MANUAL

DOE M 205.1-2

Approved: 6-26-05
Review: 6-26-07
Expires: 6-26-09

CLEARING, SANITIZATION, AND DESTRUCTION OF INFORMATION SYSTEM STORAGE MEDIA, MEMORY DEVICES, AND RELATED HARDWARE MANUAL

U.S. DEPARTMENT OF ENERGY

Office of the Chief Information Officer

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of the Chief Information Officer

CLEARING, SANITIZATION, AND DESTRUCTION OF INFORMATION SYSTEM STORAGE MEDIA, MEMORY DEVICES, AND RELATED HARDWARE MANUAL

1. PURPOSE. Ensuring confidentiality throughout the life cycle of Department of Energy (DOE) information and information systems is critical to the success of the Department's mission. This Manual establishes DOE requirements and responsibilities for clearing, sanitizing, and destroying DOE information system storage media, memory devices, and related hardware. This Manual will—

   a. Define and provide procedures for clearing, sanitization and destruction activities to ensure confidentiality appropriate to the processing of storage media, memory devices, and related hardware.

   b. Establish requirements for ensuring appropriate confidentiality to all information sensitivity levels.

2. CANCELLATIONS. DOE N 205.12, *Clearing, Sanitizing, and Destroying Information System Storage Media, Memory Devices, and Other Related Hardware,* dated 2-19-04. Cancellation of a directive does not by itself modify or otherwise affect any contractual obligation to comply with the directive. Canceled directives that are incorporated by reference in a contract remain in effect until the contract is modified to delete the references to the requirements in the canceled directives.

3. APPLICABILITY.

   a. Primary DOE Organizations, including National Nuclear Security Administration (NNSA) Organizations. Except for the exclusions in paragraph 3c, this Manual applies to all Primary DOE Organizations that own or operate DOE information systems or national security systems. See Attachment 1 for a complete list of Primary DOE Organizations. This Manual automatically applies to any Primary DOE Organizations created after the Manual is issued.

      The NNSA Administrator shall assure that NNSA employees and contractors comply with their respective responsibilities under this Manual.

   b. Site/Facility Management Contractors. Except for the exclusions in paragraph 3c, the Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Manual that will apply to site/facility management contractors whose contracts include the CRD.

      (1) The CRD must be included in site/facility management contracts that may involve automated access to DOE information systems (site/facility management contractors to which the CRD is intended to be applied are listed in Attachment 3).

      (2) This Manual does not automatically apply to other than site/facility management contractors. Any application of requirements of this Manual

to other than site/facility management contractors will be communicated separately.

(3) The Heads of Primary DOE Organizations are responsible for telling their appropriate contracting officers which site/facility management contractors are affected by this Manual. Once notified, contracting officers are responsible for incorporating the CRD into the laws, regulations, and DOE directives clause of affected site/facility management contracts.

(4) As the laws, regulations, and DOE directives clause of site/facility management contracts states, regardless of the performer of the work, site/facility management contractors with the CRD incorporated into their contracts are responsible for compliance with the requirements of the CRD.

(a) Affected site/facility management contractors are responsible for flowing down the requirements of this CRD to subcontracts at any tier to the extent necessary to ensure the site/facility management contractors' compliance with the requirements.

(b) Contractors must not flow down requirements to subcontractors unnecessarily or imprudently. That is, contractors will—

1 ensure that they and their subcontractors comply with the requirements of the CRD and

2 incur only costs that would be incurred by a prudent person in the conduct of competitive business.

c. Exclusions.

(1) Consistent with the responsibilities identified in Executive Order (E.O.) 12344, dated February 1, 1982, the director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE Manual for activities under the Deputy Administrator's cognizance.

(2) The requirements set forth in this Manual are not applicable to media that have been used to process Special Access Program (SAP) information or Sensitive Compartmented Information (SCI). Intelligence SAP information and SCI will adhere to more stringent program requirements as specified by the Director of Central Intelligence and promulgated into their security plans. Non-intelligence SAP information will be handled as

specified by Government program security officer as promulgated in program security manuals.

4. SUMMARY. This Manual is divided into two chapters that define requirements and responsibilities for clearing, sanitizing, and destroying DOE information system storage media, memory devices, and other related hardware. These chapters address mandatory procedures and management processes.

   a. Chapter I describes the requirements.

   b. Chapter II defines roles and responsibilities.

   c. Attachment 1 is a list of the Primary DOE Organizations to which this Manual is applicable.

   d. Attachment 2 is the CRD.

   e. Attachment 3 lists site/facility management contractors to which the CRD is intended to be applicable.

   f. Attachment 4 is a list of definitions pertinent to this Manual.

   g. Attachment 5 lists DOE-approved procedures for clearing, sanitizing, and destroying information system storage media, memory devices, and related hardware.

5. IMPLEMENTATION. Primary DOE Organizations and contractors must implement the requirements and meet the responsibilities defined in this Manual within 90 days of its issuance. The heads of Primary DOE Organizations will disseminate requirements and responsibilities to all organizational levels. In addition, as established by DOE O 205.1, *Department of Energy Cyber Security Management Program*, dated 3-21-03, paragraph 4d, the Program Cyber Security Plans (PCSPs), Cyber Security Program Plans (CSPPs), and their associated Security Plans must be developed, approved and maintained in accordance with this directive.

6. REFERENCES. The following references contain cyber security program requirements and guidance that may be helpful in implementing this Manual.

   a. E.O. 12829, National Industrial Security Program (January 6, 1993).

   b. E.O. 12958, Classified National Security Information, as amended (April 17, 1995).

   c. E.O. 12968, Access to Classified Information (August 2, 1995).

   d. E.O.13231, Critical Information Protection in the Information Age (October 16, 2001).

e. Homeland Security Presidential Directive 7 (HSPD-7), Critical Infrastructure Identification, Prioritization and Protection, (December 17, 2003).

f. National Industrial Security Operating Manual (NISPOM), dated January 1995.

g. National Institute of Standards and Technology Special Publication 800-53, Recommended Security Controls for Federal Information Systems, dated February 2005.

h. National Security Agency Central Security Service, Degausser Products List, February 17, 2004.

i. Office of Management and Budget Circular A-130, Revised, Management of Federal Information Resources, Appendix III, "Security of Federal Automated Information Resources," dated 11-30-00.

j. Public Law (P.L.) 106-65 National Nuclear Security Administration Act (October 6, 1999), as amended, established a separately organized agency within the Department of Energy.

k. P.L. 83-703, the Atomic Energy Act of 1954, as amended.

l. P.L. 89-487, the Freedom of Information Act of 1979, as amended by the Electronic Freedom of Information Act Amendments of 1996 (P.L. 104-231).

m. P.L. 93-438, the Energy Reorganization Act of 1974.

n. P.L. 93-579, the Privacy Act of 1974, as amended [5 U.S.C. § 552a].

o. P.L. 107-347, the E-Government Act of 2002, Title III, Federal Information Security Management Act of 2002 (FISMA), December 17, 2002.

7. CONTACT. Questions concerning this Manual should be addressed to the Office of the Chief Information Officer, 202-586-0166.

SAMUEL W. BODMAN
Secretary of Energy

CONTENTS

CHAPTER I. REQUIREMENTS

1. INTRODUCTION. This Manual addresses three activities that support the confidentiality security objective provided in the Federal Information Security Management Act of 2002 and reinforced in cited references: clearing, sanitization, and destruction. In keeping with sound fiscal management practices, DOE must conserve its information resources and reuse media when possible.[1] Each of these activities is used to meet the objectives of both resource conservation and maintaining confidentiality throughout the life cycle of the information.

   Clearing is utilized for processing media that will be reused at the same or higher classification levels and categories. Cleared media that contained classified or unclassified controlled information must be protected by measures commensurate with the highest level and any category of information the media ever contained. Clearing does not lower the classification levels or categories of the media. The media must retain classification labels/markings and controls. Any medium must be protected at the level and any category for which it is marked, even if it never contained information commensurate with the marking.

   Sanitization is utilized for media that will be reused at lower classification levels or categories, or released from classified or sensitive environments.

   Destruction is utilized for media that are no longer being used or that contains or formerly contained classified or unclassified controlled information. All media must be physically destroyed to preclude recovery of any of its information.

2. CLASSIFIED MEDIA.

   a. Clearing.

      (1) Media that will be reused at the same as previous or higher classification levels and categories than previously applied must be cleared unless it will be used within the same need-to-know context (i.e., all persons accessing data/media devices have the same authorized, need-to-know access as was required to access the data previously).

      (2) Cleared media that once contained classified information must be protected by measures commensurate with the highest classification level and any category of information ever stored on the media.

      (3) Overwriting is an acceptable method for clearing media. The approved procedure is described in Attachment 5 of this Manual.

[1] Classified media must not be reused in an unclassified environment.

b. Sanitization.

(1) Media that will be reused at lower than previous classification levels or categories and that will remain in classified environments must be sanitized.

(2) Media that will be released from the DOE-controlled environment must be destroyed.

(3) Media that will be released from the classified environment must be sanitized or destroyed. Classified media or formerly classified media must not be used in an unclassified environment.

(4) Sanitizing procedures must ensure that there is no opportunity for recontamination and that there is a documented chain-of-custody (DOE F 5635.3 Classified Document Receipt) for each device being sanitized (i.e., sanitization is done in only one central location, such as a sanitization warehouse).

(5) Cyber security professionals[2] tasked with the physical act of sanitizing computer equipment also must affix to the equipment a signed label verifying that the equipment has been sanitized. At minimum, labels must—

(a) describe the equipment;

(b) provide a statement indicating that the equipment has been sanitized in accordance with requirements of this Manual; and

(c) record the date, the printed name, and the signature of the certifier.

(6) The certifier also must document and submit that same information to the responsible Primary DOE Organization, which must maintain that documentation for a minimum of 5 years.

c. Destruction.

(1) Media that will be released from the DOE-controlled environment must be destroyed.

(2) Media that contains or did contain classified information that has been identified for destruction must be destroyed.

[2] As used in this Manual, "cyber security professionals" means qualified individuals that possess knowledge and experience in information technology security.

(3) Classified media must be sufficiently destroyed to preclude recovery of any of the information it contained.

(4) Methods for destroying media include pulverizing, smelting, incinerating, disintegrating, applying acid solutions, etc., to ensure that data cannot be retrieved by any currently known methods. All methods for destruction must be approved by the designated approving authority (DAA).

3. UNCLASSIFIED MEDIA.

a. Clearing and Sanitization of Unclassified Computer Equipment.

(1) Before DOE-owned or DOE-managed hard drives or systems containing hard disks are transferred internally, they must be cleared. This requirement also applies to equipment used for DOE support.

(2) Media that will be released from DOE-controlled environments must be sanitized or destroyed.

(3) Systems or equipment declared surplus or donated to outside organizations must be sanitized.

(4) Individuals involved in sanitizing computer equipment must check all components and peripherals for removable media to be sanitized/destroyed (i.e., remove the computer case to check for additional media).

(5) One-pass overwrite is sufficient for clearing unclassified computer media that did not contain unclassified controlled information previously [e.g., unclassified controlled nuclear information (UCNI), Naval Nuclear Propulsion Information (NNPI), official use only (OUO), etc.].

(6) Three-pass overwrite is required for sanitizing unclassified computer media that previously contained unclassified controlled information (UCNI, NNPI, OUO, etc.).

b. Quality Control. Overwritten hard drives intended for disposal or donation must be subjected to random sampling to verify that the overwriting process has been successfully completed.

(1) Sampling must be conducted and overwrite must be verified by trained cyber security professionals other than those who perform overwrite.

(2) A minimum of 20 percent of all overwritten hard drives will be examined in the sampling process.

(3) Requirements for overwrite training, sampling overwritten hard drives, and verifying that the overwrite process was successful must be established in the contractor's CSPP.

4. DOCUMENTATION. Once computer equipment has been cleared and/or sanitized, the cyber security professional who performed the actions must document the following:

a. media serial number, make, and model;

b. classification level (if applicable);

c. purpose for clearing and/or sanitizing; and

d. procedures used.

5. TRAINING, EDUCATION, AND AWARENESS.

a. DOE personnel must be trained at least annually on the risks of disclosing classified and unclassified controlled and the requirements for removing classified and unclassified controlled information from storage media, memory devices, and related hardware.

b. Personnel responsible for clearing, sanitizing, or destroying DOE information system storage media, memory devices, and other hardware also must be trained in techniques for checking and verifying that procedures to remove the information were effective.

c. Local sanitization awareness must be addressed in each Primary DOE Organization's cyber security training and awareness program.

CHAPTER II. ROLES AND RESPONSIBILITIES

1. OFFICE OF THE CHIEF INFORMATION OFFICER (OCIO).

   a. Develops cyber security policy, directives, and guidance.

   b. Provides performance oversight for the implementation of Department-wide policy and guidance for clearing, sanitizing, and destroying storage media, memory devices, and other hardware.

   c. Maintains records according to an approved DOE records schedule.

   d. Coordinates with the Office of Security to ensure a consistent approach to preventing unauthorized access to or disclosure of the Department's classified and unclassified controlled information.

   e. Maintains a service to validate on request that no recoverable information resides on samples of a DOE organization's sanitized devices.

2. HEADS OF PRIMARY DOE ORGANIZATIONS (Attachment 1). Note that except for paragraph 3a below, authority for these actions may be reassigned.

   a. Establish controls to ensure that requirements of this Manual are implemented.

   b. Ensure that plans and procedures for clearing, sanitizing, and destroying information system storage media, memory devices, and related hardware are incorporated into organization PCSPs in a manner consistent with Chapter I, paragraphs 2 and 3, and Attachment 5 of this Manual (i.e., chain-of-custody procedure for storage media to be sanitized). In addition, PCSP must address media that has been contaminated with classified and unclassified controlled information (i.e. email contamination).

   c. Ensure that personnel receive adequate training in requirements set forth in this Manual and in local sanitization procedures. Training plans are to be documented in the Primary Organization's PCSP.

3. DESIGNATED APPROVING AUTHORITY. The DAA must be a senior Federal DOE management official with the authority to formally assume responsibility for operating the information system at an acceptable level of risk to DOE operations, DOE assets, or individuals.

   a. Approves all products used to perform overwrites.[3]

[3] The DOE Cyber Forensics Lab is available to assist with the verification of the clearing/sanitization of media.

b. Only approved software compatible with the specific hardware intended for overwriting will be used.

c. Specifies and approves procedures for sanitizing storage media.

4. INFORMATION SYSTEMS SECURITY OFFICER (ISSO). ISSO or ISSO designee must review the results of overwrites to verify that the methods used completely overwrote all classified information.

**DEPARTMENTAL ELEMENTS, AND BY AGREEMENT,
THE NATIONAL NUCLEAR SECURITY ADMINISTRATION (NNSA),
TO WHICH DOE M 205.1-2 IS APPLICABLE**

Office of the Secretary
Departmental Representative to the Defense Nuclear Facilities Safety Board
Energy Information Administration
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Hearings and Appeals
Office of Inspector General
Office of Intelligence
Office of Legacy Management
Office of Management, Budget and Evaluation/Chief Financial Officer
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Security and Safety Performance Assurance
Secretary of Energy Advisory Board
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT

DOE M 205.1-2, *Clearing, Sanitization, and Destruction of Information System Storage Media, Memory Devices, and Related Hardware Manual*

Regardless of the performer of the work, the contractor is responsible for complying with and flowing down the requirements of this Contractor Requirements Document (CRD) to subcontractors at any tier to the extent necessary to ensure the contractor's compliance with the requirements. In doing so, the contractor must not flow down requirements to subcontractors unnecessarily or imprudently. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD.

This CRD establishes requirements with which Department of Energy (DOE) and National Nuclear Security Administration (NNSA) contractors with access to DOE information systems must comply. This CRD supplements requirements defined in the CRD for DOE O 205.1, *Department of Energy Cyber Security Management Program*, dated 3-21-03, including requirements for cyber resource protection, risk management, program evaluation, and cyber security plan development and maintenance. The contractor will ensure that it and its subcontractors cost-effectively comply with the requirements of this CRD.

The requirements set forth in this CRD are not applicable to media that have been used to process Special Access Program information or sensitive compartmented information.

1. INTRODUCTION. Three activities support the confidentiality and security objectives of the Federal Information Security Management Act of 2002: clearing, sanitization, and destruction. In keeping with sound fiscal management practices, DOE contractors must conserve information resources and reuse media whenever possible.[1] Each of these activities is used to meet the objectives of conserving resources and maintaining confidentiality throughout the life cycle of the information.

   Clearing is utilized for processing media that will be reused at the same or higher classification levels and categories. Cleared media that contained classified or unclassified controlled information must be protected by measures commensurate with the highest level and any category of information the media ever contained. Clearing does not lower the classification levels or categories of the media. The media must retain classification labels/markings and controls. Any medium must be protected at the level and any category for which it is marked, even if it never contained information commensurate with the marking.

   Sanitization is utilized for media that will be reused at lower classification levels or categories, or released from classified or sensitive environments.

   Destruction is utilized for media that are no longer being used or that contain or formerly contained classified or unclassified controlled information. All media must be physically destroyed to preclude recovery of any of its information.

[1] Classified media must not be reused in an unclassified environment.

2. DEPARTMENT OF ENERGY APPROVED PROCEDURES. DOE-approved procedures for clearing, sanitizing, and destroying information system storage media, memory devices, and other related hardware that have been used to process, store, or contain classified information are listed in Appendix A of this CRD. These procedures should be implemented in a cost-effective manner, though competitive business cost is not the overriding factor.

3. CLASSIFIED MEDIA.

a. Clearing.

(1) Media that will be reused at the same as previous or higher classification levels or categories than previously applied must be cleared unless it will be used within the same need-to-know context (i.e., all persons accessing data/media devices have the same authorized, need-to-know access as was required to access the data previously).

(2) Cleared media that once contained classified information must be protected by measures commensurate with the highest classification level and any category of information ever stored on the media.

(3) Overwriting is an acceptable method for clearing media. The approved procedure is described in Appendix A to this CRD.

b. Sanitization.

(1) Media that will be reused at lower than previous classification levels or categories and that will remain in classified environments must be sanitized.

(2) Media that will be released from the DOE-controlled[2] environment must be destroyed.

(3) Media that will be released from the classified environment must be sanitized or destroyed. Classified media or formerly classified media must not be used in an unclassified environment.

(4) Sanitizing procedures must ensure there is no opportunity for recontamination and that there is a documented chain-of-custody (e.g., DOE F 5635.3, Classified Document Receipt) for each device being sanitized (i.e., sanitization is done in one central location, such as a sanitization warehouse).

(5) The sanitization of computer equipment must include documentation certifying that the process has been successfully completed in the form of

[2] "DOE-controlled" is intended to include DOE contractor-controlled property.

a signed label affixed to the equipment verifying that the equipment has been sanitized. At minimum, labels must—

(a) describe the equipment;

(b) provide a statement indicating that the equipment has been cleared and/or sanitized in accordance with requirements of this CRD; and

(c) record the date, the printed name, and the signature of the certifier.

(6) The certifier also must document and submit that same information to the responsible DOE organization.

c. Destruction.

(1) Media that will be released from the DOE-controlled environment must be destroyed.

(2) Media that contains or did contain classified information that has been identified for destruction must be destroyed.

(3) Classified media must be sufficiently destroyed to preclude recovery of any of the information it contained.

(4) Methods for destroying media include pulverizing, smelting, incinerating, disintegrating, applying acid solutions, etc., to ensure that data cannot be retrieved by any currently known methods. All methods for destruction must be approved by the designated approving authority (DAA) of the Primary DOE Organization (DAA must be a federal employee).

4. UNCLASSIFIED MEDIA.

a. Clearing and Sanitization of Unclassified Computer Equipment.

(1) Before DOE-owned or DOE-managed hard drives or systems containing hard disks are transferred internally, they must be cleared. This requirement also applies to equipment used for DOE support.

(2) Media that will be released from DOE-controlled environments must be sanitized or destroyed.

(3) Systems or equipment declared surplus or donated to outside organizations must be sanitized.

(4) During sanitization of computer equipment, all drives must be checked for removable media to be sanitized/destroyed (i.e., removing the computer case to check for additional media).

(5) One-pass overwrite is sufficient for clearing unclassified computer media that do not contain unclassified controlled information [e.g., Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Propulsion Information (NNPI), Official Use Only (OUO), etc].

(6) Three-pass overwrite is required for sanitizing unclassified computer media that previously contained unclassified controlled information (UCNI, NNPI, OUO, etc.).

b. Quality Control. Overwritten hard drives intended for disposal or donation must be subjected to random sampling to verify that the overwriting process has been successful.

(1) Sampling must be conducted and overwrite must be verified by trained individuals other than those who performed overwrites.

(2) A minimum of 20 percent of all overwritten hard drives will be examined in the sampling process.

(3) Requirements for overwrite training, sampling overwritten hard drives, and verifying that the overwrite process was successful must be established in the contractor's cyber security program plan (CSPP).

5. DOCUMENTATION. Once computer equipment has been cleared and/or sanitized, the certifier must document the following:

a. media serial number, make, and model;

b. classification level (if applicable);

c. purpose for clearing and/or sanitizing; and

d. procedures used.

6. TRAINING, EDUCATION AND AWARENESS.

a. All contractor personnel must be trained at least annually on the risks associated with disclosure of classified and unclassified controlled information and requirements for removing classified and unclassified controlled information from storage media, memory devices, and related hardware.

b. All contractor personnel who are responsible for clearing, sanitizing, or destroying Federal information system storage media, memory devices, and other hardware must receive training in techniques to check, verify, and determine that procedures to remove the information were effective.

APPENDIX A.

TABLES ON DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZATION, AND DESTRUCTION OF INFORMATION ON ELECTRONIC MEDIA

TABLE 1. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZATION, AND DESTRUCTION OF STORAGE MEDIA*

MEDIA TYPE†	CLEARING‡	SANITIZATION‡	DESTRUCTION‡
Magnetic Tapes **			
Type I	1 or 2	1 or 2	4
Type II	1 or 2	2	4
Type III	4	4	4
Magnetic Disks**			
Floppies, Zip Drive Media	1, 2, or 3	2	4
Bernoulli Boxes	1, 2, or 3	4	4
Removable Hard Disks	1, 2, or 3	1, 2, or 3+	4 or 5
Nonremovable Hard Disks	3	1, 2, or 3+	4 or 5
Optical Disks			
Magneto-optical: Read Only	6	6	4
Write Once, Read Many (WORM)	6	6	4
Read Many, Write Many	6	6	4
Other			
Floptical	6	6	4
Helical-scan Tapes	6	6	4
Cartridges	6	6	4
Optical	6	6	4

Procedures: †

1. Degauss with a Type 1 degausser.§
2. Degauss with a Type 2 degausser.§
3. Overwrite all locations with a pseudorandom pattern twice and then overwrite all locations with a known pattern.
4. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed.
5. Remove the entire recording surfaces by sanding or applying acid.
6. Not applicable.

* NSA/CSS Manual 130-2, *Media Declassification and Destruction Manual*, November 2000, or subsequent update may be used as a supplement for these procedures.

** Magnetic tape and disk media defined by their magnetic coercivity in units of Oersteds (Oe) must be degaussed in accordance with NSA/CSS Manual 130-2, *Media Declassification and Destruction Manual*, November 2000 or subsequent updates.

† Program offices are responsible for developing clearing, sanitizing, and destroying procedures for media types not listed.

‡ Numbers in the table refer to the procedures listed.

§ All degaussing products used to clear or sanitize media **must** be certified by the National Security Agency (NSA) and be listed on NSA Degausser Approved Products List.

+ Not authorized for classified hard disks or hard disks that formerly contained classified information.

TABLE 2. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZATION, AND DESTRUCTION ELECTRONIC MEMORY DEVICES*

MEDIA TYPE†	CLEARING‡	SANITIZATION‡	DESTRUCTION‡
Read-Only Memory (ROM)	13	13	11 (see 12)
Random Access Memory (RAM) (Volatile)	3 or 5	5, then 10	11
Programmable ROM (PROM)	13	13	11
Erasable PROM (UV PROM)	6	7, then 3 and 10	11
Electrically Alterable PROM (EAPROM)	8	8, then 3 and 10	11
Electrically Erasable PROM (EEPROM)	9	9, then 3 and 10	11
Flash Erasable PROM (FEPROM)	9	9, then 3 and 10	11

Procedures:‡

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

* NSA/CSS Manual 130-2, *Media Declassification and Destruction Manual*, November 2000, or subsequent update may be used as a supplement for these procedures.

† Program offices are responsible for developing clearing, sanitizing, and destroying procedures for media types not listed.

‡ Numbers in the table refer to the procedures listed.

§ All degaussing products used to clear or sanitize media **must** be certified by the National Security Agency (NSA) and be listed on the Degausser Approved Products List.

TABLE 3. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZATION, AND DESTRUCTION OF HARDWARE*

MEDIA TYPE†	CLEARING‡	SANITIZATION‡	DESTRUCTION‡
Printer Ribbons	7	7	7
Platens	8	2	7
Toner Cartridges	6	6	8
Laser Drums	4	3	7
Cathode-Ray Tubes (If there is Classified Burn-In)	8	7	7
Fax Machines	5	5	7
All other storage media devices	8	8	7

Procedures: †

1. Overwrite at least five consecutive times with unclassified data.
2. Chemically clean so no visible trace of data remains.
3. Print at least five pages of randomly generated unclassified data. The pages should not include any blank spaces or solid black areas.
4. Print three blank copies. If unable to get a clean output, print an unclassified test pattern or black copy; then run three blank copies.
5. For fax machines that have memory and other storage media incorporated, treat each component per procedures listed in Tables 1 and 2 of this appendix.
6. 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 and area.
7. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure the media are physically destroyed.
8. Not applicable.

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

* NSA/CSS Manual 130-2, *Media Declassification and Destruction Manual*, November 2000, or subsequent update may be used as a supplement for these procedures.

† Program offices are responsible for developing clearing sanitizing, and destroying procedures for media types not listed.

‡ Numbers in the table refer to the procedures listed.

CONTRACTOR REQUIREMENTS DOCUMENT (CRD) APPLICABILITY

The CRD for DOE M 205.1-2 is intended to apply to all DOE contractor site/facilities and the site/facility management contracts applicable to the following sites/facilities.

- Lawrence Berkeley National Laboratory
- Pacific Northwest National Laboratory
- Brookhaven National Laboratory
- Sandia National Laboratories
- National Renewable Energy Laboratory
- Stanford Linear Accelerator Center
- Bettis Atomic Power Laboratory
- Argonne National Laboratory
- Idaho National Laboratory
- Thomas Jefferson National Accelerator Facility
- Ames National Laboratory
- Oak Ridge National Laboratory
- Knolls Atomic Power Laboratory
- Lawrence Livermore National Laboratory
- Los Alamos National Laboratory
- Savannah River Site
- Princeton Plasma Physics Laboratory
- Fermi National Accelerator Center
- West Valley Project
- Strategic Petroleum Reserve
- Oak Ridge Y-12 National Security Complex
- Pantex Plant
- Waste Isolation Pilot Plant
- Nevada Test Site
- Kansas City Plant
- National Civilian Radioactive Waste Program (Yucca Mountain)
- Hanford Environmental Restoration
- Oak Ridge Environmental Management
- Mound Environmental Management Project
- Project Hanford
- River Protection Project Tank Farm Management
- Rocky Flats
- Fernald Environmental Management Project
- Grand Junction Technical & Remediation Services
- Grand Junction Facilities & Operations Services
- Oak Ridge Institute of Science & Education
- Occupational Health Services at the Hanford Site

DEFINITIONS

Clearing. Removal of data from information system storage devices and other peripheral devices with storage capacity in such a way that the data may not be reconstructed using common system capabilities (i.e., keyboard strokes). The data may be reconstructed using laboratory methods, however. Cleared media may be reused at the same classification level or at a higher level. Overwriting is one method of clearing.

Contaminate. Media that has been exposed to classified or unclassified controlled information.

Degauss. Procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing.

Degausser. A device that removes data from a storage medium by removing magnetism.

Disposal. The act or process of getting rid of media.

DOE-controlled environment. An area within a DOE-controlled facility or within a DOE contractor-controlled facility.

Information systems. A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

Internally transferred. Computer equipment that is to be transferred within DOE but outside the direct line of authority. For example, a computer with a hard disk in the Office of Cyber Security may be transferred to another person within the Office of Cyber Security without being cleared. If the computer were to be transferred to someone in DOE outside of the Office of Cyber Security, it would have to be cleared first.

Storage device. Information system storage device (also system storage device or storage device) refers to any device capable of storing electronic data in a non-volatile state [e.g., optical media (CD, DVD), magnetic media (hard drive, floppy drive, tape) and solid state media (USB drives, ASIC chip technology)].

Nonremovable media. Fixed storage devices such as hard drives, which provide internal information/data storage.

Overwriting. A procedure for destroying data from storage media by recording patterns of meaningless data over the data stored on the media. The approved procedure is to overwrite all locations three times with a pseudorandom pattern twice and then overwrite all locations with a known pattern.

Pulverizing. Pounding, crushing, or grinding to a powder or dust.

Removable media. Media not attached to information systems via the internal bus of the information system.

Sanitization. The process of removing data from media before it is reused in environments that do not provide acceptable levels of protection for the data stored in the media before sanitizing. Information system resources will be sanitized before release from classified information controls or released for use at lower classification levels.

Smelting. Melting to separate metallic constituents of a device.

ATTACHMENT 5

TABLES ON DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZATION, AND DESTRUCTION OF INFORMATION ON ELECTRONIC MEDIA

TABLE 1. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZATION, AND DESTRUCTION STORAGE MEDIA *

MEDIA TYPE†	CLEARING‡	SANITIZATION‡	DESTRUCTION‡
Magnetic Tapes**			
Type I	1 or 2	1 or 2	4
Type II	1 or 2	2	4
Type III	4	4	4
Magnetic Disks**			
Floppies, Zip Drive Media	1, 2, or 3	2	4
Bernoulli Boxes	1, 2, or 3	4	4
Removable Hard Disks	1, 2, or 3	1, 2, or 3+	4 or 5
Nonremovable Hard Disks	3	1, 2, or 3+	4 or 5
Optical Disks			
Magneto-optical: Read Only	6	6	4
Write Once, Read Many (WORM)	6	6	4
Read Many, Write Many	6	6	4
Other			
Floptical	6	6	4
Helical-scan Tapes	6	6	4
Cartridges	6	6	4
Optical	6	6	4

Procedures: †
1. Degauss with a Type 1 degausser.§
2. Degauss with a Type 2 degausser.§
3. Overwrite all locations with a pseudorandom pattern twice and then overwrite all locations with a known pattern.
4. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed.
5. Remove the entire recording surfaces by sanding or applying acid.
6. Not applicable.

* NSA/CSS Manual 130-2, *Media Declassification and Destruction Manual*, November 2000, or subsequent update may be used as a supplement for these procedures.

** Magnetic tape and disk media defined by their magnetic coercivity in units of Oersteds (Oe) must be degaussed in accordance with NSA/CSS Manual 130-2, *Media Declassification and Destruction Manual*, November 2000 or subsequent updates.

† Program offices are responsible for developing clearing, sanitizing, and destroying procedures for media types not listed.

‡ Numbers in the table refer to the procedures listed

§ All degaussing products used to clear or sanitize media **must** be certified by the National Security Agency (NSA) and be listed on NSA Degausser Approved Products List.

+ Not authorized for classified hard disks or hard disks that formerly contained classified information.

TABLE 2. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZATION, AND DESTRUCTION ELECTRONIC MEMORY DEVICES*

MEDIA TYPE†	CLEARING‡	SANITIZATION‡	DESTRUCTION‡
Read-Only Memory (ROM)	13	13	11 (see 12)
Random Access Memory (RAM) (Volatile)	3 or 5	5, then 10	11
Programmable ROM (PROM)	13	13	11
Erasable PROM (UV PROM)	6	7, then 3 and 10	11
Electrically Alterable PROM (EAPROM)	8	8, then 3 and 10	11
Electrically Erasable PROM (EEPROM)	9	9, then 3 and 10	11
Flash Erasable PROM (FEPROM)	9	9, then 3 and 10	11

Procedures:‡

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

* NSA/CSS Manual 130-2, *Media Declassification and Destruction Manual*, November 2000, or subsequent update may be used as a supplement for these procedures.

† Program offices are responsible for developing clearing, sanitizing, and destroying procedures for media types not listed.

‡ Numbers in the table refer to the procedures listed.

§ All degaussing products used to clear or sanitize media **must** be certified by the National Security Agency (NSA) and be listed on the Degausser Approved Products List.

TABLE 3. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZATION, AND DESTRUCTION HARDWARE*

MEDIA TYPE†	CLEARING‡	SANITIZATION‡	DESTRUCTION‡
Printer Ribbons	7	7	7
Platens	8	2	7
Toner Cartridges	6	6	8
Laser Drums	4	3	7
Cathode-Ray Tubes (If there is Classified Burn-In)	8	7	7
Fax Machines	5	5	7
All other storage media devices	8	8	7

Procedures: †

1. Overwrite at least five consecutive times with unclassified data.
2. Chemically clean so no visible trace of data remains.
3. Print at least five pages of randomly generated unclassified data. The pages should not include any blank spaces or solid black areas.
4. Print three blank copies. If unable to get a clean output, print an unclassified test pattern or black copy; then run three blank copies.
5. For fax machines that have memory and other storage media incorporated, treat each component per procedures listed in Tables 1 and 2 of this attachment.
6. 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 and area.
7. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure the media are physically destroyed.
8. Not applicable.

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

* NSA/CSS Manual 130-2, *Media Declassification and Destruction Manual*, November 2000, or subsequent update may be used as a supplement for these procedures.

† Program offices are responsible for developing clearing sanitizing, and destroying procedures for media types not listed.

‡ Numbers in the table refer to the procedures listed.