Cyber Security Technical and Management Requirements

Media Clearing, Purging, and Destruction (TMR-10)
October 10, 2007

Department of Energy (DOE) Order 205.1A, *Department of Energy Cyber Security Management*, charges Senior DOE Management to implement cyber security within their respective organizations, based on their determination, assessment, and documentation of DOE and program-unique threats and risks. In carrying out this charge, Senior DOE Management is required by the Order to develop a Program Cyber Security Plan (PCSP) that defines cyber security requirements for all subordinate organizations and programs. The Order requires that the PCSP requirements comply with the Federal Information Security Management Act (FISMA), Presidential directives and Executive orders, Office of Management and Budget (OMB) directives, Federal Information Processing Standards (FIPS), Departmental policies, and DOE Chief Information Officer (CIO) Cyber Security Technical and Management Requirements (TMRs). This TMR document provides Senior DOE Management general direction and minimum requirements for unclassified and National Security Systems to be used in preparing each PCSP.

This TMR document describes the major elements of sanitization (clearing, purging, and destruction) of electronic media, hardware, and devices and establishes a risk-based approach to sanitization that is to be covered in each PCSP. It also provides guidance for the Departmental implementation of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, *Guidelines for Media Sanitization*, elements of NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, and the National Security Agency Evaluated Products List. Senior DOE Management may specify and implement additional requirements in each PCSP to address specific risks, vulnerabilities, or threats within its operating units.

Cancellations

This TMR replaces DOE CIO Guidance CS-11, *Media Clearing, Purging, and Destruction Guidance*, dated January 2007.

Implementation

This document defines management and technical cyber security requirements to be incorporated into Senior DOE Management PCSPs within 90 days of the TMR issue date.

Requirements

TMR-10-1, Senior DOE Management Sanitization Policy

Senior DOE Management is responsible for developing and documenting in the PCSP, and implementing policies and procedures for performing sanitization (clearing, purging, or destroying) of electronic media, hardware, and devices for all operating units, programs, and systems. At a minimum, the Senior DOE Management PCSP is to address the following.

1. Maintenance on equipment and tools used for clearing, purging, and destruction is regularly scheduled and performed to ensure proper operation and calibration.

2. Processes for the handling and control of media, electronic devices, and hardware prior to clearing, purging, or destruction are documented and followed.

    a. Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. For example, overwriting is an acceptable method for clearing media.

    b. Purging is a level of media sanitization that removes data in such a way that it cannot be reconstructed and renders data unrecoverable by laboratory attack methods.

    c. Destruction is the result of actions taken to ensure that media cannot be reused as originally designed or intended and information is virtually impossible or prohibitively expensive to recover.

3. The sanitization procedures, software, equipment/tools, and special processes are identified, documented, and approved by the Designated Approving Authority (DAA).

4. The requirements for removing information from storage media, memory devices, and related hardware are to be included in the training and awareness program and reviewed with all users on a regular basis.

5. Personnel performing or verifying the clearing, purging, or destruction of storage media, memory devices, and other hardware are to be trained in equipment/tool operation, approved techniques, and procedures.

6. Completed purging processes are to be verified as follows:

    d. No fewer than 20 percent of the purged media are sampled on a random basis to verify that the purging process has been successfully completed.

    e. The verification is conducted by individuals other than those performing the purging processes.

    f. The completion and verification of the purging process is documented.

TMR-10-2, Procedures for Media Clearing, Purging, and Destruction

The Senior DOE Management PCSP is to document requirements and processes for the clearing, purging, and destruction of unclassified and classified media, storage devices, and other hardware for all operating units, programs, and systems. The PCSP is to address the minimum sanitization criteria and the processes described below.

1. Minimum Sanitization Criteria. Table 1, Table 2, and Table 3 outline the basic sanitization processes and tools based on different technologies and media types.

a. National Security Agency Central Security Service (NSA/CSS) Manual 130-2, *Media Declassification and Destruction Manual*, November 2000, or subsequent update may be used as a supplement for the applicable processes identified in the tables.

b. NIST SP 800-88, *Guidelines for Media Sanitization*, or subsequent update may be used as a supplement for the applicable processes identified in the tables.

c. Refer technologies and media types not listed in the tables or references to the DOE CIO for defining clearing, purging, and destroying processes.

2. Unclassified Storage Media Processes.

a. Storage media that has been used for Sensitive Unclassified Information (SUI) processing is tracked and controlled until it is purged or destroyed.

b. Storage media that has been used in unclassified processing of information where the confidentiality impact is moderate or high must be tracked and destroyed if the unclassified information is located in bad sectors or the storage media cannot be cleared or purged.

c. In addition to the clearing processes listed in Tables 1 through 3, processes to clear unclassified storage media are to include the following:

(1) Storage media hosting Government information is to be cleared if it will be reused by a potential user who has a different authority for access, including Need-to-Know.

(2) Only overwriting software and hardware that are compatible with the media to be overwritten are to be used. Care should be used to ensure a match of software and hardware to the media, considering the make, model, and manufacturing date of the media.

(3) One-pass overwrites are sufficient for clearing storage media that does not contain SUI.

(4) Individuals performing unclassified storage media clearing must certify and document successful completion of the process to include:

(a) Storage media unique identification (e.g., serial number, make, and model);

(b) The Information Type with the highest confidentiality impact hosted on the media prior to clearing;

(c) Purpose of clearing (e.g. reuse, release, etc.);

(d) The procedure used; and

(e) The date, the printed name, and signature of the certifying individual.

d. All unclassified storage media is to be approved for public release or purged if the media is to be released to the public domain without review. The media is to be purged if it is to be reused on a system containing information which has a Security Category (confidentiality, impact) less than its current use.

e. In addition to the purging processes listed in Tables 1 through 3, processes to purge unclassified storage media are to include the following:

(1) Individuals performing unclassified storage media purging must certify that the purging process has been successfully completed by affixing a label to the storage media. At a minimum, the label must document:

(a) Storage media unique identification (e.g., serial number, make, and model);

(b) The Information Type with the highest confidentiality impact hosted on the storage media prior to purging;

(c) Purpose of purging;

(d) The procedure used; and

(e) The date, printed name, and signature of the certifying individual.

(2) Storage media that cannot be purged must be destroyed

3. Classified Storage Media Processes.

a. Storage media that has been used in classified processing and is no longer being used or needed for archiving is tracked and controlled until it is destroyed, and the destruction is documented as required by the DOE Classified Matter Protection and Control (CMPC) program.

b. Decision and handling processes regarding reuse of classified storage media at lower classification level(s) include formal risk and cost analyses and testing and are documented and justified.

c. In addition to the clearing processes listed in Tables 1 through 3, processes to clear classified storage media are to include the following.

(1) Storage media that will be reused on a different system for the same or more restrictive Information Group or a potential user has a different Need-to-Know must be cleared.

(2) Only overwriting software and hardware that are compatible with media to be overwritten will be used.

(3) Cleared storage media that has been used in classified processing must be protected commensurate with the highest Information Group (i.e. classification level and category of information) it has ever contained. The media must be handled in accordance with applicable DOE CMPC processes.

(4) Individuals involved in clearing classified storage media must certify and document the successful completion of the process to include:

(a) Storage media unique identification (e.g., serial number, make, and model);

(b) Most restrictive Information Group hosted prior to clearing;

(c) Purpose for clearing;

(d) The procedure used; and

(e) The date, printed name, and signature of the certifying individual.

d. In addition to the purging processes listed in Tables 1 through 3 processes to purge classified storage media are to include the following.

(1) Classified storage media that will be reused at a less restrictive Information Group must be purged.

(2) Classified storage media that cannot be purged must be destroyed.

(3) Classified storage media that has been purged may not be donated, sold, etc. (i.e., released from the DOE environment) to outside organizations.

(4) Individuals performing purging of classified storage media must certify the process has been successfully completed by affixing a label to the storage media. At a minimum, the label must document:

(a) Storage media unique identification (e.g., serial number, make, and model);

(b) Most restrictive Information Group hosted prior to purging;

(c) Purpose of purging;

(d) A statement that the storage media contains no classified information;

(e) The procedure used; and

(f) The date, printed name, and signature of the certifying individual.

Table 1. Approved Processes for Clearing, Purging, and Destroying Storage Media

MEDIA TYPE	CLEARING‡	PURGING‡	DESTROYING‡
Magnetic Tapes			
Type I	1, 2, or 3	1, 2, 3, or 4	5
Type II	1, 2, or 3	2, 3, or 4	5
Type III	2 or 3	3 or 4	5
Magnetic Disks			
Floppies, Zip drives	1, 2, 3, or 4	X	5
Bernoulli Boxes	1, 2, 3, or 4	X	5
Removable Hard Disks	1, 2, 3, or 4	1, 2, 3, or 4	5 or 6
Non-removable Hard Disks	4	1, 2, 3, or 4	5 or 6
Optical Disks			
Magneto-optical: Read Only	X	X	5
Write Once, Read Many (WORM)	X	X	5
Read Many, Write Many	X	X	5
Other			
Floptical	X	X	5
Helical-scan Tapes	X	X	5
Cartridges	X	X	5
Optical	X	X	5
CD-R, -RW, -ROM	X	X	5 or 7
DVD	X	X	5 or 7
All other storage media	X	X	5

‡Numbers in the table refer to the processes listed.

Processes: †

1. Degauss with a Type 1 degausser.§
2. Degauss with a Type 2 degausser.§
3. Degauss with a Type 3 degausser.§
4. Overwrite all locations with a pseudorandom pattern twice and then with a known pattern.
5. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed.
6. Remove the entire recording surfaces by sanding or applying acid.
7. Grind surface of CD or DVD to ensure the entire recording surface is removed. Only NSA Group D equipment and associated processes approved for the specific media may be used.

X. No process authorized.

Table 2.
Approved Processes for Clearing, Purging, and Destroying Electronic Memory Devices

MEDIA TYPE	CLEARING‡	PURGING‡	DESTROYING‡
Magnetic Bubble Memory	2	1 or 2	9
Magnetic Core Memory	2	1 or 2	9
Magnetic Plated Wire	2	2 and 3	9
Magnetic-Resistive Memory	2	X	9
Read-Only Memory (ROM)	X	X	9 (see 10)
Random Access Memory (RAM) (Volatile)	2 or 4	4, then 8	9
Programmable ROM (PROM)	X	X	9
Erasable PROM (UV PROM)	5	5, then 2 and 8	9
Electrically Alterable PROM (EAPROM)	7	6, then 2 and 8	9
Electrically Erasable PROM (EEPROM)	2	7, then 2 and 8	9
Flash Erasable PROM (FEPROM)	7	7, then 2 and 8	9
All other storage media devices	X	X	9

‡Numbers in the table refer to the processes listed.

§All degaussing products used to clear or purge media **must** be appropriate to the type of media, certified by the National Security Agency (NSA), and listed on the Degausser Products List of the NSA *Information Systems Security Products and Services Catalogue*.

Processes: ‡

1. Degauss with a NSA approved Type III degausser§
2. Overwrite all locations with a pseudorandom pattern twice and then with a known pattern.
3. Purging is not authorized if data resided in same location for more than 72 hours; purging is not complete until each overwrite has resided in memory for a period longer than the classified data resided in memory.
4. Remove all power, including batteries and capacitor power supplies, from RAM circuit board.
5. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time requirements by a factor of 3.
6. Pulse all gates.
7. Perform a full chip purge/erase (see manufacturer's data sheet for procedure).
8. Check with ISSO to determine whether additional processes are required.
9. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed.
10. Destruction required only if ROM contained a classified algorithm or classified data.

X. No process authorized.

Table 3. Approved Processes for Clearing, Purging, and Destroying Hardware

MEDIA TYPE	CLEARING‡	PURGING‡	DESTROYING‡
Printer Ribbons	5	5	5
Platens	X	1	5
Toner Cartridges	4	4	X
Laser Drums	2	2	5
Cathode-Ray Tubes (If there is Classified Burn-In)	X	5	5
Fax Machines	3	3	5
Cell Phones	6	X	5
Personal Digital Assistant (PDA) (Palm, Pocket PC, etc)	6	X	5
Routers/ Copy machines	6	X	5
All other storage media devices	X	X	5

‡Numbers in the table refer to the processes listed.

Processes: †

1. Chemically clean so no visible trace of data remains.
2. Print three blank copies. If unable to get a clean output, print an unclassified test pattern or black copy; then run three blank copies.
3. For fax machines that have memory and other storage media incorporated, treat each component per processes listed in tables 1 and 2.
4. Upon completion of copying or facsimile processing of classified material, users are required to run one or multiple blank copies to ensure the removal of all classified materials from processing device.
5. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure the media is physically destroyed.
6. Manually delete all information, then perform a full manufacturers reset to reset the instrument back to factory default settings

X. Not applicable.

Note: All copies printed for clearing and purging purposes must be destroyed as classified waste.

TMR-10-3, Special Processes for Media Reuse

The Senior DOE Management PCSP is to document processes for the clearing, purging, and destruction of unclassified and classified media, storage devices, and other hardware intended for reuse for all operating units, programs, and systems. The PCSP is to address the applicable minimum criteria for reuse classified media in an unclassified environment and decontamination of unclassified media described below.

1. Reusing Classified Storage Media in an unclassified environment.
    a. Reuse of classified storage media must be identified in the System Security Plan (SSP) of the system where the media is used and the media must be tracked/controlled until it is purged or destroyed.

    b. The storage media is to be purged by overwriting the entire storage media using the three-pass overwrite process described in Table 1.

    c. The software used is to provide information about sectors overwritten and bad sectors that cannot be overwritten.

    d. Quality controls are to be documented and deployed for review of overwrite process results and verification that all the classified information was completely overwritten

    e. The storage media must be destroyed if classified information is located in bad sectors or the storage media cannot be purged.

    f. Individuals performing purging of the classified storage media planned for reuse must certify the process has been successfully completed by affixing a label to the storage media. At a minimum, the label must document:

        (1) Storage media unique identification (e.g., serial number, make, and model);

        (2) Most restrictive Information Group hosted prior to purging;

        (3) Purpose of purging;

        (4) A statement that the storage media contains no classified information;

        (5) The procedure used; and

        (6) The date, printed name, and signature of the Certification Agent.

2. Purging Partially Contaminated Storage Media.
    a. Areas of non-removable storage media partially contaminated with an information type of a higher confidentiality impact or more restrictive Information Group may

be purged using the three-pass process described in Table 1 and continue use in its current information system in the following situations:

(1) When unclassified storage media operated with a confidentiality impact of low or not applicable is contaminated with relatively small amounts of unclassified information with a confidentiality impact of moderate or high (non-Public) (less than 0.1 percent of the capacity of the non-removable storage media).

(1) When unclassified storage media is contaminated with relatively small amounts of classified information (less than 20 megabytes of information and less than 0.001 percent of the capacity of the non-removable storage media).

(2) When the classified storage media is contaminated with relatively small amounts of information from a more restrictive Information Group (less than 0.1 percent of the capacity of the non-removable storage media).

b. The software used to overwrite contaminated storage media must overwrite all contaminated locations, including temporary data file locations, file slack, free space, and directories; provide confirmation of overwrite of specified areas and of successful completion; and provide information about sectors overwritten and bad sectors that cannot be overwritten.

c. Quality controls are to be documented and deployed for review of overwrite process results and verification that all the contaminating information was completely overwritten.

d. The storage media must be destroyed if classified information is located in bad sectors or the storage media cannot be purged.

e. Records to be maintained, as a minimum, are

(1) Storage media serial number, make, and model;

(2) Contaminating Information Group;

(3) Purpose of purging;

(4) A statement that the storage media no longer contains the Information Group;

(5) The procedure used; and

(6) The date, printed name, and signature of the certifying individual.

TMR-10-4, Operating Unit Policies and Procedures

The Senior DOE Management PCSP is to direct operating units to develop, document, and implement policies and procedures for media clearing, purging, and destruction compliant with the requirements defined in the PCSP and commensurate with the level of security required for the organization's environment and specific needs.