|  |
| --- |
| **{COMMAND}** |
| **{SYSTEM NAME} {ACRONYM}** |
| **System Version: {VERSION}****eMASS# {EMASS#}****Confidentiality: {CONFIDENTIALITY}****Integrity: {INTEGRITY}****Availability: {AVAILABILITY}** |
| **Department of the {SERVICE}** |
| **{LOGO}** |
|  |
| **Media Protection Plan****Document Version: 1.0.0****{DATE}** |
| Prepared by: {ORGANIZATION}**DISTRIBUTION IS LIMITED TO U.S. GOVERNMENT AGENCIES AND THEIR CONTRACTORS.****OTHER REQUESTS FOR THIS DOCUMENT MUST BE REFERRED TO: {ORGANIZATION}** |

**Change Record**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Author | Changes Made / Section(s) |
| {DATE} | 1.0.0 | {ORGANIZATION} | Initial Document |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Amplifying Guidance**

1. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01F, "Information Assurance (IA) and Support to Computer Network Defense (CND)" 
2. DODM NUMBER 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification" 
3. DODM NUMBER 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information" 
4. DODM NUMBER 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information" 
5. DODM NUMBER 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)" 
6. DOD CIO Memorandum, 3 July 2007, “Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media” 
7. NIST Special Publication 800-88 R1, "Guidelines for Media Sanitization" 
8. CTO 08-001, "JTF-GNO Communications Tasking Order (CTO) 08-001, Encryption of Sensitive Unclassified Data at Rest (DAR) on Mobile Computing Devices and Removable Storage Media Used Within the Department of Defense (DoD)" 
9. CTO 08-001 (Attachment), "JTF-GNO Communications Tasking Order (CTO) 08-001, Encryption of Sensitive Unclassified Data at Rest (DAR) on Mobile Computing Devices and Removable Storage Media Used Within the Department of Defense (DoD) (Attachment)" 
10. CTO 10-133, "USCYBERCOM Communications Tasking Order (CTO) 10-133 Protection of Classified Information on Department of Defense Secret Internet Protocol Router Network (SIPRNet)" 
11. CTO 10-133A, "Communications Tasking Order (CTO) 10-133 10-133A, Amplifying Guidance" 
12. National Security Agency (NSA) Media Destruction Guidance 

**Table of Contents**

[1.0 OVERVIEW 1](#_Toc433030253)

[1.1 Applicability 1](#_Toc433030254)

[1.2 Roles and Responsibilities 1](#_Toc433030255)

[2.0 STORAGE AND PROTECTION 2](#_Toc433030256)

[2.1 Storage 2](#_Toc433030257)

[2.2 Protection During Transport 2](#_Toc433030258)

[3.0 MARKING AND LABELING 3](#_Toc433030259)

[3.1 Non-digital Media 3](#_Toc433030260)

[3.2 Removable Media 3](#_Toc433030261)

[4.0 SANITIZATION 3](#_Toc433030262)

[APPENDIX A – DETAILED COMPLIANCE MATRIX 6](#_Toc433030263)

[ENCLOSURE 1 – SANITIZATION CERTIFICATE 32](#_Toc433030264)

[ENCLOSURE 2 – REMOVABLE MEDIA INVENTORY 34](#_Toc433030265)

[Figure 1 - Sanitization and Disposition Decision Flow 5](#_Toc433030294)

[Table 1 - SP-800-53v4 Compliance Matrix 1](#_Toc433030300)

[Table 2 - Roles and Responsibilities 2](#_Toc433030301)

# **OVERVIEW**

The information security concerns regarding media protection resides not in the media itself, but in the recorded information. The issue of media protection is driven by the information placed intentionally or unintentionally on the media. Electronic media used on a system should be assumed to contain information commensurate with the security categorization of the system’s confidentiality. If not handled properly, release of these media could lead to an occurrence of unauthorized disclosure of information.

This plan does not claim to cover all possible media that {ACRONYM} could use to store information, nor does it attempt to forecast the future media that may be developed during the effective life of this plan. Users are expected to make protection decisions based on the security categorization of the information contained on the media and the overarching regulations that govern media disposal, sanitization and control listed in the [Amplifying Guidance](#guidance) section of this document.

This document complies with the following requirements from NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations". A detailed compliance matrix can be found in [Appendix I, “Detailed Compliance Matrix”](#_APPENDIX_I_–).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CNTL NO. | CONTROL NAME | PRIORITY | LOW | MOD | HIGH |
| [MP-1](#MP1) | Media Protection Policy and Procedures | P1 | MP-1 | MP-1 | MP-1 |
| [MP-2](#MP2) | Media Access | P1 | MP-2 | MP-2 | MP-2 |
| [MP-3](#MP3) | Media Marking | P2 | Not Selected | MP-3 | MP-3 |
| [MP-4](#MP4) | Media Storage | P1 | Not Selected | MP-4 | MP-4 |
| [MP-5](#MP5) | Media Transport | P1 | Not Selected | MP-5 (4) | MP-5 (4) |
| [MP-6](#MP6) | Media Sanitization | P1 | MP-6 | MP-6 | MP-6 (1) (2) (3) |
| [MP-7](#MP7) | Media Use | P1 | MP-7 | MP-7 (1) | MP-7 (1) |
| [MP-8](#MP8) | Media Downgrading | P0 | Not Selected | Not Selected | Not Selected |

Table - SP-800-53v4 Compliance Matrix

## **1.1 Applicability**

This Media Protection Plan applies to {ACRONYM} and its components.

## **1.2 Roles and Responsibilities**

The following roles have been established for the {ACRONYM} in accordance DoD 5200.01-M, CTO 10-133, and CTO 08-001 to restrict access to media:

| Role | Responsibility | Point of Contact |
| --- | --- | --- |
| Commanding Officer | Overall responsibility for the protection of classified information on Department of the Navy systems. | {NAME}{PHONE}{EMAIL} |
| Information Systems Security Manager (ISSM) | Information security staff members may be needed during certain stages of incident handling (prevention, containment, eradication, and recovery)—for example, to alter network security controls (e.g., firewall rulesets). | {NAME}{PHONE}{EMAIL} |
| Data Transfer Agent (DTA) | Perform the transfer, and ensure proper handling and documentation of media. | {NAME}{PHONE}{EMAIL} |

Table - Roles and Responsibilities

# **2.0 STORAGE AND PROTECTION**

## **2.1 Storage**

**Classified Media** – all classified media shall be secured under conditions adequate to deter and detect access by unauthorized persons. Holdings of classified media will be reduced to the minimum required to accomplish the mission. GSA establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, modular vaults, alarm systems, and associated security devices suitable for storing and protecting classified information. [DoDI 3224.03](http://www.dtic.mil/whs/directives/corres/pdf/322403p.pdf) describes requirements for acquiring physical security equipment for use within the Department of Defense. Refer to [DODM NUMBER 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information"](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf) for specific guidance.

**For Official Use Only Media** – During working hours, reasonable steps shall be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing, or leaving FOUO information unattended where unauthorized personnel are present). After working hours, FOUO information may be stored in unlocked containers, desks, or cabinets if Government or Government-contract building security is provided. If such building security is not provided or is deemed inadequate, the information shall be stored in locked desks, file cabinets, bookcases, locked rooms, etc. Refer to refer to [DODM NUMBER 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)"](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf) for specific guidance.

## **2.2 Protection During Transport**

FIPS 140-2 or other NSA approved cryptographic mechanisms will be used to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.

Appropriately cleared and briefed personnel may be authorized to escort or carry classified material between locations when other means of transmission or transportation cannot be used. The Heads of the DoD Components shall establish procedures to ensure that hand-carrying of classified material is minimized to the greatest extent possible and does not pose unacceptable risk to the information. Hand carrying may be authorized only when:

1. The information is not available at the destination and operational necessity or a contractual requirement requires it.
2. The information cannot be sent via a secure e-mail, facsimile transmission or other secure means.
3. The appropriate official authorizes the hand-carry according to procedures the Head of the DoD Component establishes.
4. The hand-carry is accomplished aboard a U.S. carrier, or a foreign carrier if no U.S. carrier is available, and the U.S. escort retains custody and physical control of the information at all times.
5. Arrangements have been made for secure storage of the information at a U.S. Government or cleared U.S. contractor facility.

Refer to [DODM NUMBER 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information"](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol3.pdf) for specific guidance.

# **3.0 MARKING AND LABELING**

## **3.1 Non-digital Media**

All classified information shall be identified clearly by marking, designation, or electronic labeling. If physical marking of the medium containing classified information is not possible, then identification must be accomplished by other means. The term “marking” includes other concepts of identifying the classification of the information. Markings, designations, and electronic labeling shall be conspicuous and immediately apparent and shall:

1. Alert holders to the presence of classified information.
2. Identify, as specifically as possible, the exact information needing protection and the level of protection required.
3. Give information on the source(s) of and reasons for classification of the information.
4. Identify the office of origin and document originator applying the classification markings.
5. Provide guidance on information sharing, and warn holders of special access, dissemination control, or safeguarding requirements.
6. Provide guidance on downgrading and declassification for classified information.

The proper marking of a classified document is the specific responsibility of the original or derivative classifier (i.e., the author or originator of the information). Derivative classifiers shall refer to the source document(s), security classification guide(s), or other guidance issued by the original classification authority (OCA) when determining the markings to apply.

Refer to [DODM NUMBER 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information"](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf) for specific guidance.

## **3.2 Removable Media**

Removable storage media used with computers, IT systems, and other electronic devices will be conspicuously marked. (Examples of such media include, but are not limited to, compact discs, DVDs, removable hard disks, flash or “thumb” drives, magnetic tape reels, disk packs, floppy disks and diskettes, disk cartridges, optical discs, paper tape, magnetic cards, memory chips, and tape cassettes and micro-cassettes.) Internal media identification will include security markings in a form suitable for the media. All such devices bearing classified information must be conspicuously marked with the highest level of classification of information stored on the device and any dissemination control notices that apply to the information.

For classified information, refer to [DODM NUMBER 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information"](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol2.pdf) for specific guidance.

For Controlled Unclassified Information, refer to [DODM NUMBER 5200.01, Volume 4, "DoD Information Security Program: Controlled Unclassified Information (CUI)"](http://www.dtic.mil/whs/directives/corres/pdf/520001_vol4.pdf) for specific guidance.

# **4.0 SANITIZATION**

In accordance with [CCI-001028](#CCI001028), DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88. Sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This plan will assist {ACRONYM} and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information. It does not, and cannot, specifically address all known types of media; however, the described sanitization decision process can be applied universally. The categories of sanitization are defined as follows:

1. **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
2. **Purge** applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
3. **Destroy** renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data

It is suggested that the {ACRONYM} categorize the information, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then, the {ACRONYM} can choose the appropriate type(s) of sanitization. {ACRONYM} will use the following process to assist them in making sanitization decisions that are commensurate with the security categorization of the confidentiality of information contained on the media. The decision process is based on the confidentiality of the information, not the type of media. Once {ACRONYM} decides what type of sanitization is best for their individual case, then the media type will influence the technique used to achieve this sanitization goal.



Figure - Sanitization and Disposition Decision Flow

Validating the selected information sanitization and disposal process is an essential step in maintaining confidentiality. Two types of verification should be considered. The first is verification every time sanitization is applied (where applicable, as most Destroy techniques do not support practical verification for each sanitized piece of media). The second is a representative sampling verification, applied to a selected subset of the media. If possible, the sampling should be executed by personnel who were not part of the original sanitization action.

Following sanitization, a certificate of media disposition will be completed for each piece of electronic media that has been sanitized. An example sanitization certificate is contained within [Enclosure 1, “Sanitization Certificate”](#_Enclosure_1_–). [NIST SP 800-88 Rev. 1](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf), Appendix A contains detailed Minimum Sanitization Recommendations.

# **APPENDIX A – DETAILED COMPLIANCE MATRIX**

The following table provides traceability between this document and the Assessment Procedures contained within NIST Special Publication 800-53A Revision 4, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations".

| Control Number | AssessmentNumber | CCI Number | Confidentiality | Integrity | Availability | Assessment Procedures | Reference |
| --- | --- | --- | --- | --- | --- | --- | --- |
| MP-1 | MP-1 (a) (1) | CCI-002566 | HighModerateLow | HighModerateLow |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the personnel or roles as all users. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-1 | MP-1 (a) (1) | CCI-000995 | HighModerateLow | HighModerateLow |  | DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-1 | MP-1 (a) (1) | CCI-000996 | HighModerateLow | HighModerateLow |  | DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-1 | MP-1 (a) (2) | CCI-000999 | HighModerateLow | HighModerateLow |  | DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-1 | MP-1 (a) (2) | CCI-001000 | HighModerateLow | HighModerateLow |  | DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-1 | MP-1 (b) (1) | CCI-000998 | HighModerateLow | HighModerateLow |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 5 years reviewed annually - updated as appropriate but at least within 10 years of date of issuance. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-1 | MP-1 (b) (1) | CCI-000997 | HighModerateLow | HighModerateLow |  | DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-1 | MP-1 (b) (2) | CCI-001002 | HighModerateLow | HighModerateLow |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as annually reviewed annually - updated as appropriate. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-1 | MP-1 (b) (2) | CCI-001001 | HighModerateLow | HighModerateLow |  | DoDI 5200.01 and DoDM 5200.01 Vol. 1-4 meet the DoD requirements for media protection policy and procedures. DoD Components are automatically compliant with this CCI because they are covered by the DoD level policies, DoDI 5200.01 and DoDM 5200.01 Vol. 1-4. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-2 | MP-2 | CCI-001003 | HighModerateLow | HighModerateLow |  | The organization conducting the inspection/assessment interviews organizational personnel with information system media protection responsibilities to ensure the organization being inspected/assessed restricts access to all types of digital and/or non-digital media containing information not cleared for public release to the personnel or roles defined in MP-2, CCI 1005. DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.  | [Section 1.2](#_1.2_Roles_and) |
| MP-2 | MP-2 | CCI-001005 | HighModerateLow | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines the documented personnel or roles to restrict access to media to ensure the access is granted IAW DoD 5200.01-M, CTO 10-133, and CTO 08-001. DoD has determined the personnel or roles are not appropriate to define at the Enterprise level, but personnel must be identifiedIAW DoD 5200.01-M, CTO 10-133, and CTO 08-001. | [Section 1.2](#_1.2_Roles_and) |
| MP-2 | MP-2 | CCI-001004 | HighModerateLow | HighModerateLow |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the types of digital and non-digital media as all types of digital and/or non-digital media containing information not cleared for public release.   | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-3 | MP-3 (a) | CCI-001010 | HighModerate |  |  | The organization conducting the inspection/assessment obtains a sampling of information system media and information system output to verify that it is marked in compliance with DoDM 5200.01 Vol. 1-4. | [Section 3](#_3.0_MARKING_AND) |
| MP-3 | MP-3 (b) | CCI-001011 | HighModerate |  |  | The organization conducting the inspection/assessment examines information system media to ensure it is marked IAW DoDM 5200.01 Vol. 1-4. | [Section 3](#_3.0_MARKING_AND) |
| MP-3 | MP-3 (b) | CCI-001012 | HighModerate |  |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the list of information system media as nothing unless otherwise exempted by DoDI 5200.01 and DoDM 5200.01 Vol 1-4 | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-3 | MP-3 (b) | CCI-001013 | HighModerate |  |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the controlled areas as all areas unless otherwise exempted by DoDI 5200.01 and DoDM 5200.01 Vol 1-4 | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-4 (2) | MP-4 (2) | CCI-001007 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system's environment to ensure the organization being inspected/assessed implements automated mechanisms to restrict access to media storage areas. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-4 (2) | MP-4 (2) | CCI-001008 | blank | blank | blank | The organization conducting the inspection/assessment examines the information system's environment to ensure the organization being inspected/assessed implements automated mechanisms to audit access attempts and access granted to media storage areas. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-4 | MP-4 (a) | CCI-001014 | HighModerate | HighModerate |  | The organization conducting the inspection/assessment obtains and examines the list of all digital and non-digital media containing sensitive, controlled, and/or classified information within areas approved for processing or storing data IAW the sensitivity and/or classification level of the information contained on/within the media to ensure that physical controls are in place and that it is securely stored as defined in PE-3. DoD has defined the digital and non-digital media types as all digital and non-digital media containing sensitive, controlled, and/or classified information.  DoD has defined the controlled areas as areas approved for processing or storing data IAW the sensitivity and/or classification level of the information contained on/within the media. | [Section 2.1](#_2.1_Storage) |
| MP-4 | MP-4 (a) | CCI-001015 | HighModerate | HighModerate |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the digital and non-digital media types as all digital and non-digital media containing sensitive, controlled, and/or classified information. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-4 | MP-4 (a) | CCI-001016 | HighModerate | HighModerate |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the controlled areas as areas approved for processing or storing data IAW the sensitivity and/or classification level of the information contained on/within the media. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-4 | MP-4 (b) | CCI-001018 | HighModerate | HighModerate |  | The organization conducting the inspection/assessment obtains and examines the list of media and verifies it is being stored and protected IAW DoDM 5200.01 M Vol. 1-4. | [Section 2.1](#_2.1_Storage)[Enclosure 2](#_ENCLOSURE_2_–) |
| MP-5 (3) | MP-5 (3) | CCI-001026 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines documentation identifying the custodian that is at all times responsible for the transport of the all information system media, from pick-up to final delivery and receipt acknowledgement. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-5 (4) | MP-5 (4) | CCI-001027 | HighModerate | HighModerate |  | The organization conducting the inspection/assessment obtains and examines the Security Plan to ensure the organization being inspected has identified FIPS 140-2 or other NSA approved cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. | [Section 2.2](#_2.2_Protection_During) |
| MP-5 | MP-5 (a) | CCI-001020 | HighModerate | HighModerate |  | The organization conducting the inspection/assessment obtains and examines the organization's records management policy or process to ensure appropriate protection of information according to its classification or designation during transport outside of controlled areas, IAW security measures defined in DoDM 5200.01 M Vol. 1-4 and DoDD 5015.2. | [Section 2.2](#_2.2_Protection_During) |
| MP-5 | MP-5 (a) | CCI-001021 | HighModerate | HighModerate |  | DoD has defined the types of information system media as all digital and non-digital media containing sensitive, controlled, and/or classified information.  The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-5 | MP-5 (a) | CCI-001022 | HighModerate | HighModerate |  | DoD has defined the security safeguards as DoDI 5200.1R and other organizationally defined security safeguards. The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-5 | MP-5 (b) | CCI-001023 | HighModerate | HighModerate |  | The organization conducting the inspection/assessment obtains and examines the list of organization defined security measures (MP-2) to ensure method of accountability for information system media during transport outside of controlled areas has been identified. | [Section 2.2](#_2.2_Protection_During) |
| MP-5 | MP-5 (c ) | CCI-001025 | HighModerate | HighModerate |  | The organization conducting the inspection/assessment obtains and examines the documented activities to ensure the organization being inspected/assessed documents activities associated with the transport of information system media. | [Section 2.2](#_2.2_Protection_During) |
| MP-5 | MP-5 (d) | CCI-001024 | HighModerate | HighModerate |  | The organization conducting the inspection/assessment obtains and examines the list of personnel authorized to transport information system media outside of controlled areas. Organizational personnel with information system media transport responsibilities and security management personnel are to be interviewed. The purpose of the reviews and reviews is to determine if the organization has established restrictions associated with the transport of information system media to authorized personnel only. | [Section 2.2](#_2.2_Protection_During) |
| MP-6 (1) | MP-6 (1) | CCI-002567 | High |  |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of media sanitization actions to ensure the organization being inspected/assessed reviews and approves media sanitization actions. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MP-6 (1) | MP-6 (1) | CCI-002568 | High |  |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of media sanitization actions to ensure the organization being inspected/assessed tracks and documents media sanitization actions. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MP-6 (1) | MP-6 (1) | CCI-002569 | High |  |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of media sanitization actions to ensure the organization being inspected/assessed verifies media sanitization actions. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MP-6 (1) | MP-6 (1) | CCI-002570 | High |  |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of media disposal actions to ensure the organization being inspected/assessed reviews and approves media disposal actions. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MP-6 (1) | MP-6 (1) | CCI-002571 | High |  |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of media disposal actions to ensure the organization being inspected/assessed tracks and documents media disposal actions. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MP-6 (1) | MP-6 (1) | CCI-002572 | High |  |  | The organization conducting the inspection/assessment obtains and examines the documented process as well as the record of media disposal actions to ensure the organization being inspected/assessed verifies media disposal actions. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MP-6 (2) | MP-6 (2) | CCI-001030 | High |  |  | The organization conducting the inspection/assessment obtains and examines documented test plans and evidence of past tests to ensure that tests are conducted every 180 days to verify correct performance of sanitization equipment and procedures. DoD has defined the frequency as every 180 days. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MP-6 (2) | MP-6 (2) | CCI-001031 | High |  |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as every 180 days. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-6 (3) | MP-6 (3) | CCI-001032 | High |  |  | The organization conducting the inspection/assessment obtains and examines media sanitization records, audit records, and any other relevant documents or records.  The objective of the reviews is to confirm the organization is in compliance with the list of defined circumstances requiring the sanitization of portable storage devices prior to connecting such devices to the information system. | The system is not considered a HIGH level. Therefore, this AP is not applicable. |
| MP-6 (3) | MP-6 (3) | CCI-001033 | High |  |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the circumstances as when such devices are first purchased from the manufacturer or vendor prior to initial use, when being considered for reuse, or when the organization loses a positive chain of custody for the device. Media obtained from unknown sources shall not be sanitized and reused. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-6 (7) | MP-6 (7) | CCI-002573 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process as well as a sampling of records of sanitization actions to ensure the organization being inspected/assessed enforces dual authorization for the sanitization of information system media defined in MP-6 (7), CCI 2574. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-6 (7) | MP-6 (7) | CCI-002574 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system media to ensure the organization being inspected/assessed defines the information system media that dual authorization should be enforced for sanitization. DoD has determined the information system media is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-6 (8) | MP-6 (8) | CCI-002575 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information systems, system components, or devices to ensure the organization being inspected/assessed defines information systems, system components, or devices that information should be purged/wiped either remotely or under the organization-defined conditions. DoD has determined the information systems, system components, or devices are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-6 (8) | MP-6 (8) | CCI-002576 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented conditions to ensure the organization being inspected/assessed defines conditions in which information from organization-defined information systems, system components, or devices should be purged/wiped.  DoD has determined the conditions are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-6 (8) | MP-6 (8) | CCI-002577 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process to ensure the organization being inspected/assessed provides the capability to purge /wipe information from information systems, system components, or devices defined in MP-6 (8), CCI 2575 either remotely or under conditions defined in MP-6 (8), CCI 2576. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-6 | MP-6 (a) | CCI-001028 | HighModerateLow |  |  | The organization conducting the inspection/assessment obtains and examines media sanitization records, audit records, any other relevant documents or records, and sanitization tools to ensure sanitization is in compliance with DoDM 5200.01 Vol. 1-4 and uses techniques and procedures IAW NIST SP 800-88. The objective of the review is to verify the organization is sanitizing its digital and non-digital information system media prior to disposal, release for reuse, or release out of the organizational control. DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88. DoD has defined the information system media as all media. | [Section 4](#_4.0_SANITIZATION)[Enclosure 1](#_Enclosure_1_–) |
| MP-6 | MP-6 (a) | CCI-002578 | HighModerateLow |  |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the information system media as all media. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-6 | MP-6 (a) | CCI-002579 | HighModerateLow |  |  | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the sanitization techniques as techniques and procedures IAW NIST SP 800-88. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-6 | MP-6 (b) | CCI-002580 | HighModerateLow |  |  | The organization conducting the inspection/assessment obtains and examines the audit trail of sanitization actions to ensure the organization being inspected/assessed implements sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. | [Section 4](#_4.0_SANITIZATION)[Enclosure 1](#_Enclosure_1_–) |
| MP-7 | MP-7 | CCI-002581 | HighModerateLow | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines the documented type of information system media to ensure the organization being inspected/assessed defines the types of information system media to restrict or prohibit on organization-defined information systems or system components using organization-defined security safeguards. DoD has determined the types of information system media are not appropriate to define at the Enterprise level. | [Section 4](#_4.0_SANITIZATION)[Enclosure 1](#_Enclosure_1_–) |
| MP-7 | MP-7 | CCI-002582 | HighModerateLow | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines the documented information systems or system components to ensure the organization being inspected/assessed defines the information systems or system components to restrict or prohibit the use of organization-defined types of information system media using organization-defined security safeguards. DoD has determined the information systems or system components are not appropriate to define at the Enterprise level. | [Section 4](#_4.0_SANITIZATION)[Enclosure 1](#_Enclosure_1_–) |
| MP-7 | MP-7 | CCI-002583 | HighModerateLow | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines the documented security safeguards to ensure the organization being inspected/assessed defines the security safeguards to use for restricting or prohibiting the use of organization-defined types of information system media on organization-defined information systems or system components. DoD has determined the security safeguards are not appropriate to define at the Enterprise level. | [Section 4](#_4.0_SANITIZATION)[Enclosure 1](#_Enclosure_1_–) |
| MP-7 | MP-7 | CCI-002584 | HighModerateLow | HighModerateLow |  | The organization conducting the inspection/assessment obtains and examines the documented controls and examines information system procedures associated with the use of media to ensure the organization being inspected/assessed documents and enforces controls for the use of media defined in MP-7, CCI 2581 on systems defined in MP-7, CCI 2582 using security safeguards defined in MP-7, CCI 2583. | [Enclosure 2](#_ENCLOSURE_2_–) |
| MP-7 (1) | MP-7 (1) | CCI-002585 |  | HighModerateLow |  | The organization conducting the inspection/assessment examines a sampling of portable storage devices used in the information system to ensure that the devices have an identifiable owner. | [Enclosure 2](#_ENCLOSURE_2_–) |
| MP-7 (2) | MP-7 (2) | CCI-002586 | blank | blank | blank | The organization conducting the inspection/assessment examines a sampling of media used in the information system to ensure sanitization-resistant media is not used. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-8 (1) | MP-8 (1) | CCI-002587 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system media downgrading actions to ensure the organization being inspected/assessed documents information system media downgrading actions. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-8 (2) | MP-8 (2) | CCI-002588 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the record of tests to ensure the organization being inspected/assessed implements tests defined in MP-8 (2), CCI 2590 at a minimum annually to verify correct performance of equipment. DoD has defined the frequency as at a minimum annually. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-8 (2) | MP-8 (2) | CCI-002589 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the record of tests to ensure the organization being inspected/assessed implements tests defined in MP-8 (2), CCI 2590 at a minimum annually to verify correct performance of procedures. DoD has defined the frequency as at a minimum annually.  | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-8 (2) | MP-8 (2) | CCI-002590 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented tests to ensure the organization being inspected/assessed defines tests to employ for downgrading equipment. DoD has determined the tests are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-8 (2) | MP-8 (2) | CCI-002591 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the frequency as at a minimum annually. | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-8 (3) | MP-8 (3) | CCI-002593 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the record of public release of media as well as records of information system media downgrade to ensure the organization being inspected/assessed implements a process to downgrade information system media containing any Controlled Unclassified Information (CUI) prior to public release in accordance with applicable federal and organizational standards and policies. DoD has defined the Controlled Unclassified Information (CUI) as any Controlled Unclassified Information (CUI). | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-8 (3) | MP-8 (3) | CCI-002592 | blank | blank | blank | The organization being inspected/assessed is automatically compliant with this CCI because they are covered at the DoD level. DoD has defined the Controlled Unclassified Information (CUI) as any Controlled Unclassified Information (CUI). | Automatically compliant with this CCI because they are covered at the DoD level |
| MP-8 (4) | MP-8 (4) | CCI-002594 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the record of release of media containing classified information as well as records of information system media downgrade to ensure the organization being inspected/assessed implements a process to downgrade information system media containing classified information prior to release to individuals without required access authorizations in accordance with NSA standards and policies. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-8 | MP-8 (a) | CCI-002596 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system media downgrading process to ensure the organization being inspected/assessed defines an information system media downgrading process that includes employing downgrading mechanisms with organization-defined strength and integrity.  DoD has determined the information system media downgrading process is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-8 | MP-8 (a) | CCI-002597 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented strength and integrity to ensure the organization being inspected/assessed defines strength and integrity for downgrading mechanisms to establish an organization-defined information system media downgrading process.  DoD has determined the strength and integrity are not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-8 | MP-8 (b) | CCI-002598 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented process defined in MP-8, CCI 2596 to ensure it is commensurate with the security category and/or classification level of the information to be removed and the access authorizations of the potential recipients of the downgraded information. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-8 | MP-8 (c ) | CCI-002599 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the documented information system media to ensure the organization being inspected/assessed defines and identifies the information system media requiring downgrading. DoD has determined the information system media is not appropriate to define at the Enterprise level. | NIST has not allocated this AP. Therefore, this AP is not applicable. |
| MP-8 | MP-8 (d) | CCI-002600 | blank | blank | blank | The organization conducting the inspection/assessment obtains and examines the record of downgrade activities to ensure the organization being inspected/assessed implements the process defined in MP-8, CCI 2596 to downgrade media defined in MP-8, CCI 2599. | NIST has not allocated this AP. Therefore, this AP is not applicable. |

# **ENCLOSURE 1 – SANITIZATION CERTIFICATE**

|  |
| --- |
| CERTIFICATE OF SANITIZATION |
| PERSON PERFORMING SANITIZATION |
| Name: Enter text. | Title: Click or tap here to enter text. |
| Organization: Enter text. | Location: Click or tap here to enter text. | Phone: Click or tap here to enter text. |
| MEDIA INFORMATION |
| Make/Vendor: Enter text. | Model Number: Enter text. |
| Serial Number: Enter text. |
| Media Property Number: Enter text. |
| Media Type: Enter text. | Source: Enter text. |
| Classification: Click or tap here to enter text. | Data Backed Up:  | Yes [ ]  | No [ ]  | Unknown [ ]  |
| Backup Location: Enter text. |
| SANITIZATION DETAILS |
| Method Type: | Clear [ ]  | Purge [ ]  | Damage [ ]  | Destruct [ ]  |
| Method Used: | Degauss [ ]  | Overwrite [ ]  | Block Erase [ ]  | Crypto Erase [ ]  | Other [ ]  |
| Method Details: Enter text. |
| Tool Used *(include version)*: Enter text. |
| Verification Method: | Full [ ]  | Quick Sampling [ ]  | Other [ ]  |
| Post Sanitization Classification: Enter text. |
| Notes: Enter text. |
| MEDIA DESTINATION |
| Internal Reuse [ ]  | External Reuse [ ]  | Recycling [ ]  | Manufacturer [ ]  | Other [ ]  |
| Details: Enter text. |
| SIGNATURE |
| *I attest that the information provided on this statement is accurate to the best of my knowledge* |
| Signature:  | Date: Enter a date. |
| VALIDATION |
| Name: Enter text. | Title: Enter text. |
| Organization: Enter text. | Location: Enter text. | Phone: Enter text. |
| Signature:   | Date: Enter a date. |

# **ENCLOSURE 2 – REMOVABLE MEDIA INVENTORY**

The following table contains the inventory of {ACRONYM} removable storage devices and their compliance status with the [Removable Storage and External Connections Security Technical Implementation Guide (STIG)](http://iasecontent.disa.mil/stigs/zip/Apr2015/U_Removable_Storage_and_External_Connections_V1R3_STIG.zip).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **STO-ALL-010IA Approved** | **STO-ALL-030Device ID** | **Authorized Users** | **Make** | **Model** | **STO-ALL-02Gov. Owned** | **STO-DRV-010Password/PIN** | **STO-DRV-021NSA Approved** | **STO-DRV-025DAR Enforced** | **STO-DRV-040Signed Firmware** |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |