IT Security Procedural Guide: Media Protection (MP) CIO-IT Security-06-32

Revision 6

November 18, 2021

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- June 6, 2018		
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
		Revision 6 - November 18, 2021		
1	Dean/ Klemens	Revisions included: • Updated to NIST SP 800-53, Revision 5 controls • Updated format.	Align to current NIST guidance and GSA parameters.	Throughout

Approval

IT Security Procedural Guide: Media Protection (MP), CIO-IT Security 06-32, Revision 6, is hereby approved for distribution.

DocuSigned by:
Bo Berlas
FD717926161544F...

Bo Berlas
GSA Chief Information Security Officer

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

Table of Contents

List of Figures and Tables

Notes:

- Hyperlinks in running text will be provided if they link to a location within this document (i.e., a different section or an appendix). Hyperlinks will be provided for external sources unless the hyperlink is to a web page or document listed in Section 1.4.
- It may be necessary to copy and paste hyperlinks in this document (Right-Click, Select Copy Hyperlink) directly into a web browser rather than using Ctrl-Click to access them within the document.

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 to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality. The principles and practices for protecting media described in this guide are based on guidance from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 5*, "Security and Privacy Controls for Information Systems and Organizations*" and NIST SP 800-88, Revision 1, "*Guidelines for Media Sanitization.*"

Every GSA information system must follow the media protection 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.

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 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), and 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 (RMF) from NIST SP 800-37, Revision 2, "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy."* Table 1-1, CSF Categories/Subcategories and the NIST MP control family lists the Categories and Subcategories from the CSF that are supported by the implementation of policies, procedures, and processes from the NIST SP 800-53 MP control family. Throughout the remainder of this guide the identifier MP will be used when referring to NIST controls or the control family, otherwise media protection will be used. CIO 2100.1 and this procedural guide provide GSA's policies and procedural guidance regarding protecting media for GSA information systems and implementation of the MP controls.

Table 1-1: CSF Categories/Subcategories and the MP Control Family

CSF Category/Subcategory Identifier	Definition/Description
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated. *(CIO 2100.1 and Sections 1.3 and 3.1 of this guide)* **ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners. *(CIO 2100.1 and Section 2 of this guide)*
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-6:** Data is destroyed according to policy
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-2:** Removable media is protected and its use restricted according to policy

1.1 Purpose

The purpose of this guide is to provide guidance for the NIST SP 800-53 MP controls 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 and media 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. All GSA information systems must adhere to the requirements and guidance

provided with regards to the procedures, processes, and methods for protecting media as described in this guide. Per CIO 2100.1, a GSA information system is an information system:

- used or operated by GSA; or
- used or operated on behalf of GSA by a contractor of GSA or by another organization.

1.3 Policy

CIO 2100.1 contains the following policy statements regarding media protection.

Chapter 4, Policy for Protect Function

3. Data security.

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

4. Information protection processes and procedures.

n. 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 before disposal or transfer outside of GSA.

6. Protective technologies.

d. 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.
e. 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.
f. Users must secure portable storage devices and removable media using the same policies and procedures as paper documents as prescribed by OHRM policies.
g. Users must protect portable storage devices and removable media in the same manner as a valuable personal item and should not leave them unattended in public places, automobiles, etc.

1.4 References

Federal Laws, Standards, Regulations, and Publications:

- EO 13800, *"Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure"*
- FIPS PUB 140-3, "*Security Requirements for Cryptographic Modules"*[1]

[1] NIST has issued FIPS 140-3, FIPS 140-2 modules are still being validated and will be accepted through September 22, 2026. For additional information see the NIST cryptographic module validation program web page.

- FIPS PUB 199, "*Standards for Security Categorization of Federal Information and Information Systems*"
- GRS 3.1 General Technology Management Records, National Archives and Records Administration (NARA)
- NIST CSF, "*Framework for Improving Critical Infrastructure Cybersecurity*"
- NIST SP 800-37, Revision 2, "*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"*
- NIST SP 800-53, Revision 5, "*Security and Privacy Controls for Information Systems and Organizations*"
- NIST SP 800-88, Revision 1, "*Guidelines for Media Sanitization*"

GSA Policies, Procedures, Guidance:

- GSA Order CIO 1820.2, "*GSA Records Management Program*"
- GSA Order CIO 2100.1, "*GSA Information Technology (IT) Security Policy*"
- GSA Order CIO 2103.2,"*Controlled Unclassified Information (CUI) Policy*"
- GSA Order PBS 3490.3, "*Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property*"

The GSA CIO-IT Security Procedural Guides listed below are available on the IT Security Procedural Guides page.

- CIO-IT Security-01-02, "*Incident Response (IR)*"
- CIO-IT Security-06-30, "*Managing Enterprise Cybersecurity Risk*"
- CIO-IT Security-09-44, "*Plans of Action & Milestones (POA&M)*"
- 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, Chapter 2. Throughout this guide, specific processes, and procedures for implementing NIST's MP controls are described.

2.1 Chief Information Security Officer (CISO)

Responsibilities include the following:

- Implementing and overseeing GSA's IT Security Program by developing and publishing security policies and IT security procedural guides that are consistent with the policy.
- Manage the development, documentation, and dissemination of the maintenance policy and procedures with regard to MP controls.
- Ensuring IT Acquisitions align with GSA information security requirements.

- Providing guidance, advice, and assistance to all S/SO/R on IT security issues, the IT Security Program, and security policies.

2.2 Authorizing Official (AO)

Responsibilities include the following:

- Ensuring that GSA information systems under their purview have implemented the required MP controls in accordance with GSA and Federal policies and requirements.
- Identifying the level of acceptable risk for an information system and determining whether an acceptable level of risk has been obtained, including risks associated with MP controls.
- Ensuring all information systems, applications, or sets of common controls under their purview have a current authorization to Operate (ATO) issued per GSA CIO-IT Security-06-30.
- Ensuring a plan of action and milestones (POA&M) entry is developed and managed to address any MP controls that are not fully implemented.

2.3 Information Systems Security Manager (ISSM)

Responsibilities include the following:

- Assisting ISSOs, as necessary, to ensure MP controls are in place and operating as intended.
- Verifying systems under their purview have appropriately addressed MP controls.
- Coordinating with the AO, System Owner, ISSOs, and OCISO Directors, as necessary, regarding MP control implementation and compliance with NIST and GSA requirements.
- Working with the ISSO and System Owner to develop and manage POA&Ms regarding MP controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.

2.4 Information Systems Security Officer (ISSO)

Responsibilities include the following:

- Ensuring necessary MP controls are in place and operating as intended.
- Coordinating with ISSMs and System Owners, as necessary, regarding MP control implementation and compliance with NIST and GSA requirements.
- Working with the System Owner and ISSM to develop and manage POA&Ms regarding MP controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.

2.5 System Owners

Responsibilities include the following:

- Ensuring necessary MP security controls are in place and operating as intended.

- Coordinating with ISSOs and ISSMs, as necessary, regarding MP control implementation and compliance with NIST and GSA requirements.
- Working with ISSOs and ISSMs to develop and manage POA&Ms regarding MP controls that are not fully implemented for their respective systems per GSA CIO-IT Security-09-44.
- Ensuring records of media sanitization performed in support of MP controls are documented and retained in accordance with GSA and Federal guidance.
- Obtaining the resources necessary to securely implement and manage NIST SP 800-53 MP controls for their respective systems.

2.6 Data Owners

Responsibilities include the following:

- Coordinating with System Owners, ISSMs, ISSOs, and Custodians to ensure media containing data is properly stored, maintained, and protected per GSA policies, regulations and any additional guidelines established by GSA.
- Coordinating with IT security personnel including the ISSM and ISSO and System Owners to ensure implementation of MP controls in compliance with NIST and GSA requirements.
- Ensuring system media is properly marked, transported, and sanitized per MP controls and GSA requirements.

2.7 Custodians

Responsibilities include the following:

- Coordinating with ISSMs, ISSOs, and System Owners to ensure the protection of media in support of MP controls is performed as described in the guide.
- Ensuring records of media sanitization performed in support of MP controls are documented and retained in accordance with GSA and Federal guidance.

2.8 Authorized Users of IT Resources

Responsibilities include the following:

- Ensuring PII/CUI 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 deices is encrypted with GSA provided encryption.
- Ensuring any media used as part of their duties is protected per the MP 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 per the MP controls and the procedures in this guide.
- Working with Custodians, Data Owners, and System Owners to ensure system media is properly marked, transported, and sanitized per MP controls and GSA and Federal requirements.

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 140-3[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 is 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.

3.1 Sanitization Methods

FIPS 199 system security categorization along with several 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?

[2] Ibid, 3.

- 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) 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 (Figure 3-1), 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 regarding media sanitization to understand and implement 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.

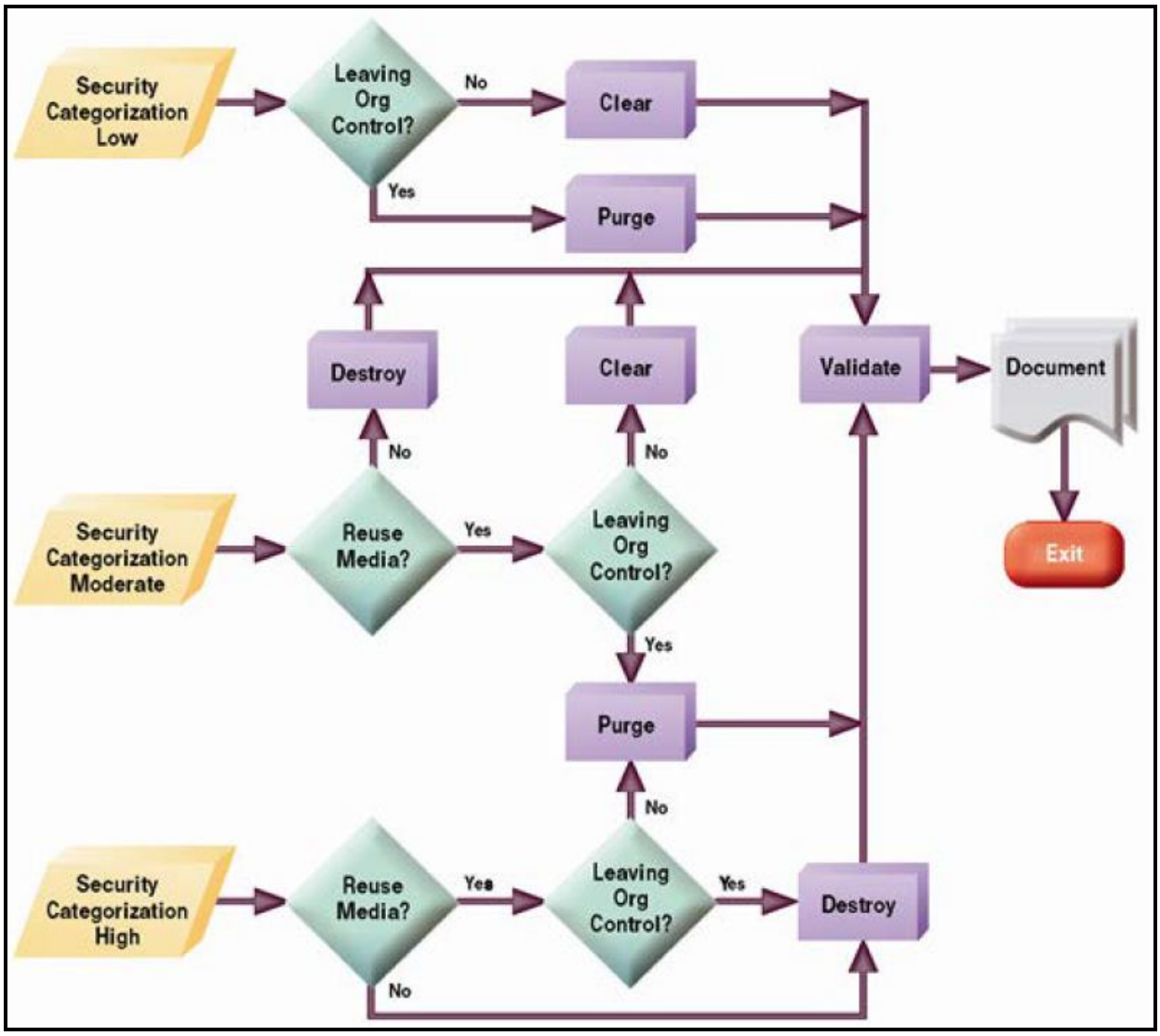

Figure 3-1: Sanitization and Disposition Decision Flow

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 assist, 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 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.

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 Sanitization Information Form is available on the IT Security Forms and Aids 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)
- Sanitization Method (Clear, Purge, Destroy)
- Date Conducted
- Person Performing
- Person Validating
- Final Disposition of Media (Disposed, Reused Internally, Reused Externally, Returned to Manufacturer).

Consistent with the NARA General Records Schedule 3.1: General Technology Management Records, Information technology operations and management records (Item 020), the completed document must be maintained for 3 years by the System Owner.

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 CISA, OIG, and U.S. Congress IAW this guide and the CISA Federal Incident Notification Guidelines.*

4 GSA Implementation Guidance for MP Controls

The GSA-defined parameter settings included in the control requirements are in blue, italicized text and offset by brackets in the control text. As stated in Section 1.2, Scope, the requirements outlined within this guide apply to all GSA systems and must be followed by all GSA Federal employees and contractors 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 information systems operated on behalf of GSA. Any additional instructions or requirements for contractor systems will be included in the "Additional Contractor System Considerations" portion of each control section. The MP controls apply to all types of media and their usage, for example backup media (e.g., tapes), media with archived data, and media used during development or testing require adherence to the media protection processes and procedures specified in this guide.

Table 4-1 identifies the designation of MP controls as Common, Hybrid, or System-Specific Controls for both Federal and Contractor systems. Effectively, common controls are provided by GSA at the enterprise level or by one of GSA's Major Information Systems (e.g., General Support System), system specific controls are implemented at the system level, and hybrid controls have shared responsibilities. CIO-IT Security-18-90, the ISPP, describes the GSA enterprise-wide common and hybrid controls and outlines the responsible parties for implementing them.

Note: Until the ISPP is updated to NIST SP 800-53, Revision 5, contact ispcompliance@gsa.gov for guidance if there is a discrepancy between this guide and the ISPP.

Table 4-1: Designation of MP Controls

System Type	Federal	Contractor
Common	MP-1	
Hybrid		MP-1
System-Specific	MP-2, MP-3, MP-4, MP-5, MP-6, MP-6 (1), MP-6(2), MP-6(3), MP-7	MP-2, MP-3, MP-4, MP-5, MP-6, MP-6(1), MP-6(2), MP-6(3), MP-7

Table 4-2 identifies GSA MP control applicability at the FIPS 199 Low, Moderate, and High levels.

Table 4-2: GSA Designation of MP Control Applicability

FIPS 199 Level	Applicable Controls
Low	MP-1, MP-2, MP-6, MP-7
Moderate	MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7
High	MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-6(1), MP-6(2), MP-6(3), MP-7

4.1 MP-1 Policy and Procedures

Control:

a. Develop, document, and disseminate to [*personnel with IT security responsibilities as defined in GSA CIO Order 2100.1*]:
   1. [*Organization-level*] media protection policy that:
      (a) Addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
      (b) Is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines; and
   2. Procedures to facilitate the implementation of the media protection policy and the associated media protection controls;

b. Designate an [*CISO*] to manage the development, documentation, and dissemination of the media protection policy and procedures; and

c. Review and update the current media protection:
   1. Policy [*annually, as part of CIO 2100.1, GSA IT Security Policy*] and following [*changes to Federal or GSA policies, requirements, or guidance*]; and

2. Procedures [*at least every three (3) years*] and following [*changes to Federal or GSA policies, requirements, or guidance*].

GSA Implementation Guidance: Control MP-1 is applicable at all FIPS 199 levels. MP-1 is a Common Control for Federal systems and a Hybrid Control for Contractor systems.

Common Control Implementation:

The GSA media protection policy is defined in the GSA IT Security Policy, CIO 2100.1, which addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance regarding protecting media for GSA and its systems. This policy is consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. This policy is disseminated GSA-wide via GSA's InSite centralized agency web site.

Media protection procedures are documented in CIO-IT Security-06-32, "*IT Security Procedural Guide: Media Protection (MP)*" [this guide]. The procedures facilitate the implementation of the media protection policy and associated controls. The guide is disseminated GSA-wide via GSA's InSite centralized agency web site.

Per 2100.1, the CISO is responsible for managing the development and publishing of all security policies and IT security procedural guides.

The GSA OCISO is responsible for reviewing and updating CIO 2100.1 annually.

The GSA OCISO is responsible for reviewing and updating CIO-IT Security-06-32 every three years and following changes to Federal or GSA policies, requirements, or guidance.

Federal System System-Specific Expectation:
None, MP-1 is a common control.

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.

Note: Contractor systems, per CIO 2100.1, are information systems in GSA's inventory processing or containing GSA or Federal data where the infrastructure and applications are wholly operated, administered, managed, and maintained by a contractor in non-GSA facilities.

4.2 MP-2 Media Access

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

GSA Implementation Guidance: Control MP-2 is applicable at all FIPS 199 levels. MP-2 is a System-Specific Control for both Federal and Contractor systems.

Access to digital and non-digital media associated with the 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' for the information on the media are allowed access to media.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

4.3 MP-3 Media Marking

Control:

a. Mark system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
b. Exempt [*no media (i.e., all media must be marked)*] from marking if 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. MP-3 is a System-Specific Control for both Federal and Contractor systems.

FIPS 199 Moderate and High systems must mark all media associated with the 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.

CIO Order CIO 2103.1 and PBS Order 3490.3 require all media containing Controlled Unclassified Information (CUI) to be marked. Detailed information on marking media with CUI is available in GSA's CUI Marking Manual.

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: Vendors/contractors are required to comply with the control statements.

4.4 MP-4 Media Storage

Control:

a. Physically control and securely store [*digital media including magnetic tapes, external/removable hard drives, flash/thumb drives, and disks of any type*] within [*locked cabinets or safes in secure/controlled facilities within the authorization boundary*]; and
b. Protect system media types defined in MP-4a 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. MP-4 is a System-Specific Control for both Federal and Contractor systems.

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 are 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 issuance through check-out and check-in procedures to maintain accountability. The media specified must be protected as described until it is sanitized or destroyed using the methods described in Section 3.

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 140-3[3] validated encryption modules/mechanisms to encrypt PII, PCI, and business sensitive data.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

4.5 MP-5 Media Transport

Control:

a. Protect and control [*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 validated encryption module/mechanism*];
b. Maintain accountability for system media during transport outside of controlled areas;
c. Document activities associated with the transport of system media; and
d. Restrict the activities associated with the transport of system media to authorized personnel.

GSA Implementation Guidance: Control MP-5 is applicable at the FIPS 199 Moderate and High levels. MP-5 is a System-Specific Control for both Federal and Contractor systems.

[3] Ibid, 3.

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 140-3 encryption module/mechanism; non-digital media including but not limited to hard copy output, microfilms, 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.

An employee or contractor shall not physically take PII in any media form from GSA facilities (including GSA managed programs housed at contractor facilities under contract), without written permission from the employee's supervisor, the data owner, and the system AO. Approvals shall be filed with the employee's supervisor.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

4.6 MP-6 Media Sanitization

Control:

a. Sanitize [*all information system media, both digital and non-digital*] prior to disposal, release out of organizational control, or release for reuse using [*techniques and methods described in IT Security Procedural Guide: Media Protection (MP), CIO-IT Security-06-32*]; and
b. Employ 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, and Verify. Review, approve, track, document, and verify media sanitization and disposal actions.
(2) Media Sanitization | Equipment Testing. Test sanitization equipment and procedures [*annually*] to ensure that the intended sanitization is being achieved.
(3) Media Sanitization | Nondestructive Techniques. Apply nondestructive sanitization techniques to portable storage devices prior to connecting such devices to the system under the following circumstances: [*(1) Positive 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. MP-6 and all its enhancements are System-Specific Controls for both Federal and Contractor systems.

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; specific 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 reviewed, approved, tracked, documented, and verified upon completion, and that any sanitization equipment used is tested annually to ensure they are performing as required. The GSA Sanitization Information Form or other means as described in Section 3.2.5 may be used to support this control.

For MP-6 enhancement (3), FIPS 199 High impact systems must ensure all portable storage devices are sanitized (see Section 3.2) using nondestructive techniques 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: Vendors/contractors are required to comply with the control statements.

4.7 MP-7 Media Use

Control:

a. [*Restricts*] the use of [*digital storage devices, including backup media, removable media, and mobile devices*] on [*GSA information systems*] using [*GSA S/SO recommended and GSA CISO and AO approved security safeguards*]; and
b. Prohibit the use of portable storage devices in organizational systems when such devices have no identifiable owner.

GSA Implementation Guidance: Control MP-7 is applicable at all FIPS 199 levels. MP-7 is a System-Specific Control for both Federal and Contractor systems.

All systems shall restrict the use of the device(s) specified in part a of this control to devices 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. The use of portable storage devices when such devices have no identifiable owner is prohibited. The specific means of restricting or prohibiting use is up to system owners but must be approved by the GSA CISO and AO.

Additional Contractor System Considerations: Vendors/contractors are required to comply with the control statements.

5 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.