizational or non-organizational personnel or organizations. Some of the techniques to protect media during transport and storage include cryptographic techniques and approved custodian services.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must adequately address transport risks of media associated with the ICT supply chain. The requirements established for MP-5 for transport and MP-4 for storage of media apply when media with GSA data from GSA systems enters the supply chain.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

5.3 MP-6 Media Sanitization (ICT SCRM)

NIST SP 800-161 Supplemental ICT SCRM Guidance: Media is used throughout the SDLC. Media traversing or residing in the ICT supply chain may originate anywhere including from system integrators, suppliers, and external service providers. It can be new, refurbished, or reused. Media sanitization is critical to ensure that information is removed before the media is used, reused or discarded. NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, control enhancements MP-6 (1), (2), (3), (7), and (8) provide mechanisms for performing media sanitization.

GSA Implementation Guidance: FIPS 199 High systems that have incorporated SCRM must adequately address media sanitization risks associated with the ICT supply chain. The media sanitization requirements and activities established for MP-6 must be followed before media from GSA systems is released into the supply chain for reuse or is discarded.

Additional Contractor System Considerations: *No additional considerations, however vendor/contractor systems must comply with the control IAW the guidance above.*

6 Summary

GSA contractors and Federal employees should use this guide and the noted references to facilitate implementation of media protection requirements. Where there is a conflict between NIST guidance and GSA guidance, contact the OCISO ISP Division at ispcompliance@gsa.gov.