NSA/CSS POLICY 6-22
HANDLING OF NSA/CSS INFORMATION STORAGE MEDIA

DATE:	21 November 2019 (See Document History)
OFFICE OF PRIMARY INTEREST:	Security Engineering Services, 968-7777s.
RELEASABILITY:	This policy is approved for public release. The official document is available on the Office of Policy (P12) website ("go policy").
AUTHORITY:	Gregory L. Smithberger, NSA/CSS Chief Information Officer
ISSUED:	9 June 2017

PURPOSE AND SCOPE

1. This document establishes policy and assigns responsibilities for the secure handling of all NSA/CSS *information storage media (ISM)*, including the proper labeling of classified and unclassified ISM, the *administrative declassification* of previously classified ISM, and obtaining approval to *release* these media from controlled facilities. ISM includes, but is not limited to, *magnetic storage*, *optical storage*, and *solid state storage*, whether the ISM is connected to an *information system (IS)* internally or externally.

2. This policy applies to users of all classified and unclassified IS resources for which the Director, NSA/Chief, CSS has operational *information system security* responsibility. This policy implements relevant portions of References a, b, and c.

POLICY

3. All ISM must be protected at the more restrictive of the following levels of classification:

a. The classification of the data stored on the ISM, including handling caveats and dissemination controls; or

b. The classification of the most restrictive data that can be accessed on the IS *security domain* in which the ISM has been used.

4. All ISM shall bear external *security labels* or markings indicating the most restrictive security classification at which it must be protected, in accordance with NSA/CSS Policy Manual 1-52, "NSA/CSS Classification Guide" (Reference d).

5. If an ISM used in a less restrictive security domain is subsequently used in a more restrictive security domain, it permanently assumes the sensitivity of the more restrictive domain and must be relabeled to reflect the more restrictive classification or security requirements. See paragraph 9 for guidance specific to optical ISM.

6. ISM labeled for use in a more restrictive IS security domain shall not be used in a less restrictive IS security domain. Data that is classified at a less restrictive level than an IS security domain may be written to a brand-new ISM without taking on the more restrictive requirements of the IS security domain only after completion of the steps described in paragraph 32.

7. ISM users shall scan removable media each time it is used in an NSA/CSS IS using current *NSA/CSS Enterprise Solutions Baseline*-approved anti-malware software, in accordance with NSA/CSS Policy 6-7, "Malware Incident Prevention and Handling" (Reference e).

8. The use of ISM that are considered to be removable media (e.g., optical discs, thumb drives, SD cards) shall be in accordance with NSA/CSS Policy Instruction 6-0004, "Using Removable Media for Data Transfer on NSA/CSS Information Systems" (Reference f). Given the restrictions of this policy and the destructive nature of the ISM *sanitization* techniques outlined in NSA/CSS Policy Manual 9-12, "NSA/CSS Storage Device Sanitization Manual" (Reference g), a magnetic or solid-state ISM may only be used for a single data transfer between security domains of differing classification levels. Any requests for *exception* to this restriction must follow the requirements in paragraph 33. See paragraph 9 for guidance specific to optical ISM.

9. Optical storage media (e.g., CD, DVD) labeled for a less restrictive IS security domain may be used in an IS of a more restrictive IS security domain without a change to the optical ISM classification status provided the user can confirm that the optical storage drive in the more restrictive IS is read-only. If the user cannot confirm that the optical storage drive in the more restrictive IS is read-only, then the optical ISM must assume the classification/sensitivity of the most restricted information processed on that system and the ISM must be relabeled accordingly.

10. Under no circumstances shall personally-owned or -produced media (e.g., music CDs) be used in any classified or unclassified NSA/CSS IS or network.

11. Classified ISM from a controlled facility can be released to an uncontrolled facility for recycling or disposal only after it has been sanitized and then administratively declassified in accordance with ICS 500-18, "Removable Media Management" (Reference a), and Reference g. The release of an ISM is an administrative risk decision that can only be made after all sanitization procedures have been successfully completed.

12. Classified ISM may be used to transport information between NSA/CSS-controlled areas according to the guidance in NSA/CSS Policy 5-25, "Hand-Carrying Classified Material" (Reference h).

13. Continual administrative declassification and release of ISM that is a requirement of an organization's daily mission shall be documented and maintained as part of the *System Security Plan (SSP)* for the system(s) in question.

14. ISM that is categorized as a restricted item per the requirements of NSA/CSS Policy Manual 5-23, "Physical Security Requirements for Controlled Areas Manual" (Reference i), must be approved by an appropriate *Information System Security Manager (ISSM)* ("go issm") and Security and Counterintelligence prior to being introduced into an NSA/CSS sensitive compartmented information facility (SCIF).

PROCEDURES

Labeling ISM

15. ISM must be labeled with a color-coded *security label* or otherwise marked to clearly identify the approved classification level of the ISM. Color-coded security labels (Standard Forms 706 through 712) may be ordered through the supply system or by contacting an appropriate *Information System Security Officer (ISSO)* ("go isso").

16. Security labels shall be affixed to all ISM in a manner that does not adversely affect proper operation of media devices or drives.

17. Optical storage media shall have the approved classification level written in permanent marker on the media itself. Color-coded security labels may be affixed to the external cases.

18. ISM that is too small to reasonably attach a security label to may be otherwise marked in a manner that clearly indicates the classification of the ISM. For example:

a. A microSD card could be marked with a serial number that corresponded to a number on its case, and the classification of the media could be marked on the case.

b. A USB flash drive could have a lanyard affixed to it, and the classification of the drive could be marked on the lanyard.

19. Unlabeled ISM still in the vendor's original packaging (i.e., shrink-wrap) shall be treated as unclassified.

20. Unlabeled ISM that is not in the manufacturer's original package shall be stored and protected at the classification level of the facility to minimize the possibility of compromise to classified or sensitive information. Users should contact their local facility *mission security officer (MSO)* ("go msos") with questions about storage of classified information.

Sanitizing and administratively declassifying ISM

Unclassified ISM

21. Unclassified ISM never used in a classified IS, and not containing for official use only (FOUO) information, Privacy Act information, or *personally identifiable information (PII)*, does not require sanitizing.

22. Unclassified ISM never used in a classified IS, and containing FOUO, Privacy Act, or PII data shall be sanitized before release for disposal or recycling to properly protect the information in accordance with Reference d and NSA/CSS Policy 1-22, "Protecting Privacy on NSA/CSS Electronic Information Systems" (Reference j).

23. Personally-produced unclassified music CDs must remain in the workplace and must be disposed of through the special burn process when no longer needed, in accordance with Reference i.

Sanitizing ISM

24. Requests for sanitization of ISM must be authorized by the requestor's supervisor/government lead, the appropriate ISSO ("go isso"), and the appropriate system owner.

25. Media that has ever contained classified information, other than communications security (COMSEC) material, shall be sanitized using the destruction procedures specified in Reference g. Media that has ever contained COMSEC material shall be destroyed using the procedures specified in CNSSI 4004.1, "Destruction and Emergency Procedures for COMSEC and Classified Material" (Reference k). If the COMSEC status of the information is unknown, the media shall be sanitized using the more destructive sanitization procedure of those listed for that media type in Reference g or Reference k.

26. Methods for the sanitizing of classified ISM will be different for magnetic, solid state, and optical storage devices. Instructions for each type are provided in Reference g.

27. At the completion of the sanitization process, all labels or markings that indicate previous use or data classification shall be removed.

Administrative Declassification

28. Administrative declassification of ISM may only be authorized by an appropriate ISSO ("go isso"), the requestor's supervisor/government lead, and the system owner upon successful completion of sanitization procedures.

29. Administrative declassification of ISM shall be recorded by the ISSO and shall include the following:

a. A description of the media (type, manufacturer, model number, serial number);

b. The classification of the data on the media;

c. A description of the sanitization procedures;

d. The name(s) of the individual(s) executing the procedures (e.g., data transfer agent (DTA)/ISSO/system administrator) as well as the names of at least two individuals who have verified the results. Individual(s) executing the procedures may also be included as the individuals verifying the results;

e. The detailed reason for the release;

f. The intended recipient of the ISM; and

g. The date of administrative declassification approval.

30. If an ISM cannot be sanitized, it must not be administratively declassified or released from an NSA/CSS-controlled facility, and must be maintained or destroyed in accordance with Reference g.

Release of ISM

31. Classified magnetic and solid state ISM may be released from an NSA/CSS-controlled facility to an environment *not controlled* by NSA/CSS only if the ISM meets the following conditions:

a. The ISM is capable of being sanitized;

b. The sanitization process has been successfully completed in accordance with this policy and Reference g;

c. The administrative declassification process has been documented and approved by the appropriate supervisor/government lead, ISSO, and system owner; and

d. The ISM is relabeled, if applicable, in accordance with requirements in this policy and Reference g.

32. Data of a less restrictive classification produced on a classified IS may be written to a new, never-used ISM in accordance with the NSA/CSS Data Transfer Agent process ("go dta"). This ISM may then be labeled UNCLASSIFIED, CONFIDENTIAL, or SECRET, as appropriate. The requestor must obtain documented authorization from their supervisor/government lead and an appropriate ISSO ("go isso"). The requestor should consult a *Classification Advisory Officer (CAO)* about proper classification and marking of the data being transferred. However, it is ultimately the responsibility of the requestor to ensure that the classification of the information is consistent with the classification constraints of the system to which the data is being transferred. If UNCLASSIFIED data is intended for public release, the requestor must request a prepublication review in accordance with NSA/CSS Policy 1-30, "Review of NSA/CSS Information Intended for Public Release" (Reference l).

Exceptions

33. Organizations requesting an exception to this policy will submit a formal written request to the appropriate ISSO ("go isso") for review. The ISSO will then forward the request to the NSA/CSS Deputy *Authorizing Official (AO)* for a decision. Exception decisions will be made on a case-by-case basis. The Deputy AO will notify the Security and Counterintelligence Group of all exceptions granted. The appropriate ISSO shall review exceptions annually. If the exception is still required, an updated request must be submitted to the Deputy AO.

RESPONSIBILITIES

Directors, Cryptologic Center Commanders/Chiefs, and Service Cryptologic Component Commanders

34. The Directors, Cryptologic Center Commanders/Chiefs, and Service Cryptologic Component Commanders shall establish procedures to provide oversight for, and ensure proper control of, all ISM under their purview.

Security and Counterintelligence Group

35. The Security and Counterintelligence Group shall:

a. Render documented decisions, in coordination with appropriate ISSMs, on requests for the introduction/removal of restricted ISM to/from an NSA/CSS SCIF.

b. Conduct counterintelligence IS security incident reviews for incidents involving ISM and coordinate, as appropriate, with the Office of the Inspector General (OIG), the appropriate ISSO, the NSA/CSS Information Systems Incident Response Team (NISIRT), and the Office of the General Counsel.

NSA/CSS Deputy Authorizing Official (AO)

36. The NSA/CSS Deputy Authorizing Official (AO) shall:

a. Render documented decisions on requests for exceptions to this policy; and

b. Inform the Security and Counterintelligence Group of any approved exception requests.

Supervisors and Government Leads

37. Supervisors (for government personnel) and government leads (for contractor employees) shall:

a. Render documented decisions, in coordination with the appropriate ISSO and system owner, on requests to sanitize ISM;

b. Determine the requirement for ISM under their purview to be administratively declassified and/or released based on mission and operational need;

c. Render documented decisions, in coordination with the appropriate ISSO and system owner, on requests by subordinates to administratively declassify and/or release ISM under their purview; and

d. Coordinate with the appropriate ISSO to review requests by subordinates for data transfers using removable media.

Information System Security Managers (ISSMs)

38. Information System Security Managers (ISSMs) shall:

a. Render documented decisions, in coordination with Security and Counterintelligence, on requests for the introduction/removal of restricted ISM to/from an NSA/CSS SCIF; and

b. Review all computer security incident reports (CSIRs) related to sanitized, declassified, and/or released ISM to determine possible impact on the integrity of data on systems under their purview and inform the Security Health Officers (SHO) of any such impact.

Information System Security Officers (ISSOs)

39. Information System Security Officers (ISSOs) shall:

a. Render documented decisions, in coordination with the appropriate supervisor and system owner, on requests to sanitize media for systems under their purview;

b. Render documented decisions, in coordination with the appropriate supervisor and system owner, on requests to administratively declassify and/or release ISM under their purview;

c. Ensure that the release of ISM under their purview is in accordance with this policy;

d. Coordinate with the requestor's supervisor/government lead to review requests for data transfers using removable media and systems under their purview;

e. Ensure users of systems under their purview comply with this policy and the procedures implementing it through education, awareness, and random physical inspections of ISM to ensure that all ISM is labeled in accordance with this policy and Reference a;

f. Review requests for exceptions to this policy and forward to the NSA/CSS Deputy AO for decision. Any approved exceptions must be reviewed annually for continued need. If the exception is still required, an updated request must be submitted to the Deputy AO for decision;

g. Review any approved exceptions annually for continued need. If the exception is still required, an updated request must be submitted to the Deputy AO for decision;

h. Ensure that Deputy AO-approved requests for exceptions are documented in the appropriate SSP;

i. Perform, or supervise the performance of, sanitizing of ISM under their purview in accordance with Reference g, this policy, and its administrative declassification procedures; and

j. Maintain a copy of the administrative declassification/release authorization pertaining to ISM under their purview.

System Owners

40. System owners shall:

a. Render documented decisions, in coordination with the appropriate supervisor and ISSO, on requests to sanitize media for systems under their purview; and

b. Render documented decisions, in coordination with the appropriate supervisor and ISSO, on requests to administratively declassify and/or release ISM associated with systems under their purview.

Center for Storage Device Sanitization Research

41. The Center for Storage Device Sanitization Research shall provide technical guidance for the sanitization and/or destruction of ISM (Reference g).

REFERENCES

a. Intelligence Community Standard (ICS) 500-18, "Removable Media Management," dated 16 February 2011

b. Committee on National Security Systems Policy (CNSSP) No. 26, "National Policy on Reducing the Risk of Removable Media for National Security Systems," dated May 2013

c. Department of Defense Instruction (DoDI) 8500.01, "Cybersecurity," dated 14 March 2014

d. NSA/CSS Policy Manual 1-52, "NSA/CSS Classification Guide," dated 2 June 2015

e. NSA/CSS Policy 6-7, "Malware Incident Prevention and Handling," dated 4 January 2017

f. NSA/CSS Policy Instruction 6-0004, "Using Removable Media for Data Transfer on NSA/CSS Information Systems," dated 19 February 2016

g. NSA/CSS Policy Manual 9-12, "NSA/CSS Storage Device Sanitization Manual," dated 15 December 2014

h. NSA/CSS Policy 5-25, "Hand-Carrying Classified Material," dated 16 December 2014

i. NSA/CSS Policy Manual 5-23, "Physical Security Requirements for Controlled Areas Manual," dated 20 May 2013

j. NSA/CSS Policy 1-22, "Protecting Privacy on NSA/CSS Electronic Information Systems," dated 9 January 2012

k. Committee on National Security Systems Instruction (CNSSI) 4004.1, "Destruction and Emergency Procedures for COMSEC and Classified Material," dated August 2006, with Annex B as amended, dated 24 October 2008

l. NSA/CSS Policy 1-30, "Review of NSA/CSS Information Intended for Public Release," dated 13 May 2015

GLOSSARY

administrative declassification—The process of recording information about the sanitization of information storage media (ISM). This information must be recorded before sanitized media may be released from an NSA/CSS-controlled facility (e.g., for destruction or recycling). These steps are authorized and performed by an information systems security officer (ISSO) and include recording the following information about ISM: a description of the media; classification of the data on the media (prior to sanitization); sanitation procedures; who performed the procedures; reason for release; intended recipient; and date of administrative declassification approval.

Authorizing Official (AO)—Senior (Federal) official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (Source: NSA/CSS Policy Glossary)

Classification Advisory Officer (CAO)—Individuals responsible for assisting their organizations to ensure that protected information is properly classified, marked, and safeguarded and that the employees in their organizations understand and properly apply classification rules and guidance. (Source: NSA/CSS Policy Glossary)

exception—Indicates that an implementation of one or more security requirements is temporarily postponed and that satisfactory mitigations for the requirement(s) may be used for a specified period of time. This is in contrast to a waiver that implies a security requirement has been set aside and need not be implemented at all. (Source: NSA/CSS Policy Glossary)

information storage media (ISM)—Data storage objects capable of being read from, or written to, by an IS to include, but not limited to, diskettes, optical disks, CDs, DVDs, thumb drives, and other removable media. Other terms for ISM include magnetic storage media, data storage media, or removable storage media.

information system (IS)—Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition/collection, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. IS examples are: stand-alone systems, Local Area Networks (LANs), supercomputers, process control computers that perform special purpose computing functions (e.g., Supervisory Control and Data Acquisition (SCADA), other Industrial Control Systems, embedded computer systems),

and the communications networks that disseminate information. (Source: NSA/CSS Policy Glossary)

information system security—The protection of information systems (ISs) against unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats. (Source: NSA/CSS Policy Glossary)

Information System Security Manager (ISSM)—Individual responsible for the information assurance of a program, organization, system, or enclave. (Source: NSA/CSS Policy Glossary)

Information Systems Security Officer (ISSO)—Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program. (Source: NSA/CSS Policy Glossary)

magnetic storage—Tapes, hard disk drives, diskettes, and other magnetic media which store data.

Mission Security Officer (MSO)—A professional Security Officer assigned to a Directorate, Associate Directorate, or major office, to provide full-range security guidance and assistance to senior management, supervisors, and all personnel within the assigned organization.

NSA/CSS Enterprise Solution Baseline—A common suite of enterprise approved standard hardware and software products that support corporate goals to reduce IT complexity, improve collaboration through interoperability, improve information system security, and manage IT costs. (Source: NSA/CSS Policy Glossary)

optical storage—Compact Disks (CD), Digital Versatile Disks (DVD), and other optical removable media (i.e., Blu-Ray, Holographic) which store data. (Source: NSA/CSS Policy Glossary)

personally identifiable information (PII)—Information which can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information which is linked or linkable to a specified individual. (Source: NSA/CSS Policy Glossary)

release—Final authorization given by the ISSO to allow ISM to leave an NSA/CSS-controlled facility. Classified media may only be released after approved sanitization and administrative declassification procedures have been completed.

sanitization—The removal of information from the storage device such that data recovery using any known technique or analysis is prevented. Sanitization includes the removal of data from the storage device, as well as the removal of all labels, markings, and activity logs. The method of sanitization varies depending upon the storage device in question, and may include degaussing, incineration, shredding, grinding, embossing, etc. (Source: NSA/CSS Policy Glossary)

security domain—A domain that implements a security policy and is administered by a single authority. (Source: CNSSI 4009)

security label—Information that represents or designates the value of one or more security relevant attributes (e.g., classification) of a system resource. (Source: CNSSI 4009)

solid state storage—Random access memory (RAM), read-only memory (ROM), field programmable gate array (FPGA), and smart cards which store data (solid state storage includes thumb drives and other portable flash memory). (Source: NSA/CSS Policy Glossary)

system security plan (SSP)—The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. (Source: NSA/CSS Policy Glossary)

DOCUMENT HISTORY

Date	Approved by	Description
9 June 2017	Gregory L. Smithberger, NSA/CSS Chief Information Officer	Policy issuance; supersedes NSA/CSS Policy 6-22 dated 27 May 2015
21 November 2019	Chief, Policy	An administrative update to incorporate accessibility enhancements