Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Standard

Office Instruction:	**CSO-STD-2004**
Office Instruction Title:	**Electronic Media and Device Handling Standard**
Revision Number:	**2.0**
Effective Date:	**December 31, 2019**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-STD-2004, “Electronic Media and Device Handling Standard,” provides standards for electronic media handling for all information sensitivity levels.
Training:	As requested

Approvals			
Primary Office Owner	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)	**Signature**	**Date**
SWG Chair	Bill Bauer	/RA/	12/9/19
CISO	Jonathan Feibus	/RA/	12/10/19

TABLE OF CONTENTS

List of Tables

Computer Security Standard
CSO-STD-2004

Electronic Media and Device Handling Standard

1 PURPOSE

CSO-STD-2004, "Electronic Media and Device Handling Standard," provides the minimum requirements for all electronic media and devices storing all sensitivity levels of non-public Nuclear Regulatory Commission (NRC) information. These requirements serve to minimize the probability of NRC information compromise. In addition to supporting good computer security practices, this standard supports the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27002, "Information technology — Security techniques — Code of practice for information security management," the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," and Committee on National Security Systems Policy (CNSSP) No. 26, "National Policy on Reducing the Risk of Removable Media for National Security Systems."

This standard is intended for:

- NRC authenticated users of NRC computing resources who must comply with the requirements in this standard.
- System owners, system administrators, and Information System Security Officers (ISSOs) who have the required knowledge, skills, and abilities to apply the requirements within this standard.

2 INTRODUCTION

Electronic media (also referred to as removable media) is frequently small and often disposable and allows for easy access and viewing of data via an electronic device (e.g., personal computers, servers) in secured locations. However, malware can also be transferred using removable media, and removable media use sometimes results in sensitive information being transferred to systems not authorized to process that level of information sensitivity. As a result, both users and system owners have a role in protecting the data contained on the media. All electronic media needs to be protected from unauthorized disclosure, modification, removal, and destruction. Electronic media can be active or passive:

- Active Electronic Media: Provides the ability to manipulate information (e.g., hard drives, Universal Serial Bus [USB], memory sticks [thumb drives]).
- Passive Electronic Media: Provides a container for information storage (e.g., Compact Disks [CDs], Digital Video Disks [DVDs], Blu-Ray disks, magnetic tapes).

This standard defines the requirements for accessing, protecting, labeling, reusing, sanitizing, and destroying electronic media and devices containing sensitive information.

3 GENERAL REQUIREMENTS

This section addresses the general requirements that all users, system owners, system administrators, and ISSOs, who are authorized to administer, configure, or use electronic media or devices must comply with as the minimum set of controls.

Only electronic media approved for the specific information sensitivity or classification level shall be used for that information level. Use of electronic media for information processing must only be performed in locations authorized to process the level of information associated with the electronic media.

All electronic media and devices must be sanitized in accordance with Section 4.6, Sanitization of Electronic Media and Devices prior to excessing the media or devices. Electronic media and devices at the Safeguards Information (SGI) or classified information sensitivity level shall not be excessed.

All NRC-assigned Government Furnished Equipment (GFE) smartphones and tablets, and all international loaner smartphones, tablets,[1] and laptops[2] used for international travel must follow sanitization and quarantine requirements in accordance with Section 4.6.1, International Travel – Electronic Media Sanitization, and Section 4.6.2, International Travel – Electronic Media Quarantine.

3.1 Computer Security Incidents

Any suspected computer security incident affecting electronic media or devices (e.g., tampering, unauthorized use, loss, or theft) must be reported immediately to the NRC Computer Security Incident Response Team (CSIRT) via telephone at (301) 415-6666 or via email at CSIRT@nrc.gov.

3.2 Required Encryption

System owners shall ensure that electronic media and devices used to process and/or store non-public information that are outside of facilities approved by the Authorizing Official (AO) are configured with software that fully encrypts the entire storage media using full disk encryption in accordance with CSO-STD-2009, “Cryptographic Control Standard.” For example, electronic media and devices used at an employee’s home, or while traveling between NRC locations must be fully encrypted per the requirements stated above.

The only exception to this is use of a personally owned computer to run an approved remote access solution in accordance with CSO-STD-2105, “NRC User Remote Access and International Travel Security Standard.” In the case of Citrix Broadband Remote Desktop (BRD), information is not processed or stored on the personally owned computer, but rather on a Citrix server where images are transmitted to the user for viewing.

Thumb drives used for non-public information storage must automatically encrypt all information stored on the electronic device in accordance with CSO-STD-2009. This means when

[1] Further information and guidance on the usage of international loaner smartphones and tablets is provided within the NRC Service Catalog: https://drupal.nrc.gov/ocio/catalog/31187

[2] International loaner laptops are also referred to as NRC Loaner Mobile Desktop – International devices within the NRC Service Catalog, which provides further information and guidance on their usage: https://drupal.nrc.gov/ocio/catalog/247

information is placed on the electronic device, the electronic device automatically encrypts the information regardless of user configuration or intervention.

3.3 Managing Information Sensitivity Levels

Electronic media must be managed at the highest level of information the media is used to process, transmit, or store, and must only be used on equipment authorized for that level of information processing. For example:

- If writeable electronic media with a Sensitive Unclassified Non-Safeguards Information (SUNSI) sensitivity level is connected to a device (e.g., computer) that processes, stores, or transmits SGI as the highest sensitivity level, the media must then be considered SGI media whether or not the user believes SGI resides on the media.
- If electronic media with an SGI sensitivity level is connected to a device (e.g., computer) that processes, stores, and transmits only SUNSI information, the computer must then be considered SGI from that point forward whether or not the user believes SGI was transferred to the computer.

The only exception to this is when there is an information spill. An information spill occurs when SGI or classified information is placed on a system not authorized to process that information. In the case of an information spill, agency risk must be assessed and the appropriate action determined by Office of the Chief Information Officer (OCIO) Security Operations in concert with CSIRT, and the NRC Chief Information Security Officer (CISO) must be informed of the decision.

3.4 Managing Encrypted Electronic Media and Devices

Encryption provides a level of protection that permits users to take electronic media and devices with them while traveling to other locations. However, the media and devices may only be used in facilities approved to process the media sensitivity level, and the media and devices must be under the control of the individual at all times when outside of NRC facilities.

NRC protects various levels of sensitive information using encrypted electronic media:

- NRC authenticated users must manage all electronic media (active and passive) at the sensitivity level of the most sensitive information (based upon the level of the information in plaintext) with which the media has been used to store, transmit, or process and can only be used on networks and systems at the highest level of sensitivity of the information on the media.

  The exception to this is where an encrypted file is transmitted across networks or computers where the means to decrypt the file are not accessible on the lower sensitivity network/computer and where the file is to be decrypted on a separate computer. For example, an encrypted SGI file is transmitted across the Internet from a licensee to the NRC to be placed on removable media for transferring the encrypted file to a computer authorized to process SGI. Encryption and decryption keys only reside on computers authorized to process SGI.
- Encrypted electronic media control within NRC facilities must follow the control identified for the unencrypted sensitivity level. For example, encrypted SGI electronic media must

be controlled as SGI, and encrypted classified electronic media must be controlled as classified information.

- Encrypted electronic media that is introduced to a system (e.g., USB drive mounted to a device) must be scanned for malware as soon as the information on the media is decrypted. This requirement does not apply to resident media, such as a hard drive that is an integral part of a host workstation.

3.5 NRC-Approved Electronic Media and Devices

The NRC Technical Reference Model (TRM) identifies the technologies and commercial products that are considered appropriate technologies for use at NRC. Actual implementations must be authorized to operate by the AO. The following requirements apply to active electronic media:

- Only NRC-issued active electronic media approved in the TRM is permitted to be used with NRC equipment.
- Only NRC-issued active electronic media approved for use in non-NRC equipment may be used with non-NRC equipment.
- Active electronic media that is used to perform upgrades or install patches to systems and devices must be managed at the level of the system to which the media connects. For example, active media used to patch an SGI system must be labeled as SGI and only used for SGI systems and devices.

The active electronic media distributing office (the office that provides active media to an individual or group of individuals) is considered the media owner. For classified and SGI active electronic media, the media owner must track the media by unique identifier (preferably by serial number) and the identification of the individual to which the active media was provided.

3.6 Labeling Electronic Media

All electronic media and devices must be appropriately labeled with the highest sensitivity/classification level of information on the media. The label must be affixed to a surface on the media that is typically seen by users. Appendix C, Electronic Media and Device Labels, provides labeling requirements and label formats that must be applied to all electronic media and devices.

3.7 Human Readable Output

Human readable output from electronic media or devices must be labeled in accordance with marking requirements identified for paper documents of the sensitivity/classification level in:

- MD 12.2, “NRC Classified Information Security Program,” labeling requirements apply to all classified information output;
- MD 12.7, “NRC Safeguards Information Security Program,” labeling requirements apply to all SGI output; and

- "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information"[3] labeling requirements apply to all SUNSI output.

3.8 Reuse of Electronic Media and Devices

All electronic media and devices that meet the criteria for reuse must be sanitized prior to being reused for another purpose, in accordance with Section 4.5, Secure Reuse of Electronic Media and Devices.

3.9 Sanitization and Destruction of Electronic Media and Devices

System owners must ensure that all electronic media and devices are either sanitized of all sensitive information or destroyed before the media or device is either reused or leaves NRC control, in accordance with Section 4.6, Sanitization of Electronic Media and Devices and Section 4.7, Secure Destruction of Electronic Media and Devices.

4 SPECIFIC REQUIREMENTS

This section provides specific requirements for electronic media and devices.

4.1 Approval and Verification of Electronic Media and Devices

This section provides specific requirements for approval and verification of electronic media and devices for use at different information sensitivity/classification levels.

4.1.1 Classified Information

Electronic media used for classified information must:

- Have specific approval from the National Security Agency (NSA), the cognizant authority for classified electronic media;
- Have been purchased or acquired from authorized and trusted sources;
- Be scanned using an NRC authorized method before introducing the electronic media into any operational system (this must be performed each time before inserting the media into a system);
- Go through a verification process to ensure that the electronic media contains only the minimum files that are necessary, and that the files are authenticated and scanned so that they are free of malicious software. This must be completed prior to the media being inserted into a National Security System (NSS); and
- Go through a verification process authorized by NRC for Assured File Transfer using a non-networked, stand-alone machine.

[3] https://drupal.nrc.gov/sites/default/files/SUNSI-Policy-Procedures.pdf

Classified systems permitting use of electronic media must:

- Prohibit automatic execution of any content by electronic media unless specifically authorized by the NRC CISO; and
- Implement access controls (e.g., read/write protections) for the electronic media, as appropriate.

4.1.2 SGI

Electronic media used for SGI must have specific approval from the CISO, the cognizant authority for SGI electronic media.

4.1.3 SUNSI

Electronic media and devices used for SUNSI must have specific approval from the AO, the cognizant authority for SUNSI electronic media and devices.

4.1.4 Plaintext NRC Information

Electronic media or devices that contain plaintext NRC information must be protected according to the confidentiality sensitivity of the information stored on the media (e.g., classified, SGI, SUNSI). If an electronic device does not have any capability to store information except on removable media, only the removable media must be controlled.

4.2 Physical Protection of Electronic Media and Devices

All electronic media and devices (e.g., laptop) used for non-public information must be physically controlled when transported outside of an approved building or facility.

4.2.1 Classified Information

Encrypted classified electronic media are considered to be sensitive and must be physically protected using one of the following methods:

- Must be in the user's continuous personal possession;
- Must be in the possession of an equivalently cleared responsible designee; or
- Must be stored in a secure facility or container that is approved for classified national security information storage when not in use.

4.2.2 SGI

Encrypted SGI electronic media are considered sensitive and must be physically protected using one of the following methods:

- Must be in the user's continuous personal possession;
- Must be in the possession of an equivalently cleared responsible designee; or
- Must be stored in a secure facility or container that is approved for SGI storage by the Office of Administration (ADM), Division of Facilities and Security (DFS) when not in use.

4.3 Labeling Electronic Media and Devices

This section provides the specific requirements for labeling electronic media and devices. All electronic media and devices must be appropriately labeled according to the highest level of information with which the media or device has been used. The label must be affixed to a surface on the media that is typically seen by users. Label formats are provided in Appendix C, Electronic Media and Device Labels.

All unlabeled media and devices are assumed to contain information up to the SUNSI sensitivity level. When not in use, electronic media and devices that are a higher level of sensitivity than SUNSI and cannot be labeled due to their small size (e.g., microSD cards) must be stored in an approved container labeled with the appropriate sensitivity level.

4.3.1 Classified Information and SGI

All electronic media and devices that contain classified information or SGI must be appropriately labeled even if the media or device is encrypted.

4.3.1.1 Special Handling Caveats

A Special Access Program is established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level. The number of persons who have access to this information is reasonably small and commensurate with the objective of providing enhanced protection for the information involved. Where information on media has special handling caveats, the media must be labeled with those caveats. In addition, the labels must not be visible to others outside of spaces authorized for open storage of that information.

4.3.2 Plaintext (Other than SUNSI Plaintext)

Electronic media and devices that contain other than SUNSI plaintext must be marked with the sensitivity and classification level of the information on the media or device, and the label must be color-coded.

4.3.3 SUNSI

All electronic media and devices that contain SUNSI should be appropriately labeled, but labeling is not required.

4.3.4 Publicly Available Information

Since the default sensitivity level of unlabeled information is SUNSI, all electronic media or devices that only contain publicly available information should be labeled to ensure that sensitive information is not used with the media or device and that individuals know the media or device can be used with computers that do not have protections required for sensitive information.

4.3.5 Encrypted Electronic Media and Devices

Electronic media and devices that contain encrypted information, other than encrypted SUNSI, must:

- Be marked with the sensitivity and classification level of the information on the media or device, and
- Indicate that the information is encrypted.

When the media is outside facilities approved by NRC for sensitive information processing, the label should not readily indicate the information sensitivity to those without a need-to-know to avoid drawing attention to the media or device during transport. This allows the user to determine which systems the media or device is approved to connect to without notifying other individuals of the sensitivity of the information being protected. Appendix A provides specific labels that are used when transporting media outside of NRC facilities that are more obscure as to the content but that permit the user to know the sensitivity level of information on the device.

4.4 Loss or Compromise of Electronic Media and Devices

Whenever positive control of any electronic media or device is lost, or when the media or device is left unattended, the media or device is considered to be compromised, and must be handled as follows:

- Loss of positive control of electronic media or devices must be reported immediately to the CSIRT using secure means appropriate to the sensitivity of the information stored on the media or device. The CSIRT must notify the system owner to determine the impact of the loss and the required action to be taken via required secure means.
- Compromised active electronic media may be reinitialized by authorized personnel if a CISO-approved re-initialization process is available for the media. If this is not the case, the electronic media must be replaced and destroyed. Re-initialized and retired electronic media must only be reused at the same sensitivity level or higher, in accordance with Section 4.5, Secure Reuse of Electronic Media and Devices, or be destroyed in accordance with Section 4.7, Secure Destruction of Electronic Media and Devices.
- Failed electronic media must be destroyed according to the destruction required for the sensitivity level of the information stored on the electronic device, whether the information is in plaintext or encrypted.
- Electronic media must be sanitized prior to connecting to a computer system if there is a belief that the media may contain malicious code.

4.5 Secure Reuse of Electronic Media and Devices

The following sections provide the specific requirements for electronic media and device reuse (e.g., CDs, DVDs, Blu-Ray disks, thumb drives, hard drives, solid state drives [SSDs], printers, scanners, and computers).

4.5.1 Classified Information

Classified electronic media and devices must:

- Only be reused at the same classification level or higher; and
- Be sanitized prior to reuse.

Reuse procedures do not need to be performed when transferring classified electronic media or devices to other individuals with the required clearances and need-to-know the information contained on the equipment and material.

4.5.2 SGI

SGI electronic media or devices must:

- Only be reused at the SGI level or higher classification level; and
- Be sanitized prior to reuse.

Reuse procedures do not need to be performed when transferring SGI electronic media or devices to other individuals who have gone through the required background check and need-to-know the information contained on the electronic media or device.

4.5.3 SUNSI

Prior to reuse, all SUNSI electronic media and device containers for information storage must be sanitized. Reuse procedures do not need to be performed when transferring SUNSI electronic media or devices to other individuals with the required background check and need-to-know the information contained on the electronic media or device.

For example, a loaner NRC thumb drive could be returned to the OCIO Customer Service Center (CSC) after a user finishes use of the drive. The CSC would then be able to sanitize, re-format, and re-encrypt the thumb drive before it is loaned out again to a new user.

4.6 Sanitization of Electronic Media and Devices

Computers and other electronic media and devices often contain components for permanent storage (e.g., the hard drive on a laptop or desktop workstation). When these components fail or are removed because they are no longer needed (e.g., due to a surplus) or are obsolete, the media storage components (e.g., hard drive, flash card, SSD) must be sanitized or destroyed. Standard deletion and disk reformatting processes do not remove the information.

System owners shall ensure:

- Media and device sanitization actions are tracked, documented, and verified.
- Preparation of equipment and material for reuse or excess requires purging of all information from the equipment or material using NRC authorized removal methods.

If media or device sanitization is required and is not possible, the media or device must be destroyed in accordance with Section 4.7, Secure Destruction of Electronic Media and Devices.

4.6.1 International Travel – Electronic Media Sanitization

Following the completion of international travel, electronic media sanitization requirements apply for all NRC-assigned GFE smartphones and tablets, and all loaner smartphones, tablets, and laptops. Sanitization must be performed using an erase utility / method in accordance with Section 4.6.6, Erase Utility / Method.

Table 4.6-1 specifies whether sanitization is required.

Table 4.6-1: International Travel Sanitization Requirements

Electronic Media / Device Type	Sanitization Applicability
International Loaner Smartphone	**Must** occur following completion of international travel.
International Loaner Tablet	
International Loaner Laptop / NRC Loaner Mobile Desktop – International	
NRC-assigned GFE Smartphone	**Should** occur following completion of international travel.
NRC-assigned GFE Tablet	

4.6.2 International Travel – Electronic Media Quarantine

Following the completion of international travel to certain high-risk countries (per State Department country designations/clearance and through collaboration with the Office of Nuclear Security and Incident Response [NSIR] and Office of International Programs [OIP]), electronic media quarantine requirements apply. Based upon the electronic media / device type, further usage may be restricted solely to the high-risk countries.

Table 4.6-2 specifies the applicable quarantine requirements.

Table 4.6-2: International Travel Quarantine Requirements

Electronic Media / Device Type	Quarantine Requirements
International Loaner Smartphone	Following completion of international travel, **must** be quarantined with further use only permitted in certain high-risk countries (per State Department country designations and through collaboration with NSIR and OIP).
International Loaner Tablet	
NRC-assigned GFE Smartphone	
International Loaner Laptop / NRC Loaner Mobile Desktop – International	Following completion of international travel, **should** be quarantined with further use only permitted in certain high-risk countries (per State Department country designations and through collaboration with NSIR and OIP).
NRC-assigned GFE Tablet	

4.6.3 Classified Information

All classified electronic media and devices must be cleaned of all information using NSA-approved classified sanitization methods prior to reuse. If reuse of the electronic media at the same classification level or a higher classification level is not possible, the media must be destroyed.

4.6.4 SGI

All SGI electronic media and devices must be cleaned of all information using CISO-approved SGI sanitization methods for reuse. If reuse of the electronic media at the SGI level is not possible, the media must be destroyed.

4.6.5 SUNSI

All SUNSI electronic media and devices must be cleaned of all information using NRC authorized sanitization methods for reuse.

4.6.6 Erase Utility / Method

An erase utility / method is required to assist in securely sanitizing electronic media or device storage to minimize the ability to recover the data. The erase utility / method must meet the following requirements:

- Is approved for the level of information on the media or device
- Uses an overwrite algorithm in accordance with Department of Defense 5220.22M-STD with a minimum of 3 over-writes to the media
- Destroys files, including temporary files
- Destroys filenames
- Destroys directories
- Destroys free space
- When destroying free space, old filenames are overwritten, and slack space is destroyed
- Deletes the Windows swap/page file

Alternatively, the erase utility / method may use a cryptographic erase if it is permitted in accordance with all requirements, guidelines, and considerations specified in NIST SP 800-88, “Guidelines for Media Sanitization,” (as amended) that are found in the following sections:

- Section 2.6, Use of Cryptography and Cryptographic Erase
- Appendix D, Cryptographic Erase Device Guidelines

Note: Many hard drives and SSDs support cryptographic erase as an alternate approach to perform data sanitization.

4.7 Secure Destruction of Electronic Media and Devices

All electronic media and devices to be destroyed, except for optical media, must be provided to ADM/DFS for destruction and a receipt must be obtained from ADM/DFS for the media or device. System owners shall ensure media disposal actions are tracked, documented, and verified.

4.7.1 Classified Information

For destruction of classified electronic media and devices located in the regions:

- Electronic media and devices at the Secret level and below must be provided to the Division of Resource Management and Administration (DRMA) Security Advisor.
- Electronic media and devices above the Secret level must be provided to the Central Top Secret Control Officer or designated alternates.

For destruction of classified electronic media and devices located in all other locations:

- Electronic media and devices at the Secret level and below must be provided to the ADM/DFS Facilities Security Specialist responsible for destruction of classified Electronic media.
- Electronic media and devices above the Secret level must be provided to the Central Top Secret Control Officer or designated alternates.

4.7.2 SGI

For destruction of SGI electronic media and devices, located in the regions, the electronic media must be provided to the Division of Resource Management and Administration (DRMA) Security Advisor.

For destruction of SGI electronic media or devices located in all other locations, the electronic media or device must be provided to the ADM/DFS Facilities Security Specialist responsible for destruction of SGI electronic media and devices.

4.7.3 Optical Media Destruction

Optical media (CDs and DVDs) storing, up to and including, Secret information may be destroyed by any office using NSA approved devices, procedures, and instructions for optical media destruction. This information can be found at: https://www.nsa.gov/Resources/Everyone/Media-Destruction/. System owners who do not have approved optical media destruction devices must provide the optical media to ADM/DFS for destruction.

4.8 Determining Need for System Electronic Media Handling Procedures

System owners must determine whether a procedure that outlines the appropriate handling of system electronic media is needed. If procedures are needed, system owners must ensure these are developed and maintained. The procedures must include the following:

- Electronic media labeling instructions;
- Electronic media access restrictions and controls;
- Electronic media approved encryption methods and procedures;
- Electronic media sharing restrictions;
- Electronic media transport requirements;
- Electronic media record requirements for inventory, authorized users/holders/recipients; and
- Electronic media storage.

APPENDIX A. ACRONYMS

ADM	Office of Administration
ADP	Automatic Data Processing
AO	Authorizing Official
BRD	Broadband Remote Desktop
CD	Compact Disk
CISO	Chief Information Security Officer
CNSSP	Committee on National Security Systems Policy
CSC	Customer Service Center
CSIRT	Computer Security Incident Response Team
CSO	Computer Security Office
DFS	Division of Facilities and Security
DRMA	Division of Resource Management and Administration
DVD	Digital Versatile Disk
EB	Encrypted Blue
ER	Encrypted Red
EOS	Encrypted Orange Stripe
FRD	Formerly Restricted Data
GFE	Government Furnished Equipment
ISSO	Information System Security Officer
ISO/IEC	International Organization for Standardization and International Electrotechnical Commission
IT	Information Technology
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
NSA	National Security Agency
NSI	National Security Information
NSIR	Office of Nuclear Security and Incident Response
NSS	National Security System
OIP	Office of International Programs
RD	Restricted Data
SD	Secure Digital
SGI	Safeguards Information
SIM	Subscriber Identity Module
SP	Special Publication

SSD	Solid State Drive
STD	Standard
SUNSI	Sensitive Unclassified Non-Safeguards Information
TRM	Technical Reference Model
USB	Universal Serial Bus

APPENDIX B. GLOSSARY

Active Electronic Media	Media that has the ability to manipulate electronic information. Examples of active electronic media include hard drives, compact flash memory, Secure Digital (SD)/Subscriber Identity Module (SIM) cards, and USB memory sticks (thumb drives).
Classified Information	Information that has been determined pursuant to Executive Order 13526 or any predecessor Order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. Classified information includes the following which requires protection against unauthorized disclosure in the interest of national security: a. Restricted Data; b. Formerly Restricted Data; and c. National Security Information processed or produced by a system. Classified information is divided into two categories, plaintext classified information and encrypted classified information.
Code Word	A single word assigned a classified meaning by an appropriate authority to ensure proper security concerning intentions, and to safeguard information pertaining to actual, real-world military plans or operations classified Confidential or higher.
Cryptographic Erase	A method of sanitization in which the media encryption key for the encrypted target data is sanitized, making recovery of the decrypted target data infeasible.
Default Sensitivity Level	At NRC, the default sensitivity level is SUNSI. If electronic media or a device is not labeled, the media or device is assumed to have a SUNSI sensitivity level.
Device Label	A label affixed to an electronic device that indicates the highest level of sensitivity with which the device has been used.
Electronic Device	Any electronic equipment that has a storage device or persistent memory, including but not limited to computers, servers, personal data assistants, smartphones, routers, switches, firewall hardware and certain models of printers and copiers.

Electronic Media	All media on which electronic data can be stored, including but not limited to hard drives, magnetic tapes, diskettes, CDs, DVDs, and USB storage devices. This media can be located in any electronic device, including but not limited to, copiers, printers, computers, smartphones, and tablets.
Encrypted Text	Text that has been submitted to a reversible process whereby the text is rendered unintelligible.
Human Readable Output	Information that can be read and understood by people, as opposed to codes read by machines.
Information Sensitivity	The level of potential impact resulting from the compromise of the confidentiality, integrity, or availability of information. Sensitivity levels include, but are not limited to, the following levels: publicly available information, SUNSI, SGI, Confidential, Secret, and Top Secret.
Media Destruction	Obliteration of the media such that the media is no longer usable, and no information can be obtained from the media.
Media Label	A label affixed to media that indicates the highest level of sensitivity with which the media has been used.
Media Labeling	The determination of the highest level of sensitivity with which the media has been used and affixing the label that indicates that level.
Media Sanitization	The overwriting of sensitive information from electronic media such that data recovery is not possible. This includes removing all information labels, markings, and activity logs.
Non-Publicly Available Information	Information that must not be made available to the public based upon the sensitivity level assigned to the information. Examples of non-publicly available information include classified information, SGI, and SUNSI.
NRC Authenticated User	An individual who has been authorized access to or use of an NRC IT system for any reason (e.g., support of an agency mission or developing or maintaining an IT system).
Passive Electronic Media	Media that provides a container for electronic information storage and does not have the ability to manipulate information. Examples of passive electronic media include CDs, DVDs, and magnetic tapes.
Plaintext	Information that is not encrypted.
Positive Control	Sufficient control to be certain (to a certain degree) that no one else has accessed the media.
Publicly Available Information	Information that is or can be made available to the public based upon an NRC determination that the information can be made available to the public.

Resident Electronic Media	Media that resides on or is connected to a device (e.g., laptop, desktop workstation) upon system boot. Examples of resident media include laptop hard drives or solid-state drives, and removable hard drives attached to workstations. If resident media is disconnected (e.g., for removable media) following system boot, then it must no longer be considered resident media upon reconnection.
Removable Media	Media, including magnetic tapes and disc packs, on which data or information can be entered, held, and retrieved, and that are easily and quickly removed from automatic data processing (ADP) equipment.
Safeguards Information	Sensitive unclassified information that specifically identifies the detailed security measures of a licensee or an applicant that are designed to protect special nuclear material or to protect the physical location of certain plant equipment that is vital to the safety of production/utilization facilities. SGI is divided into two categories, plaintext SGI and encrypted SGI.
Sanitization	See Media Sanitization.
Sanitize	See Media Sanitization.
Sensitive Unclassified Non-Safeguards Information	Information that is generally not publicly available and encompasses a wide variety of categories (e.g., personnel privacy, attorney-client privilege, confidential source, etc.). SUNSI is divided into two categories, plaintext SUNSI and encrypted SUNSI.

APPENDIX C. ELECTRONIC MEDIA AND DEVICE LABELS

Table C-1 provides the electronic media and device labeling requirements and label formats required for use on all electronic media and devices to identify the highest overall sensitivity/classification level of information on the media or device. All labels may be scaled as necessary.

Table C-1: Electronic Media Labels

Sensitivity Level of Information	Requirements	Media/Device Label
Publicly Available Information		
Publicly Available Information	Since the default sensitivity/classification level of unlabeled information is SUNSI, all electronic media and devices that contain only publicly available information must be so labeled. The label format provided must be used to label media and devices containing only publicly available information.	
SUNSI		
SUNSI – Plaintext SUNSI	Since the default sensitivity/classification level of unlabeled information is SUNSI, electronic media and devices that contain SUNSI as the highest sensitivity of information do not have to be labeled. However, users are encouraged to label the media or device to avoid confusion. The label format provided should be used to label media and devices containing plaintext SUNSI.	
SUNSI – Encrypted SUNSI	Electronic media and devices that contain encrypted SUNSI as the highest sensitivity of information do not have to be labeled. However, users are encouraged to label the media or device to avoid confusion. The label format provided should be used to label media and devices containing encrypted SUNSI.	
SGI		
SGI – Plaintext SGI	All electronic media and devices that contain SGI as the highest sensitivity of information must be labeled as SGI. The label format provided must be used to label media and devices containing plaintext SGI.	
SGI - Encrypted SGI that will NOT be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted SGI as the highest sensitivity of information must be labeled as encrypted SGI. The label format provided must be used to label media and devices containing encrypted SGI that will not be transported outside NRC facilities.	

Sensitivity Level of Information	Requirements	Media/Device Label
SGI - Encrypted SGI that MAY be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted SGI as the highest sensitivity of information must be labeled as encrypted SGI. The label format provided must be used to label media and devices containing encrypted SGI that may be transported outside NRC facilities.	
Classified Information		
Confidential Information		
Confidential Information – Plaintext Genser Confidential NSI	All electronic media and devices that contain Genser Confidential NSI as the highest sensitivity of information must be labeled as Confidential information. The label format provided must be used to label media and devices containing plaintext Genser Confidential NSI.	
Confidential Information – Encrypted Genser Confidential NSI that will NOT be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Genser Confidential NSI as the highest sensitivity of information must be labeled as Encrypted Confidential NSI. The label format provided must be used to label media and devices containing plaintext Genser Confidential NSI that will not be transported outside NRC facilities.	
Confidential Information – Encrypted Genser Confidential NSI that will MAY be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Genser Confidential NSI as the highest sensitivity of information must be labeled as Encrypted Confidential NSI. The label format provided must be used to label media and devices containing encrypted Genser Confidential NSI that may be transported outside NRC facilities. The “EB” stands for “encrypted blue.”	
Confidential Information – Plaintext Confidential RD Information	All electronic media and devices that contain Confidential RD information as the highest sensitivity of information must be labeled as Confidential RD information. The label format provided must be used to label media and devices containing plaintext Confidential RD information.	
Confidential Information – Encrypted Confidential RD that will NOT be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Confidential RD information as the highest sensitivity of information must be labeled as encrypted Confidential RD information. The label format provided must be used to label media and devices containing encrypted Confidential RD information that will not be transported outside NRC facilities.	

Sensitivity Level of Information	Requirements	Media/Device Label
Confidential Information – Encrypted Confidential RD that will MAY be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Confidential RD information as the highest sensitivity of information must be labeled as encrypted Confidential RD information. The label format provided must be used to label media and devices containing encrypted Confidential RD information that may be transported outside NRC facilities.	**EBRD**
Confidential Information – Plaintext Confidential FRD Information	All electronic media and devices that contain Confidential FRD information as the highest sensitivity of information must be labeled as Confidential FRD information. The label format provided must be used to label media and devices containing plaintext Confidential FRD information.	**Confidential FRD**
Confidential Information– Encrypted Confidential FRD that will NOT be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Confidential FRD information as the highest sensitivity of information must be labeled as Encrypted Confidential FRD information. The label format provided must be used to label media and devices containing Encrypted Confidential FRD information that will not be transported outside NRC facilities.	**Encrypted Confidential FRD**
Confidential Information – Encrypted Confidential FRD that MAY be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Confidential FRD information as the highest sensitivity of information must be labeled as Encrypted Confidential FRD information. The label format provided must be used to label media and devices containing encrypted Confidential FRD that may be transported outside NRC facilities.	**EBFRD**
Secret Information		
Secret Information – Plaintext Genser Secret NSI	All electronic media and devices that contain Genser Secret National Security Information (NSI) as the highest sensitivity of information must be labeled as Secret information. The label format provided must be used to label media and devices containing plaintext Genser Secret NSI.	**Secret**
Secret Information – Encrypted Genser Secret NSI that will NOT be Transport Outside NRC Facilities	All electronic media and devices that contain encrypted Genser Secret NSI as the highest sensitivity of information must be labeled as Encrypted Secret NSI. The label format provided must be used to label media and devices containing encrypted Genser Secret NSI that will not be transported outside NRC facilities.	**Encrypted Secret**

Sensitivity Level of Information	Requirements	Media/Device Label
Secret Information – Encrypted Genser Secret NSI that MAY be Transport Outside NRC Facilities	All electronic media and devices that contain encrypted Genser Secret NSI as the highest sensitivity of information must be labeled as Encrypted Secret NSI. The label format provided must be used to label media and devices containing encrypted Genser Secret NSI that may be transported outside NRC facilities. The "ER" stands for "encrypted red."	
Secret Information – Plaintext Secret RD Information	All electronic media and devices that contain Secret RD information as the highest sensitivity of information must be labeled as Secret RD information. The label format provided must be used to label media and devices containing plaintext Secret RD information.	
Secret Information – Encrypted Secret RD that will NOT be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Secret RD information as the highest sensitivity of information must be labeled as encrypted Secret RD information. The label format provided must be used to label media and devices containing encrypted Secret RD information that will not be transported outside NRC facilities.	
Secret Information – Encrypted Secret RD that MAY be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Secret RD information as the highest sensitivity of information must be labeled as encrypted Secret RD information. The label format provided must be used to label media and devices containing encrypted Secret RD information that may be transported outside NRC facilities.	
Secret Information – Plaintext Secret FRD Information	All electronic media and devices that contain Secret FRD information as the highest sensitivity of information must be labeled as Secret FRD information. The label format provided must be used to label media and devices containing plaintext Secret FRD information.	
Secret Information – Encrypted Secret FRD that will NOT be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Secret FRD information as the highest sensitivity of information must be labeled as Encrypted Secret FRD information. The label format provided must be used to label media and devices containing Encrypted Secret FRD information that will not be transported outside NRC facilities.	
Secret Information – Encrypted Secret FRD that MAY be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Secret FRD information as the highest sensitivity of information must be labeled as Encrypted Secret FRD information. The label format provided must be used to label media and devices containing encrypted Secret FRD that may be transported outside NRC facilities.	

Sensitivity Level of Information	Requirements	Media/Device Label
Top Secret Information		
Top Secret – Plaintext Genser Top Secret NSI	All electronic media and devices that contain Genser Top Secret National Security Information (NSI) as the highest sensitivity of information must be labeled as Top Secret information. The label format provided must be used to label media and devices containing plaintext Genser Top Secret NSI.	
Top Secret – Encrypted Genser Top Secret NSI that will NOT be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Genser Top Secret NSI as the highest sensitivity of information must be labeled as Encrypted Top Secret NSI. The label format provided must be used to label media and devices containing plaintext Genser Top Secret NSI that will not be transported outside NRC facilities.	
Top Secret – Encrypted Genser Top Secret NSI that MAY be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Genser Top Secret NSI as the highest sensitivity of information must be labeled as Encrypted Top Secret NSI. The label format provided must be used to label media and devices containing encrypted Genser Top Secret NSI that may be transported outside NRC facilities. The “EOS” stands for “encrypted orange stripe.”	
Top Secret – Plaintext Top Secret RD Information	All electronic media and devices that contain Top Secret RD information as the highest sensitivity of information must be labeled as Top Secret RD information. The label format provided must be used to label media and devices containing plaintext Top Secret RD information.	
Top Secret – Encrypted Top Secret RD that will NOT be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Top Secret RD information as the highest sensitivity of information must be labeled as Encrypted Top Secret RD information. The label format provided must be used to label media and devices containing encrypted Top Secret RD information that will not be transported outside NRC facilities.	
Top Secret – Encrypted Top Secret RD that MAY be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Top Secret RD information as the highest sensitivity of information must be labeled as encrypted Top Secret RD information. The label format provided must be used to label media and devices containing encrypted Top Secret RD information that may be transported outside NRC facilities.	

Sensitivity Level of Information	Requirements	Media/Device Label
Top Secret – Plaintext Top Secret FRD Information	All electronic media and devices that contain Top Secret FRD information as the highest sensitivity of information must be labeled as Top Secret FRD information. The label format provided must be used to label media and devices containing plaintext Top Secret FRD information.	
Top Secret – Encrypted Top Secret FRD that will NOT be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Top Secret FRD information as the highest sensitivity of information must be labeled as encrypted Top Secret FRD information. The label format provided must be used to label media and devices containing Encrypted Top Secret FRD information that will not be transported outside NRC facilities.	
Top Secret – Encrypted Top Secret FRD that MAY be Transported Outside NRC Facilities	All electronic media and devices that contain encrypted Top Secret FRD information as the highest sensitivity of information must be labeled as Encrypted Top Secret FRD information. The label format provided must be used to label media and devices containing encrypted Top Secret FRD information that may be transported outside NRC facilities.	

CSO-STD-2004 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
04-Feb-10	1.0	Initial issuance	Distribution at ISSO forum and posting on CSO web page	Upon request
22-Nov-10	1.1	Added labeling information extracted from the MD 12.5 draft	Distribution at ISSO forum and posting on CSO web page	Upon request
13-Nov-12	1.2	Added media disposal and reuse. Updated to include information from CNSSP-26. Added new table for approvals. Clarified approval for electronic media used on NRC equipment and device labeling.	Distribution at ISSO forum and posting on CSO web page	Upon request
10-Jun-14	1.3	Added destruction requirements for SGI and classified information and sanitization requirements. Reorganized structure and improved clarity and conciseness of content.	Distribution at ISSO forum and posting on CSO web page	Upon request
10-Dec-19	2.0	Added specific requirements related to electronic media and international travel.	Post to OCIO/CSO website	Upon request
9-Sep-21	2.0	Errata update to include specific information related to SSD sanitization.	Post to OCIO/CSO website	Upon request