U.S. Department of Energy
Washington, D.C.

NOTICE

DOE N 205.12

Approved: 2-19-04
Expires: 2-19-05

SUBJECT: CLEARING, SANITIZING, AND DESTROYING INFORMATION SYSTEM STORAGE MEDIA, MEMORY DEVICES, AND OTHER RELATED HARDWARE

1. OBJECTIVES. To establish Department of Energy (DOE) policy requirements and responsibilities for clearing, sanitizing, and destroying DOE information system storage media, memory devices, and other related hardware.

   a. To provide instructions for sanitizing classified, nonremovable storage media that will be reused in controlled, unclassified environments.

   b. To provide instructions for sanitizing nonremovable storage media that has become partially contaminated with classified information.

   c. To ensure that no unauthorized information can be retrieved from unclassified DOE computer equipment that is to be transferred or declared surplus.

   d. To ensure that all DOE personnel are made aware of requirements for sanitizing information system storage media, memory devices, and related hardware.

   e. To fulfill the commitment to performance-based management of DOE contracts as outlined in Secretary Abraham's May 12, 2003, memorandum, Clarification of Roles and Responsibilities, by supporting to the "maximum extent practicable, the principle to apply performance-based contracting techniques under which the contract will define what is to be done, and not how it will be done."

2. CANCELLATIONS. None.

3. APPLICABILITY.

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

   b. Site/Facility Management Contractors. Except for the exclusions in paragraph 3c, the Contractor Requirements Document (CRD), Attachment 2, sets forth requirements of this Notice 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 provide automated access to DOE information systems (Site/facility management contractors to which the CRD applies are listed in Attachment 3).

(2) This Notice does not automatically apply to other than site/facility management contractors. Any application of requirements of this Notice to other than site/facility management contractors will be communicated separately.

(3) Lead Program Secretarial Officers are responsible for telling their appropriate contracting officers which site/facility management contractors are affected by this Notice. Once notified, contracting officers are responsible for incorporating the CRD into contracts of affected site/facility management contractors via the laws, regulations, and DOE directives clause of their 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 Notice for activities under the Deputy Administrator's cognizance.

(2) The requirements set forth in this Notice are not applicable to media that have been used to process Special Access Program information or Sensitive Compartmented Information.

4. REQUIREMENTS.

a. Implementation. Primary DOE Organizations must implement the requirements and meet the responsibilities defined in this Notice within 90 days of its issuance. Requirements and responsibilities will flow down from the heads of Primary DOE Organizations to all organizational levels.

b. Clearing. See Attachment 4 for definitions of terms used in this Notice.

(1) Depending upon authorized need to know, media that will be reused at the same or a higher classification level must be cleared.

(2) Overwriting is an acceptable method for clearing media. The approved procedure is to overwrite all locations three times—

(a) the first time with a character,

(b) the second time with its complement, and

(c) the third time with a random character.

(3) Only approved overwriting software that is compatible with the specific hardware intended for overwriting will be used. Use of such software will be coordinated in advance with the owner of the data.

(4) The designated approving authority (DAA) must approve all products used to perform overwrites.

(5) Cleared media that contained classified information must be protected by measures commensurate with the highest level of information it contained.

c. Sanitizing.

(1) Media that will be reused at a lower classification level or released from a classified environment must be sanitized.

(2) Media that will be released from a DOE-controlled environment must be sanitized.

(3) Individuals involved in clearing or sanitizing computer equipment must also certify that the process has been successfully completed by

affixing 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 cleared and/or sanitized in accordance with requirements of this Notice; and

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

(4) The certifier must prepare separate documentation recording the same information and submit it to the Departmental element, which must maintain the documentation for a minimum of 5 years.

d. Destroying.

(1) Media that is no longer being used and that contains or did contain classified information must be destroyed.

(2) When classified matter is to be destroyed, it must be sufficiently destroyed to preclude any of the information it contained being recovered.

(3) Media which contained classified information must first be sanitized before being destroyed.

(4) Methods for destroying media are pulverizing, smelting, incinerating, disintegrating, applying acid solutions, etc., as approved by the DAA in accordance with national security policy.

e. 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 Attachment 2 to this Notice. Decisions to clear, sanitize, or destroy information system storage media, memory, and other related hardware should be based on cost-effectiveness.

f. Reusing Classified Media in Unclassified Environments. When nonremovable classified media (computer hard drives, etc.) are no longer required for use in classified environments (as determined by local site management), the media can be sanitized with specific overwrites and reused in unclassified environments within the same security area. This procedure is intended to be

used in conjunction with the accreditation of information systems at lower security levels.

(1) The unclassified media must be in a DOE-controlled environment.

(2) The media must not leave the controlled environment without first being destroyed.

(3) The decision to reuse media at a lower classification level may be acceptable if formal risk and cost analyses are conducted and the results of these analyses and testing of the implemented procedures verify that the national security of the United States is not adversely affected. Such analyses and decisions must be approved by heads of Departmental elements.

(4) Media are to be sanitized by overwriting using the three-step process described in Appendix A of Attachment 2.

(5) Sanitizing software must provide information about sectors overwritten and bad sectors that cannot be overwritten.

(6) The DAA must approve all products used to perform overwrites.[1]

(7) Media containing classified information designated for reuse by local site management must be sanitized. The information systems security officer (ISSO) or designee must approve overwrite methods and review the results of overwrites to verify that the method used completely overwrote all classified information.

(8) Once sanitized, media must be conspicuously marked to indicate that it once contained classified information. The media must be protected to ensure that it does not leave the controlled environment without first being destroyed.

(9) Personal computer diskettes or any other types of removable media that have contained classified information may not be reused in any unclassified system or environment.

g. Sanitizing Partially Contaminated Media.

(1) If nonremovable storage media operated in unclassified environments become contaminated with relatively small amounts of classified information (less than 20 kilobytes of information and less than 0.01

[1]The DOE Cyber Forensics Lab is available, at no charge, to assist with the verification of the sanitization of media.

percent of the capacity of the nonremovable media), the only the affected areas need to be sanitized using the process listed in Appendix A of Attachment 2.

(2) The DAA must approve all products used to perform overwrites.

(3) The ISSO or designee must approve overwrite methods and review the results of overwrites to verify that the methods used completely overwrote all classified information.

(4) If the contamination is greater than 20 kilobytes of information or greater than 0.01 percent of the capacity of the nonremovable media, the media must be treated as if it had been used in classified environments, meaning that it must be completely sanitized in accordance with the procedures listed in Appendix A of Attachment 2.

(5) The programs used to overwrite contaminated media must overwrite all addressable locations, including temporary data file locations, file slack, free space, and directories and must provide confirmation of overwrite of specified areas and of successful completion.

(6) For networked systems that have become partially contaminated, the following requirements apply.

(a) If the contamination is less than 20 kilobytes of information and less than 0.01 percent of the capacity of the nonremovable media, then only the affected areas of the contaminated systems need to be sanitized using the process listed in Appendix A of Attachment 2.

(b) If the contamination is greater than 20 kilobytes of information or greater than 0.01 percent of the capacity of the nonremovable media, then all affected systems must be completely sanitized in accordance with the procedures listed in Appendix A of Attachment 2.

(c) Personal computer diskettes or any other types of removable media that have become contaminated with classified information must be sanitized in accordance with the procedures listed in Appendix A of Attachment 2.

h. Clearing and Sanitizing Unclassified Computer Equipment.

(1) All Primary DOE Organizations must have plans to sanitize and clear DOE computer equipment and must define those plans in their respective program cyber security plans (PCSPs).

(2) All Primary DOE Organizations must describe the requirements for implementing their clearing/sanitizing plans in their respective cyber security program plans (CSPPs), including requirements for documented methods to independently verify clearing/sanitizing results.

(3) 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.

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

(5) One-pass overwrites are sufficient for clearing unclassified computer media not containing sensitive information [e.g., Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Propulsion Information (NNPI), and Official Use Only (OUO)].

(6) A minimum of three-pass overwrites are required for sanitizing unclassified computer media which contained sensitive information (UCNI, NNPI, OUO).

(7) Overwritten hard drives intended for disposal, donation, or internal transfer must be sampled on a random basis to verify that the overwriting process has been successfully completed.

(a) Sampling/verifying must be conducted by trained individuals other than those who performed the overwrites.

(b) No fewer than 10 percent of all overwritten hard drives will be examined in the sampling process.

(c) Requirements for overwrite training, sampling overwritten hard drives, and verifying the overwriting process must be established in Departmental elements' PCSPs and CSPPs.

(8) Once computer equipment has been cleared and/or sanitized, the individuals performing the actions must prepare documentation that includes—

(a) descriptions of the media (serial numbers, makes, models),

(b) classification levels,

(c) purposes for clearing and/or sanitizing, and

(d) procedures used.

i. Training.

(1) All personnel from DOE organizations must be trained on the risks associated with disclosure of sensitive information and requirements for removing sensitive information from storage media, memory devices, and related hardware.

(2) All personnel who are responsible for clearing and sanitizing 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.

(3) Local sanitization awareness must be addressed in each Primary DOE Organization's computer security training and awareness program.

5. RESPONSIBILITIES.

a. Office of the Chief Information Officer (OCIO).

(1) Responsible for all cyber security Policies, Orders, Manuals, and guidelines.

(2) Develops and maintains Department-wide policy and guidance for clearing, sanitizing, and destroying storage media, memory devices, and other hardware.

b. Office of Security.

(1) Develops media sanitization procedures in coordination with the OCIO to enable a consistent approach to preventing unauthorized access or disclosure of the Department's sensitive and classified information.

(2) Maintains an on-request service to validate that no recoverable information resides on samples of a DOE organization's sanitized devices.

c. Heads of Primary DOE Organizations (see Attachment 1). Note that except for item (1) below, authority for these actions may be reassigned.

(1) Establish controls to ensure that requirements of this Notice are implemented.

(2) Ensure that plans and procedures for clearing, sanitizing, and destroying information system storage media, memory devices, and related hardware are incorporated into the organization's PCSPs and site CSPPs in a manner consistent with paragraph 4 and the CRD for this Notice.

(3) Ensure that personnel receive adequate training in both requirements set forth in this Notice and local sanitization procedures. Training plans are to be documented in organization PCSPs.

6. REFERENCES. The following public laws and policies, national standards and guidelines, and DOE directives provide relevant processes and procedures for implementing cyber security program requirements and guidance that may be helpful in implementing this Notice.

a. Atomic Energy Act of 1954, as amended.

b. National Computer Security Center (NCSC) TG-025, *A Guide to Understanding Data Remanence in Automated Information Systems,* dated September 1991.

c. National Security Agency, Information Systems Security Products and Services Catalogue, Degausser Products List.

d. OMB Circular A-130, *Management of Federal Information Resources,* dated November 2000, Appendix III.

e. Memorandum from the Office of Safeguards and Security, to Distribution, Clarification to DOE M 5639.6-1A, *Clearing, Sanitization and Destruction of Automated Information Systems (AIS) Storage Media, Memory and Hardware,* dated 9-30-98.

f. DOE O 205.1, *Department of Energy Cyber Security Management Program,* dated 3-21-03.

7. CONTACT. Questions concerning this Notice should be directed to the Office of the Chief Information Officer, Office of Cyber Security, at 202-586-0166.

BY ORDER OF THE SECRETARY OF ENERGY:

KYLE E. McSLARROW
Deputy Secretary

PRIMARY DOE ORGANIZATIONS TO WHICH DOE N 205.12 IS APPLICABLE

Office of the Secretary
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Office of Counterintelligence
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electric Transmission and Distribution
Office of Energy Assurance
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
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 Security
Office of Security and Safety Performance Assurance
Office of the Inspector General
Office of Intelligence
Office of Legacy Management
Office of Management, Budget and Evaluation and Chief Financial Officer
National Nuclear Security Administration
Office of Nuclear Energy, Science and Technology
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Office of Independent Oversight and Performance Assurance
Secretary of Energy Advisory Board
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

CONTRACTOR REQUIREMENTS DOCUMENT

DOE N 205.12, *Clearing, Sanitizing, and Destroying Federal Information System Storage Media, Memory Devices, and Other Hardware*

This Contractor Requirements Document (CRD) establishes the requirements for Department of Energy (DOE) and National Nuclear Security Administration contractors, with access to DOE information systems. Contractors must comply with the requirements listed in the CRD.

This CRD supplements requirements contained 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.

Regardless of the performer of the work, the contractor is responsible for complying with and flowing down the requirements of this 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 unnecessarily or imprudently flow down requirements to subcontractors. That is, the contractor will ensure that it and its subcontractors comply with the requirements of this CRD and incur only those costs that would be incurred by a prudent person in the conduct of competitive business.

STORAGE MEDIA REQUIREMENTS.

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. CLEARING.

   a. Dependent upon authorized need to know, media that will be reused at the same or a higher classification level must be cleared.

   b. Overwriting is an acceptable method for clearing media. The approved overwrite procedure is to overwrite all locations three times—

      (1) the first time with a character,

      (2) the second time with its complement, and

      (3) the third time with a random character.

   c. Only approved overwriting software that is compatible with the specific hardware intended for overwriting will be used. Use of such software will be coordinated in advance with the owner of the data.

d. The designated approving authority (DAA), who must be a Federal employee, must approve all products used to perform overwrites.

e. Cleared media that contained classified information must be protected using measures commensurate with the highest level of information it contained.

2. SANITIZING.

a. Media that will be reused at a lower classification level or released from a classified environment must be sanitized.

b. Media that will be released from a DOE-controlled environment must be sanitized.

c. Individuals involved in clearing/sanitizing computer equipment must also certify that the process has been successfully completed by affixing to the equipment a signed label verifying that the equipment has been sanitized. At a minimum, the labels must—

(1) describe the equipment;

(2) provide a statement indicating that the equipment has been cleared and/or sanitized in accordance with this DOE N 205.12; and

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

d. The certifier must prepare separate documentation recording the same information and the contractor must maintain this documentation for a minimum of 5 years.

3. DESTROYING.

a. Media that is no longer being used and that contains or did contain classified information must be destroyed.

b. When classified matter is to be destroyed, it must be sufficiently destroyed to preclude any of the information it contained being recovered.

c. Media which contained classified information must first be sanitized before being destroyed.

d. Methods for destroying media are pulverizing, smelting, incinerating, disintegrating, applying acid solutions, etc., as approved by the DAA in accordance with national security policy.

4. DEPARTMENT OF ENERGY-APPROVED PROCEDURES. DOE-approved procedures for clearing, sanitizing, and destroying information system storage media, memory devices, and related hardware that have been used to process, store, or contain classified information are listed in appendix a of this CRD. Decisions to clear, sanitize,

or destroy information system storage media, memory, and other related hardware should be based on cost effectiveness.

5. REUSING CLASSIFIED MEDIA IN UNCLASSIFIED ENVIRONMENTS.

When nonremovable classified media such as computer hard drives is no longer required for use in classified environments (as determined by local site management), the media can be sanitized with specific overwrites and reused in unclassified environments within the same security area. This procedure is intended to be used in conjunction with the accreditation of information systems at a lower security level.

a. The unclassified environments must be in a DOE controlled environment.

b. The media must not leave the controlled environment without first being destroyed.

c. The decision to reuse media at a lower classification level may be acceptable if formal risk and cost analyses are conducted and the results of these analyses and testing of the implemented procedures verify that the national security of the United States is not adversely affected. Such analyses and decisions must be approved by heads of Departmental elements. Media are to be sanitized by overwriting the entire media using the three-step process described in paragraph 1a(2) of this CRD.

(1) Sanitizing software must provide information about sectors overwritten and bad sectors that cannot be overwritten.

(2) The DAA must approve all products used to perform overwrites.[1]

d. Media containing classified information, designated for reuse by local site management, must be sanitized. The contractor's lead system security officer must approve overwrite methodologies and review the results of overwrites to verify that the methodology used completely overwrote all classified information.

e. Once sanitized, media must be conspicuously marked to indicate that they once contained classified information and be protected to ensure the media do not leave the controlled environment without first being destroyed.

f. Personal computer diskettes or any other type of removable media that have contained classified information may not be reused in any unclassified system or environment.

[1]The DOE Cyber Forensics Lab is available, at no charge, to assist with the verification of the sanitization of media.

6. SANITIZING PARTIALLY CONTAMINATED MEDIA.

a. If nonremovable storage media operated in unclassified environments become contaminated with relatively small amounts of classified information (less than 20 kilobytes of information and less than 0.01 percent of the capacity of the nonremovable media), the affected areas may be sanitized using the three-step process described in paragraph 1a(2) of this CRD.

b. The DAA must approve all products used to perform overwrites.

c. The contractor's lead system security officer must approve overwrite methods and review the results of overwrites to verify that the method used completely overwrote all classified information.

d. If the contamination is greater than 20 kilobytes of information or greater than 0.01 percent of the capacity of the nonremovable media, the media must be treated as if it had been used in classified environments, meaning that it must be completely sanitized in accordance with the procedures listed in Appendix A of this CRD.

e. The programs used to overwrite contaminated media must overwrite all addressable locations, including temporary data file locations, file slack, free space, and directories, and provide confirmation of overwrite of specified areas and of successful completion.

f. For networked systems that have become partially contaminated, the following requirements apply.

(1) If the contamination is less than 20 kilobytes of information and less than 0.01 percent of the capacity of the nonremovable media, then the affected areas of the contaminated systems may be sanitized using the three-step process listed in paragraph 1a(2) of this CRD.

(2) If the contamination is greater than 20 kilobytes of information or greater than 0.01 percent of the capacity of the nonremovable media, then all affected systems must be sanitized in accordance with the procedures listed in Appendix A of this CRD.

(3) Personal computer diskettes or any other type of removable media that have become contaminated with classified information must be sanitized in accordance with the procedures listed in Table 1 of Appendix A.

7. CLEARING AND SANITIZING UNCLASSIFIED COMPUTER EQUIPMENT.

a. The contractor must describe the requirements for implementing their clearing/sanitizing plans in their respective cyber security program plans (CSPPs),

including the requirement for documented methods for independently verifying the clearing/sanitizing results.

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

c. Systems or equipment declared surplus or donated to outside organizations must be sanitized.

d. One-pass overwrites are sufficient for clearing unclassified computer media not containing sensitive information [e.g.; Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Propulsion Information (NNPI), and Official Use Only (OUO)].

e. A minimum of three-pass overwrites are required for sanitizing unclassified computer media which contained sensitive information (UCNI, NNPI, OUO).

f. Overwritten hard drives intended for disposal, donation, or internal transfer must be sampled on a random basis to verify that the overwriting process has been successfully completed.

(1) Sampling/verifying must be conducted by trained individuals other than the ones who performed the overwrites.

(2) No fewer than 10 percent of all overwritten hard drives will be examined in the sampling process.

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

g. Once computer equipment has been cleared and/or sanitized, the individuals performing the actions must prepare documentation that includes—

(1) descriptions of the media (serial numbers, makes, models),

(2) classification levels,

(3) purposes for clearing and/or sanitizing, and

(4) procedures used.

8. TRAINING.

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

b. All contractor personnel who are responsible for clearing and sanitizing 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

TABLE 1. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZING, AND DESTROYING STORAGE MEDIA*

MEDIA TYPE†	CLEARING‡	SANITIZING‡	DESTROYING‡
Magnetic Tapes			
Type I	1 or 2	1 or 2	4
Type II	1 or 2	2	4
Type III	1 or 2	X	4
Magnetic Disks			
Floppies, Zip drives	1, 2, or 3	X	4
Bernoulli Boxes	1, 2, or 3	X	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	X	X	4
Write Once, Read Many (WORM)	X	X	4
Read Many, Write Many	3	X	4
Other			
Floptical	X	X	4
Helical-scan Tapes	X	X	4
Cartridges	X	X	4
Optical	X	X	4

*Procedures listed are for storage media that have been used to process and/or store/contain classified information.

†Program offices are responsible for developing cleaning, 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 Products List of the NSA *Information Systems Security Products and Services Catalogue*.

Procedures: †

1. Degauss with a Type 1 degausser.§
2. Degauss with a Type 2 degausser.§
3. Overwrite all locations with a character, its complement, then with a random character.
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.

X. No procedure authorized.

TABLE 2. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZING, AND DESTROYING ELECTRONIC MEMORY DEVICES*

MEDIA TYPE†	CLEARING†	SANITIZING‡	DESTROYING‡
Magnetic Bubble Memory	3	1, 2, or 3	11
Magnetic Core Memory	3	1, 2, or 3	11
Magnetic Plated Wire	3	3 and 4	11
Magnetic-Resistive Memory	3	X	11
Read-Only Memory (ROM)	X	X	11 (see 12)
Random Access Memory (RAM) (Volatile)	3 or 5	5, then 10	11
Programmable ROM (PROM)	X	X	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

*The procedures listed are for electronic memory devices that have been used to process and/or store/contain classified information.

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

‡Numbers refer to the numbers in 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 Products List of the NSA *Information Systems Security Products and Services Catalogue*.

Procedures:‡

1. Degauss with a Type 1 degausser. §
2. Degauss with a Type 2 degausser. §
3. Overwrite all locations with a character, its complement, then with a random character.
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).
9. Check with ISSO or designee to determine whether additional procedures are required.
10. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed.
11. Destruction required only if ROM contained a classified algorithm or classified data.

X. No procedure authorized.

TABLE 3. DOE-APPROVED PROCEDURES FOR CLEARING, SANITIZING, AND DESTROYING HARDWARE*

MEDIA TYPE†	CLEARING‡	SANITIZING‡	DESTROYING‡
Printer Ribbons	1	1	6
Platens	X	2	6
Toner Cartridges	3	3	X
Laser Drums	4	3	6
Cathode-Ray Tubes (If there is Classified Burn-In)	X	X	6
Fax Machines	5	5	6

*The procedures listed are for hardware that have been used to process and/or store/contain classified information.
†Program offices are responsible for developing cleaning, sanitizing, and destroying procedures for media types not listed.
‡Numbers refer to the numbers in the procedures listed.

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. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure the media is physically destroyed.

X. Not applicable.

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

CONTRACTOR REQUIREMENTS DOCUMENT (CRD) APPLICABILITY

The Contractor Requirements Document for DOE N 205.12 is intended to apply to 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 Engineering & Environmental Laboratory

Thomas Jefferson Nat'l 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. The process of eradicating data on media before reusing it in an environment that provides an acceptable level of protection for the data that was on the media before clearing. All internal memory, buffer, or other reusable memory will be cleared to effectively deny access to previously shared information.

Degauss. To reduce magnetic induction to 0 (zero) by applying a reverse magnetizing field.

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

DOE-controlled environment. An area within DOE-controlled premises or within DOE contractor-controlled premises.

Internally transferred. Computer equipment that is to be transferred within DOE, but outside the direct line of authority (i.e., outside of an organizational department). 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, but if it were to be transferred to someone in DOE but outside of the Office of Cyber Security, it must be cleared first.

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

Removable media. Media that is not attached to information systems via the internal buss of the information system.

Overwriting. A procedure to destroy data from storage media by recording patterns of meaningless data over that which is stored on the media. The approved overwrite procedure is to overwrite all locations three times—the first time with a character, the second time with its complement, and the third time with a random character. For example, overwrite first with "00110101," followed by "11001010," and then "10101101."

Sanitization. The process of removing the data from media before it is reused in an environment that does not provide an acceptable level of protection for the data that was stored in the media before sanitizing. Information system resources will be sanitized before they are released from classified information controls or released for use at lower classification levels.