Nuclear Regulatory Commission
Computer Security Office
Computer Security Standard

Office Instruction:	**CSO-STD-2004**
Office Instruction Title:	**Electronic Media and Device Handling Standard**
Revision Number:	**1.2**
Effective Date:	**January 1, 2013**
Primary Contacts:	**Kathy Lyons-Burke, SITSO**
Responsible Organization:	**CSO/PST**
Summary of Changes:	CSO-STD-2004, "Electronic Media and Device Handling Standard," provides standards for electronic media handling for all levels of information.
Training:	As requested
ADAMS Accession No.:	ML100210148

Approvals				
Primary Office Owner	Policies, Standards, and Training		**Signature**	**Date**
Standards Working Group Chair	Bill Dabbs		**/RA/**	**14-Nov-12**
Responsible SITSO	Kathy Lyons-Burke		**/RA/**	**14-Nov-12**
CSO Standards DAA	CISO	Tom Rich	**/RA/**	**20-Nov-12**
	Director, OIS	Jim Flanagan	**/RA/**	**21-Nov-12**

TABLE OF CONTENTS

Computer Security Standard
CSO-STD-2004

Electronic Media and Device Handling

1 PURPOSE

The purpose of CSO-STD-2004, "Electronic Media and Device Handling Standard," is to provide the standard for electronic media and device handling for all levels of information. In addition to supporting good computer security practices, this standard supports International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27002, "Information technology — Security techniques — Code of practice for information security management"; National Institute of Standards and Technology (NIST) Special Publication 800-53, "Recommended Security Controls for Federal Information Systems and Organizations" controls MP-1, MP-2, MP-3, MP-4, MP-5, and MP-6; and Committee on National Security Systems Policy (CNSSP) No. 26, "National Policy on Reducing the Risk of Removable Media."

2 GENERAL REQUIREMENTS

Removable media offer a convenient way to transfer data between systems. However, removable media also transfer malware and sometimes results in sensitive information being transferred to systems not authorized to process that level of information sensitivity.

Electronic media and device handling requirements define steps for proper access, labeling, storage, transmittal, and removal of information on fixed and removable electronic media and devices. Electronic media can be passive (simply provides a container for information storage) or active (has the ability to manipulate information). Examples of passive electronic media include Compact Disks (CDs), Digital Versatile Disks (DVDs), and magnetic tapes. Examples of active electronic media include hard drives and Universal Serial Bus (USB) memory sticks (thumb drives). Electronic media are frequently small and often disposable and allow for the easy removal of data from secured locations. As a result, both users and system owners have a role in protecting the data contained on the media. All electronic media must be protected from unauthorized disclosure, modification, removal, and destruction. This document applies to all electronic media used for non-public NRC information storage. For additional information on authorized processes and methods, please contact the CSO.

This document represents the minimum requirements necessary for processing or handling electronic media and devices. However, an Information System Security Officer (ISSO) or system owner may need to exceed these requirements to address system specific risks.

Any suspected tampering, unauthorized use, loss, or theft of electronic devices must be reported to the Computer Security Incident Response Team (CSIRT) as soon as known. The CSIRT can be contacted at (301) 415-6666 or CS_IRT@nrc.gov.

3 SPECIFIC REQUIREMENTS

System owners shall ensure that electronic media and devices used to process and/or store NRC Sensitive Unclassified Non-Safeguards Information (SUNSI) outside of facilities approved by the Designated Approving Authority (DAA) to process sensitive information are configured with software that 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 Citrix business solution. Approved business solutions are identified on the Computer Security Office (CSO) web page (http://www.internal.nrc.gov/CSO/ApprovedBusinessSolutions.html). In the case of Citrix, 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.

All electronic media and devices that contain Safeguards Information (SGI) or classified information must be configured with software that fully encrypts the entire storage media in accordance with CSO-STD-2009, "Cryptographic Control Standard." The only exception to this is electronic media or devices that are used, stored, and never leave a facility that has been authorized for open storage of the information.

3.1 Media Sensitivity Level Determination

Electronic media must be managed at the level of information the media is used to process, transmit, or store. For example, if writeable electronic media with a SUNSI sensitivity level is connected to a 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. Likewise, if electronic media with an SGI sensitivity level is connected to a 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 where there is an information spill (placement of SGI or classified information on a system not authorized to process that information) whereby the impact to the agency of this approach is significant enough that the risk to agency operations warrants a cleanup measure be taken instead. This decision is made by the Senior IT Security Officer for Cyber Situational Awareness, Analysis, and Response in coordination with the NRC Chief Information Security Officer (CISO).

Only electronic media approved for the specific information sensitivity or classification level shall be used for that information level. Electronic media used for SGI and classified information must have a specific approval from the cognizant authority for that information. The CISO is the cognizant authority for SGI electronic media and the National Security Agency (NSA) is the cognizant authority for classified information electronic media.

Classified electronic media must be managed using equipment approved for that level of processing. SGI electronic media must be managed using SGI equipment. Electronic media used only for unclassified, non-SGI information must be managed using equipment authorized to process that level of information. Upgrades to active electronic media must be performed using computers operating at the same sensitivity level.

3.2 Management and Handling of Removable Electronic Media

The portable nature of electronic media increases the risk that sensitive or classified information can be intentionally or unintentionally removed from NRC protection and become compromised.

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 SGI and classified 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.

Only NRC-issued active electronic media approved in the Technical Reference Model (TRM) shall 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.

NRC non-public authenticated users are required to handle all media at the sensitivity level of the most sensitive information with which the media has been used and can only be used on networks and systems at the highest level of sensitivity.

Thumb drives used for SGI or classified storage must automatically encrypt all information stored on the electronic device in accordance with CSO-STD-2009, “Cryptographic Control Standard.” This means when information is placed on the electronic device, the electronic device automatically encrypts the information regardless of user configuration or intervention.

Electronic media that contains plaintext non-public NRC information must be protected according to the confidentiality sensitivity of the information stored on the media. If an electronic device does not have any capability to store information except on removable media, only the removable media must be controlled.

Portable, removable storage devices must be sanitized prior to connecting such devices to the computer system if there is a belief that the device may contain malicious code.

Electronic media used for classified information processing must:

- Have been purchased or acquired from authorized and trusted sources;
- Be scanned using an NRC authorized method before introducing the media into any operational systems (this must be performed each time before inserting the media into a system);
- Go through a verification process to ensure that the media contain 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.

Classified systems permitting use of removable media must:

- Prohibit automatic execution of any content by removable media unless specifically authorized by the NRC CISO; and

- Implement access controls (e.g., read/write protections) for the removable media, as appropriate.

3.3 Encrypted Electronic Media and Device Handling

NRC uses encrypted electronic media to protect various levels of sensitive information. The sensitivity of the media is the sensitivity of the highest level of information (sensitivity is determined based upon the level of the information in plaintext) stored on the media, and writeable electronic media must only be used with computers and computer equipment authorized to process that sensitivity of information. 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 (e.g., 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).

Encrypted electronic media control within NRC facilities must follow the control identified for the unencrypted sensitivity level. This means that, for example, encrypted SGI electronic media must be controlled as SGI, and encrypted classified electronic media must be controlled as classified information.

Encryption provides a level of protection that permits users to take electronic media and devices 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.

Encrypted electronic media that is introduced to a system, such as a 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.

3.3.1 Encrypted SGI Media

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.

The media or device must be physically controlled when transported outside of an approved building or facility in accordance with Management Directive (MD) 12.7, "NRC Safeguards Information Security Program" requirements for handling SGI (e.g., by wrapping or concealing the media or device).

3.3.2 Encrypted Classified Media

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.

The media or device must be physically controlled when transported outside of an approved building or facility in accordance with MD 12.2, "NRC Classified Information Security Program" requirements for special handling of classified information (e.g., by wrapping or concealing the media or device).

3.4 Electronic Media and Device Labeling

All electronic media and devices must be appropriately labeled and controlled according to the highest sensitivity of information with which the media or device has been used. The label must indicate the highest level of information with which the 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 A.

3.4.1 SGI and Classified Information

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

3.4.2 Publically Available Information

Electronic media or devices that only contain publicly available information must 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.

3.4.3 Unlabeled Media and Devices

The sensitivity level of unlabeled electronic media or devices is assumed to be SUNSI.

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.

3.4.4 Human-readable Output

All human-readable output from electronic media or devices must be labeled according to the highest level of information produced by the system in accordance with the following:

- MD 12.2 labeling requirements apply to all classified information output;
- MD 12.7 labeling requirements apply to all SGI output; and
- "NRC Policy for Handling, Marking, and Protecting Sensitive Unclassified Non-Safeguards Information" labeling requirements apply to all SUNSI output (see http://www.internal.nrc.gov/sunsi/pdf/SUNSI-Policy-Procedures.pdf).

3.4.5 Media and Devices Containing Plaintext

Electronic media and devices that contain other than SUNSI plaintext must be marked with the sensitivity and classification level of the media or device, and the label must be color-coded. Appendix A provides the labels that must be used.

3.4.6 Media and Devices Containing Encrypted Information

Electronic media and devices that contain encrypted information other than encrypted SUNSI must be marked with the sensitivity and classification level of the media or device and must indicate that the information is encrypted. In addition, the label should not indicate the information sensitivity to those without a need-to-know to avoid drawing attention to the media during transport. This allows the user to determine which systems the device or media are approved to connect to without notifying other individuals of the sensitivity of the information being protected.

Appendix A provides the labels that must be used.

3.5 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 shall 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 shall only be reused at the same sensitivity level or higher or be destroyed.
- 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.

3.6 Electronic Media Handling Procedures

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

3.7 Secure Reuse/Disposal of Electronic Media and Devices

The following sections describe the requirements for equipment and media reuse. Equipment includes all electronic media and devices (e.g., CDs, DVDs, thumb drives, hard drives, printers, scanners, and computers).

3.7.1 Sensitive Unclassified Non-Safeguards Information

Prior to excess or reuse, all storage media and equipment containing storage media must be sanitized. Reuse procedures do not need to be performed when transferring SUNSI equipment and material, including media, to other individuals with the required background check and need-to-know the information contained on the equipment and material.

3.7.2 Safeguards Information

SGI equipment and material, including media:

- Shall only be reused at the SGI level or higher classification level;
- Must be sanitized prior to reuse; and
- Must be destroyed if the equipment and material will no longer be used at the SGI or higher classification level.

Reuse procedures do not need to be performed when transferring SGI equipment and material, including media, to other individuals who have gone through the required background check and need-to-know the information contained on the equipment and material.

3.7.3 Classified Information

Classified information equipment and material:

- Shall only be reused at the same classification level or higher;
- Must be sanitized prior to reuse; and
- Must be destroyed if the equipment and material will no longer be used at the same classified information level or higher.

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

3.8 Sanitization of Electronic Media and Devices

Computers and other electronic devices and media often contain components for permanent storage (e.g., the hard drive on a 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) must be purged of all residual data or destroyed. Standard deletion and disk reformatting processes do not remove the information.

- System owners shall ensure media 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 for SUNSI.
- Preparation of equipment and material for reuse requires purging of all information from the equipment or material using CISO-approved removal methods for SGI. If reuse at the SGI level is not possible, the media or device must be destroyed.
- All classified information equipment and material must be purged of all information using NSA-approved classified information purging methods prior to reuse. If reuse at the same classification level or a higher classification level is not possible, the media or device must be destroyed.
- In some cases, it is not possible to remove the information contained on the equipment or material. In these cases, the equipment or material must be destroyed.

3.9 Secure Destruction of Electronic Media and Devices

All electronic media to be destroyed, except for the optical media exception listed in Section 3.9.1, shall be provided to ADM/DFS for destruction and a receipt shall be obtained from ADM/DFS for the material.

System owners shall ensure media disposal actions are tracked, documented, and verified.

3.9.1 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 Uniform Resource Locator (URL): http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml. System owners who do not have approved optical media destruction devices shall provide the optical media to ADM/DFS for destruction.

4 DEFINITIONS

Active Electronic Media	Media that has the ability to manipulate electronic information. Examples of active electronic media include hard drives, compact flash memory, SD/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: a. Restricted Data; b. Formerly Restricted Data; and c. National Security Information processed or produced by a system that requires protection against unauthorized disclosure in the interest of national security.
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.
Default Sensitivity Level	At NRC, the default sensitivity level is Sensitive Unclassified Non-Safeguards Information (SUNSI). If media or an electronic 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	Electronic devices are used for more than storage and include some type of electronic processing. Examples of electronic devices include computers, iPods, and MP3 players.
Electronic Media	Different types of data storage options. Electronic storage options change very quickly and include, but are not limited to, the following: hard drives (i.e., both internal and external); removable drives (e.g., external hard drives); CDs; DVDs; thumb drives; flash memory; SD/SIM cards; floppy disks; and magnetic tapes. This media can be located in any electronic device, including but not limited to, copiers, printers, computers, phones, and tablets.
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	Process to remove information from media such that data recovery is not possible. It includes removing all information labels, markings, and activity logs.
Non-Publicly Available Information	Information that shall not be made available to the public based upon the sensitivity level assigned to the information. Examples of non-publicly available information include SUNSI, Safeguards Information, Restricted Data, Formerly Restricted Data, and National Security Information.
Passive Electronic Media	Media that provides a container for electronic information storage and that does not have the ability to manipulate information. Examples of passive electronic media include CDs, DVDs, and magnetic tapes.
Positive Control	Sufficient control to be certain (to a certain degree) that no one else has accessed the media
Publicly Availability 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) 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 shall no longer be considered resident media upon reconnection.
Sanitization	See Media Sanitization
Sanitize	See Media Sanitization

5 ACRONYMS

ADM	Office of Administration
CD	Compact Disk
CISO	Chief Information Security Officer
CNSS	Committee on National Security Systems
CNSSP	Committee on National Security Systems Policy
CSIRT	Computer Security Incident Response Team
CSO	Computer Security Office
DAA	Designated Approving Authority
DFS	Division of Facilities and Security
DVD	Digital Versatile Disk
FRD	Formerly Restricted Data
ISSO	Information System Security Officer
ISO/IEC	International Organization for Standardization and International Electrotechnical Commission
MD	Management Directive
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSI	National Security Information
NSS	National Security System
RD	Restricted Data
SGI	Safeguards Information
SUNSI	Sensitive Unclassified Non-Safeguards Information
TRM	Technical Reference Model
URL	Uniform Resource Locator
USB	Universal Serial Bus

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

APPENDIX A Media Labels

The media must be labeled with the highest overall sensitivity/classification level of information on the media. The documents that reside on the media must be appropriately labeled in accordance with marking requirements identified for paper documents of the sensitivity/classification level.

A.1 Publicly Available Information

Since the default sensitivity/classification level of unlabeled information is SUNSI, all media that contains only publicly available information must be so labeled. The label format provided in Figure 1 shall be used to label media containing only publicly available information. The label may be scaled as necessary.

Figure 1: Label for Publicly Available Information

A.2 SUNSI Information

Since the default sensitivity/classification level of unlabeled information is SUNSI, media that contains SUNSI as the highest sensitivity of information does not have to be labeled. However, users are encouraged to label the media to avoid confusion. The label format provided in Figure 2 should be use to label media containing plaintext SUNSI. The label may be scaled as necessary.

Figure 2: Label for Plaintext SUNSI Information

Media that contains encrypted SUNSI as the highest sensitivity of information does not have to be labeled. However, users are encouraged to label the media to avoid confusion. The label format provided in Figure 3 should be use to label media containing encrypted SUNSI. The label may be scaled as necessary.

Figure 3: Label for Encrypted SUNSI Information

A.3 SGI Information

All media that contains SGI as the highest sensitivity of information must be labeled as SGI. The label format provided in Figure 4 shall be used to label media containing plaintext SGI. The label may be scaled as necessary.

Figure 4: Label for Plaintext SGI

All media that contains encrypted SGI as the highest sensitivity of information must be labeled as encrypted SGI. The label format provided in Figure 5 shall be used to label media containing encrypted SGI that will not be transported outside NRC facilities. The label format provided in Figure 6 shall be used to label media containing encrypted SGI that may be transported outside NRC facilities. The labels may be scaled as necessary.

Figure 5: Label for Encrypted SGI that will NOT be Transported Outside NRC Facilities

Figure 6: Label for Encrypted SGI that may be Transported Outside NRC Facilities

A.4 Classified Information

All media containing classified information must be labeled.

A.4.1 Confidential Information

All media that contains Genser Confidential National Security Information (NSI) as the highest sensitivity of information must be labeled as Confidential information. The label format provided in Figure 7 shall be used to label media containing plaintext Genser Confidential NSI. The label may be scaled as necessary.

Figure 7: Label for Plaintext Genser Confidential NSI

All media that contains encrypted Genser Confidential NSI as the highest sensitivity of information must be labeled as Encrypted Confidential NSI. The label format provided in Figure 8 shall be used to label media containing plaintext Genser Confidential NSI that will not be transported outside NRC facilities. The label format provided in Figure 9 shall be used to label media containing encrypted Genser Confidential NSI that may be transported outside NRC facilities. The “EB” stands for “encrypted blue.” The labels may be scaled as necessary.

Figure 8: Label for Encrypted Genser Confidential NSI that will NOT be Transported Outside NRC Facilities

Figure 9: Label for Encrypted Genser Confidential NSI that may be Transported Outside NRC Facilities

All media that contains Confidential Restricted Data (RD) information as the highest sensitivity of information must be labeled as Confidential RD information. The label format provided in Figure 10 shall be used to label media containing plaintext Confidential RD information. The label may be scaled as necessary.

Figure 10: Label for Plaintext Confidential RD Information

All media that contains encrypted Confidential RD information as the highest sensitivity of information must be labeled as encrypted Confidential RD information. The label format provided in Figure 11 shall be used to label media containing encrypted Confidential RD information that will not be transported outside NRC facilities. The label format provided in Figure 12 shall be used to label media containing encrypted Confidential RD information that may be transported outside NRC facilities. The labels may be scaled as necessary.

Figure 11: Label for Encrypted Confidential RD that will NOT be Transported Outside NRC Facilities

Figure 12: Label for Encrypted Confidential RD that may be Transported Outside NRC Facilities

All media that contains Confidential Formerly Restricted Data (FRD) information as the highest sensitivity of information must be labeled as Confidential FRD information. The label format provided in Figure 13 shall be used to label media containing plaintext Confidential FRD information. The label may be scaled as necessary.

Figure 13: Label for Plaintext Confidential FRD Information

All media that contains encrypted Confidential FRD information as the highest sensitivity of information must be labeled as Encrypted Confidential FRD information. The label format provided in Figure 14 shall be used to label media containing Encrypted Confidential FRD information that will not be transported outside NRC facilities. The label format provided in Figure 15 shall be used to label media containing encrypted Genser Confidential NSI that may be transported outside NRC facilities. The labels may be scaled as necessary.

Figure 14: Label for Encrypted Confidential FRD that will NOT be Transported Outside NRC Facilities

Figure 15: Label for Encrypted Confidential FRD that may be Transported Outside NRC Facilities

A.4.2 Secret Information

All media that contains Genser Secret National Security Information (NSI) as the highest sensitivity of information must be labeled as Secret information. The label format provided in Figure 16 shall be used to label media containing plaintext Genser Secret NSI. The label may be scaled as necessary.

Figure 16: Label for Plaintext Genser Secret NSI

All media that contains encrypted Genser Secret NSI as the highest sensitivity of information must be labeled as Encrypted Secret NSI. The label format provided in Figure 17 shall be used to label media containing plaintext Genser Secret NSI that will not be transported outside NRC facilities. The label format provided in Figure 18 shall be used to label media containing encrypted Genser Secret NSI that may be transported outside NRC facilities. The “ER” stands for “encrypted red.” The labels may be scaled as necessary.

Figure 17: Label for Encrypted Genser Secret NSI that will NOT be Transported Outside NRC Facilities

Figure 18: Label for Encrypted Genser Secret NSI that may be Transported Outside NRC Facilities

All media that contains Secret RD information as the highest sensitivity of information must be labeled as Secret RD information. The label format provided in Figure 19 shall be used to label media containing plaintext Secret RD information. The label may be scaled as necessary.

Figure 19: Label for Plaintext Secret RD Information

All media that contains encrypted Secret RD information as the highest sensitivity of information must be labeled as encrypted Secret RD information. The label format provided in Figure 20 shall be used to label media containing encrypted Secret RD information that will not be transported outside NRC facilities. The label format provided in Figure 21 shall be used to label media containing encrypted Secret RD information that may be transported outside NRC facilities. The labels may be scaled as necessary.

Figure 20: Label for Encrypted Secret RD that will NOT be Transported Outside NRC Facilities

Figure 21: Label for Encrypted Secret RD that may be Transported Outside NRC Facilities

All media that contains Secret FRD information as the highest sensitivity of information must be labeled as Secret FRD information. The label format provided in Figure 22 shall be used to label media containing plaintext Secret FRD information. The label may be scaled as necessary.

Figure 22: Label for Plaintext Secret FRD Information

All media that contains encrypted Secret FRD information as the highest sensitivity of information must be labeled as Encrypted Secret FRD information. The label format provided in Figure 23 shall be used to label media containing Encrypted Secret FRD information that will not be transported outside NRC facilities. The label format provided in Figure 24 shall be used to label media containing encrypted Genser Secret NSI that may be transported outside NRC facilities. The labels may be scaled as necessary.

Figure 23: Label for Encrypted Secret FRD that will NOT be Transported Outside NRC Facilities

Figure 24: Label for Encrypted Secret FRD that may be Transported Outside NRC Facilities

A.4.3 Top Secret

All media that contains Genser Top Secret National Security Information (NSI) as the highest sensitivity of information must be labeled as Top Secret information. The label format provided in Figure 25 shall be used to label media containing plaintext Genser Top Secret NSI. The label may be scaled as necessary.

Figure 25: Label for Plaintext Genser Top Secret NSI

All media that contains encrypted Genser Top Secret NSI as the highest sensitivity of information must be labeled as Encrypted Top Secret NSI. The label format provided in Figure 26 shall be used to label media containing plaintext Genser Top Secret NSI that will not be transported outside NRC facilities. The label format provided in Figure 27 shall be used to label media containing encrypted Genser Top Secret NSI that may be transported outside NRC facilities. The "EOS" stands for "encrypted orange stripe." The labels may be scaled as necessary.

Figure 26: Label for Encrypted Genser Top Secret NSI that will NOT be Transported Outside NRC Facilities

Figure 27: Label for Encrypted Genser Top Secret NSI that may be Transported Outside NRC Facilities

All media that contains Top Secret RD information as the highest sensitivity of information must be labeled as Top Secret RD information. The label format provided in Figure 28 shall be used to label media containing plaintext Top Secret RD information. The label may be scaled as necessary.

Figure 28: Label for Plaintext Top Secret RD Information

All media that contains encrypted Top Secret RD information as the highest sensitivity of information must be labeled as encrypted Top Secret RD information. The label format provided in Figure 29 shall be used to label media containing encrypted Top Secret RD

information that will not be transported outside NRC facilities. The label format provided in Figure 30 shall be used to label media containing encrypted Top Secret RD information that may be transported outside NRC facilities. The labels may be scaled as necessary.

Figure 29: Label for Encrypted Top Secret RD that will NOT be Transported Outside NRC Facilities

Figure 30: Label for Encrypted Top Secret RD that may be Transported Outside NRC Facilities

All media that contains Top Secret FRD information as the highest sensitivity of information must be labeled as Top Secret FRD information. The label format provided in Figure 31 shall be used to label media containing plaintext Top Secret FRD information. The label may be scaled as necessary.

Figure 31: Label for Plaintext Top Secret FRD Information

All media that contains encrypted Top Secret FRD information as the highest sensitivity of information must be labeled as Encrypted Top Secret FRD information. The label format provided in Figure 32 shall be used to label media containing Encrypted Top Secret FRD information that will not be transported outside NRC facilities. The label format provided in Figure 33 shall be used to label media containing encrypted Genser Top Secret NSI that may be transported outside NRC facilities. The labels may be scaled as necessary.

Figure 32: Label for Encrypted Top Secret FRD that will NOT be Transported Outside NRC Facilities

Figure 33: Label for Encrypted Top Secret FRD that may be Transported Outside NRC Facilities

A.5 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.