

Department of the Interior
Security Control Standard
Media Protection

April 2011

Version: 1.1



Signature Approval Page

Designated Official	
Bernard J. Mazer, Department of the Interior, Chief Information Officer	
Signature:	Date:

REVISION HISTORY

Author	Version	Revision Date	Revision Summary
Chris Peterson	0.1	January 19, 2011	Initial draft
Timothy Brown	0.2	January 25, 2011	Incorporated comments into body text
Timothy Brown	1.0	February 17, 2011	Final review and version change to 1.0
Lawrence K. Ruffin	1.1	April 29, 2011	Final revisions and version change to 1.1

TABLE OF CONTENTS

REVISION HISTORY3

TABLE OF CONTENTS4

SECURITY CONTROL STANDARD: MEDIA PROTECTION.....5

 MP-1 MEDIA PROTECTION POLICY AND PROCEDURES5

 MP-2 MEDIA ACCESS.....6

 MP-3 MEDIA MARKING.....6

 MP-4 MEDIA STORAGE7

 MP-5 MEDIA TRANSPORT8

 MP-6 MEDIA SANITATION.....10

SECURITY CONTROL STANDARD: MEDIA PROTECTION

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 describes the required process for selecting and specifying security controls for an information system based on its security categorizing, including tailoring the initial set of baseline security controls and supplementing the tailored baseline as necessary based on an organizational assessment of risk.

This standard specifies organization-defined parameters that are deemed necessary or appropriate to achieve a consistent security posture across the Department of the Interior. In addition to the NIST SP 800-53 Media Protection (MP) control family standard, supplemental information is included that establishes an enterprise-wide standard for specific controls within the control family. In some cases additional agency-specific or Office of Management and Budget (OMB) requirements have been incorporated into relevant controls. Where the NIST SP 800-53 indicates the need for organization-defined parameters or selection of operations that are not specified in this supplemental standard, the System Owner shall appropriately define and document the parameters based on the individual requirements, purpose, and function of the information system. The supplemental information provided in this standard is required to be applied when the Authorizing Official (AO) has selected the control, or control enhancement, in a manner that is consistent with the Department's IT security policy and associated information security Risk Management Framework (RMF) strategy.

Additionally, information systems implemented within cloud computing environments shall select, implement, and comply with any additional and/or more stringent security control requirements as specified and approved by the Federal Risk and Authorization Management Program (FedRAMP) unless otherwise approved for risk acceptance by the AO. The additional controls required for implementation within cloud computing environments are readily identified within the Priority and Baseline Allocation table following each control and distinguished by the control or control enhancement represented in **bold red text**.

MP-1 MEDIA PROTECTION POLICY AND PROCEDURES

Applicability: Bureaus and Offices

Control: The organization develops, disseminates, and reviews/updates at least annually:

- a. A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and
- b. Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls.

Supplemental Guidance: This control is intended to produce the policy and procedures that are required for the effective implementation of selected security controls and control enhancements in the media protection family. The policy and procedures are consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Existing organizational policies and procedures may make the need for additional specific policies and procedures unnecessary. The media protection policy can be included as part of the general information security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular information system, when required. The organizational risk management strategy is a key factor in the development of the media protection policy. Related control: PM-9.

Control Enhancements: None.

References: NIST Special Publications 800-12, 800-100.

Priority and Baseline Allocation:

P1	LOW MP-1	MOD MP-1	HIGH MP-1
-----------	-----------------	-----------------	------------------

MP-2 MEDIA ACCESS

Applicability: All Information Systems

Control: The organization restricts access to all information system media to authorized individuals using **[Assignment: organization-defined security measures]**.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection. Related controls: MP-4, PE-3.

Control Enhancements:

1. The organization employs automated mechanisms to restrict access to media storage areas and to audit access attempts and access granted.

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

References: FIPS Publication 199; NIST Special Publication 800-111.

Priority and Baseline Allocation:

P1	LOW MP-2	MOD MP-2 (1)	HIGH MP-2 (1)
-----------	-----------------	---------------------	----------------------

MP-3 MEDIA MARKING

Applicability: Moderate and High Impact Information Systems

Control: The organization:

- a. Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and
- b. Exempts **Assignment: organization-defined list of removable media types** from marking as long as the exempted items remain within any area or space for which the bureau or office has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information systems.

Supplemental Guidance: The term marking is used when referring to the application or use of human-readable security attributes. The term labeling is used when referring to the application or use of security attributes with regard to internal data structures within the information system (see AC-16, Security Attributes). Removable information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). An organizational assessment of risk guides the selection of media requiring marking. Marking is generally not required for media containing information determined by the organization to be in the public domain or to be publicly releasable. Some organizations, however, may require markings for public information indicating that the information is publicly releasable. Organizations may extend the scope of this control to include information system output devices containing organizational information, including, for example, monitors and printers. Marking of removable media and information system output is consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

Control Enhancements: None.

References: FIPS Publication 199.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD MP-3	HIGH MP-3
-----------	-------------------------	-----------------	------------------

MP-4 MEDIA STORAGE

Applicability: Moderate and High Impact Information Systems

Control: The organization:

- a. Physically controls and securely stores magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks within **Assignment: organization-defined controlled areas** using encryption utilizing a FIPS 140-2 validated encryption module for digital media or secure storage in locked cabinets or safes for non-digital media;
- b. Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Telephone systems are also considered

information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use extreme caution in the types of information stored on telephone voicemail systems. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections are sufficient to meet the requirements established for protecting the information and/or information system.

An organizational assessment of risk guides the selection of media and associated information contained on that media requiring physical protection. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact on the organization or individuals if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls to the facility where the media resides provide adequate protection.

As part of a defense-in-depth strategy, the organization considers routinely encrypting information at rest on selected secondary storage devices. The employment of cryptography is at the discretion of the information owner/steward. The selection of the cryptographic mechanisms used is based upon maintaining the confidentiality and integrity of the information. The strength of mechanisms is commensurate with the classification and sensitivity of the information. Related controls: AC-3, AC-19, CP-6, CP-9, MP-2, PE-3.

Control Enhancements:

1. The organization employs cryptographic mechanisms to protect information in storage.

Enhancement Supplemental Guidance: Related control: SC-13.

References: FIPS Publication 199; NIST Special Publications 800-56, 800-57, 800-111.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD MP-4 (1)	HIGH MP-4 (1)
-----------	-------------------------	---------------------	----------------------

MP-5 MEDIA TRANSPORT

Applicability: Moderate and High Impact Information Systems

Control: The organization:

- a. Protects and controls magnetic tapes, external/removable hard drives, flash/thumb drives, diskettes, compact disks and digital video disks during transport outside of controlled areas using encryption utilizing a FIPS 140-2 validated encryption module to protect sensitive information residing on digital media;
- b. Maintains accountability for information system media during transport outside of controlled areas; and
- c. Restricts the activities associated with transport of such media to authorized personnel.

Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas. Telephone systems are also considered information systems and may have the capability to store information on internal media (e.g., on voicemail systems). Since telephone systems do not have, in most cases, the identification, authentication, and access control mechanisms typically employed in other information systems, organizational personnel use caution in the types of information stored on telephone voicemail systems that are transported outside of controlled areas. A controlled area is any area or space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system. Physical and technical security measures for the protection of digital and non-digital media are commensurate with the classification or sensitivity of the information residing on the media, and consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. Locked containers and cryptography are examples of security measures available to protect digital and non-digital media during transport. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. An organizational assessment of risk guides: (i) the selection of media and associated information contained on that media requiring protection during transport; and (ii) the selection and use of storage containers for transporting non-digital media. Authorized transport and courier personnel may include individuals from outside the organization (e.g., U.S. Postal Service or a commercial transport or delivery service). Related controls: AC-19, CP-9.

Control Enhancements:

2. The organization documents activities associated with the transport of information system media.

Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk to include the flexibility to define different record-keeping methods for different types of media transport as part of an overall system of transport-related records.

3. The organization employs an identified custodian throughout the transport of information system media.

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

4. The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Enhancement Supplemental Guidance: This control enhancement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones). Related control: MP-4. Related controls: MP-2; SC-13.

References: FIPS Publication 199; NIST Special Publication 800-60.

Priority and Baseline Allocation:

P1	LOW Not Selected	MOD MP-5 (2) (4)	HIGH MP-5 (2) (3) (4)
-----------	-------------------------	-------------------------	------------------------------

MP-6 MEDIA SANITATION

Applicability: All Information Systems

Control: The organization:

- a. Sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse; and
- b. Employs sanitization mechanisms with strength and integrity commensurate with the classification or sensitivity of the information.

Supplemental Guidance: This control applies to all media subject to disposal or reuse, whether or not considered removable. Sanitization is the process used to remove information from information system media such that there is reasonable assurance that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, and destroying media information, prevent the disclosure of organizational information to unauthorized individuals when such media is reused or released for disposal. The organization uses its discretion on the employment of sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on the organization or individuals if released for reuse or disposal.

Control Enhancements:

1. The organization tracks, documents, and verifies media sanitization and disposal actions.
2. The organization tests sanitization equipment and procedures to verify correct performance
[Assignment: organization-defined frequency].
3. The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system under the following circumstances: [Assignment: organization-defined list of circumstances requiring sanitization of portable, removable storage devices].

Enhancement Supplemental Guidance: Portable, removable storage devices (e.g., thumb drives, flash drives, external storage devices) can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown sources and may contain various types of malicious code that can be readily transferred to the information system through USB ports or other entry portals. While scanning such devices is always recommended, sanitization provides additional assurance that the device is free of all malicious code to include code capable of initiating zero-day attacks. Organizations consider sanitization of portable, removable storage devices, for example, when such devices are first purchased from the manufacturer or vendor prior to initial use or when the organization loses a positive chain of custody for the device. An organizational assessment of risk guides the specific circumstances for employing the sanitization process. Related control: SI-3.

4. The organization sanitizes information system media containing Controlled Unclassified Information (CUI) or other sensitive information in accordance with applicable organizational and/or federal standards and policies.
5. The organization sanitizes information system media containing classified information in accordance with NSA standards and policies.

References: FIPS Publication 199; NIST Special Publications 800-60, 800-88; Web:
WWW.NSA.GOV/IA/GUIDANCE/MEDIA_DESTRUCTION_GUIDANCE/INDEX.SHTML.

Priority and Baseline Allocation:

P1	LOW MP-6	MOD MP-6 (4)	HIGH MP-6 (1) (2) (3) (4) (5)
-----------	-----------------	---------------------	--------------------------------------