MANUAL

DOE M 205.1-6

Approved: 12-23-08
Admin Chg 1: 9-1-09
Admin Chg 2: 12-22-09

MEDIA SANITIZATION 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

MEDIA SANITIZATION MANUAL

1. PURPOSE.

   a. To establish for all Departmental operating units, programs, and systems the minimum technical and management requirements for the sanitization of electronic media, hardware, and devices so as to ensure adequate protection of sensitive and/or national security information.

   b. To describe the major elements of sanitization (clearing, purging, and destruction) of information system storage media, memory devices, and other hardware and establish a risk-based approach to sanitization.

   c. To provide direction 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 (NSA) Evaluated Products List (EPL).

2. CANCELLATIONS. None.

3. APPLICABILITY.

   a. All Departmental Elements. Except for the exclusions in paragraph 3c, this Manual applies to Departmental elements that utilize Federal Information Systems (hereafter called DOE Information Systems) to collect, process, store, display, create, disseminate, or transmit classified or unclassified information, including those created after the Manual is issued. (Go to www.directives.doe.gov/pdfs/reftools/org-list.pdf for the current listing of Departmental elements.)

   The Administrator of the National Nuclear Security Administration (NNSA) will ensure that NNSA employees and contractors comply with their respective responsibilities under this Manual. Nothing in this Manual will be construed to interfere with the NNSA Administrator's authority under section 3212(d) of Public Law (P.L.) 106-65 to establish Administration-specific policies, unless disapproved by the Secretary.

   b. DOE Contractors.

      (1) Except for the exclusions in paragraph 3c, the contractor requirements document (CRD), Attachment 1, sets forth requirements of this Manual that will apply to contracts that include the CRD.

      (2) The CRD must be included in contracts that involve information systems that are used or operated on behalf of DOE, including NNSA, to collect,

possess, store, display, create, disseminate, or transmit national security or unclassified DOE/ Government information.

(3) This Manual does not automatically apply to other than site/facility management contracts. Application of any of the requirements of this Manual to other than site/facility management contracts (e.g., contracts that involve DOE Information Systems and contain DEAR clause 952.204-2, *Security Requirement*s) will be communicated as appropriate through Heads of field elements and Headquarters Departmental elements and Contracting Officers.

c. Exclusions.

(1) Consistent with the responsibilities identified in Executive Order (E.O.) 12344, section 7, the Director, Naval Nuclear Propulsion Program will ensure consistency throughout 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) Systems designated as intelligence systems are subject to the requirements of Director of National Intelligence Directives and Intelligence Community Directives and are therefore excluded from the requirements of this Manual.

4. REQUIREMENTS.

a. Senior DOE Management, as defined in DOE O 205.1A, *Department of Energy Cyber Security Management*, dated 12-4-06, can add to or strengthen these requirements for their own organizations, based on their assessment of risk, so long as any additional direction they provide to their organizations is consistent with these requirements and does not diminish the scope or effect of these DOE-wide requirements in any way.

b. Senior DOE Management Program Cyber Security Plans (PCSPs) will require their operating units to implement and maintain at least the minimum requirements in this Manual for DOE information systems no later than 6-30-2010. If an operating unit cannot implement the requirements of this Manual by the scheduled milestone, the operating unit must establish a plan of action and milestones (POA&M) for implementation of the requirements.

c. The requirements of this Manual are in addition to those outlined by DOE M 205.1-4, *National Security Systems*, and any other DOE directive issued by the CIO on security controls for unclassified information systems, and do not relieve any organization from the requirements for sanitization as outlined by these DOE directives.

Vertical line denotes change.

5. RESPONSIBILITIES. This Manual is composed of chapters that provide direction for the processes, assignment of responsibilities, and supplemental requirements for sanitizing (i.e., clearing, purging, and destroying) information system storage media, memory devices, and other hardware.

   a. The head of the departmental element is responsible for ensuring that the CRD at Attachment 1 is included in all contracts that involve information systems used or operated by a contractor or other organization on behalf of DOE, including NNSA, to collect, process, store, display, create, disseminate, or transmit national security or unclassified DOE/ Government information. Once notified, the contracting officer is responsible for incorporating the CRD into each affected contract.

   b. The heads of departmental elements are responsible for notifying contracting officers of affected site/facility management contracts to incorporate this directive into those contracts. Once notified, contracting officers are responsible for incorporating the CRD into each affected contract via the *Laws, Regulations, and DOE Directives* clause of the contracts within 90 days.

   c. The functional roles and responsibilities associated with implementing this Manual are described in Chapter II.

6. REFERENCES.

   a. Office of Management and Budget (OMB). Circulars are available online at http://www.whitehouse.gov/OMB/circulars/index.html

      OMB Circular A-130, Management of Federal Information Resources, Circular A-130, November 2000.

   b. National Security.

      (1) National Security Directive (NSD) 42, National Policy for the Security of National Security Telecommunications and Information Systems, dated July 5, 1990.

      (2) National Security Telecommunications and Information Systems Security Advisory Memorandum INFOSEC 1-99, *The Insider Threat to U. S. DOE information Systems*, dated July 1999.

      (3) National Security Agency, Media Destruction Guidance and Approved media sanitization products at http://www.nsa.gov/ia/government/mdg.cfm.

      (4) NSA/CSS website for Media Destruction Guidance and Evaluated Products List at http://www.nsa.gov/ia/government/mdg.cfm.

c. National Institute of Standards and Technology (NIST)–Special Publications. Find NIST Special Pubs at http://csrc.nist.gov/publications/PubsSPs.html.

(1) NIST Special Publication 800-88, *Guidelines for Media Sanitization*, dated September 2006.

(2) NIST Special Publication 800- 36 Guide to Selecting Information Technology Security Products, dated October 2003.

d. DOE Directives. Find directives online at www.directives.doe.gov**.**

(1) DOE P 205.1, *Departmental Cyber Security Management Policy*, dated 5-8-01.

(2) DOE O 205.1A, *Departmental Cyber Security Management*, dated 12-4-06.

(3) DOE O 243.1, *Records Management Program*, dated 2-03-06.

(4) DOE O 470.4A, *Safeguards and Security Program*, dated 5-25-07.

(5) DOE O 471.1A, *Identification and Protection of Unclassified Controlled Nuclear Information*, dated 6-30-00.

(6) DOE O 471.3, *Identifying and Protecting Official Use Only Information*, dated 4-9-03.

(7) DOE M 205.1-4, *National Security System Manual*, dated 3-8-07.

e. Other.

(1) Title XXXII of P.L. 106-65, National Nuclear Security Administration Act, as amended, which established a separately organized agency within the Department of Energy.

(2) Title 44, United States Code, Chapter 35, Subchapter III, § 3547. National security systems.

(3) Title III, P.L. 107-347, Federal Information Security Management Act (FISMA), enacted December 2002.

(4) Clinger-Cohen Act of 1996 (40 U.S.C. 1401(3)), also known as the Information Technology Management Reform Act of 1996, (Public Law 104-106), February 1996.

(5) Atomic Energy Act of 1954 as amended by the Energy Reorganization Act of 1974.

Vertical line denotes change.

(6) E-Government Act of 2002 (Public Law 107-347), December 2002.

7. DEFINITIONS.

a. Clearing: The 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. Destruction: The result of actions taken to ensure that media cannot be reused as originally intended and information is virtually impossible or prohibitively expensive to recover.

c. Operating Unit: An Operating Unit is a subordinate element, such as a program office, field office, or contractor, reporting to an Under Secretary, the Department of Energy Chief Information Officer, the Power Marketing Administrations, or Heads of Departmental Elements.

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

e. Sanitization: A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means. Sanitization now encompasses clearing, purging, and destruction of storage media.

f. Sensitive Unclassified Information (SUI): Unclassified information requiring protection mandated by policy or laws, such as Official Use Only (OUO), Export Control Information (ECI), Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Power Information (NNPI), Personally Identifiable Information (PII), and other information specifically designated as requiring SUI protection (e.g. sensitive unclassified Cooperative Research and Development Agreements (CRADA) information).

g. Storage Media: Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, LSI memory chips, and printouts (excluding display media) onto which information is recorded, stored, or printed within an information system.

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

BY ORDER OF THE SECRETARY OF ENERGY:

JEFFREY F. KUPFER
Acting Deputy Secretary

CONTENTS

CHAPTER I. REQUIREMENTS FOR SANITIZATION

1. INTRODUCTION. In addition to the requirements stated in Sections 2 and 3 and in the Tables below, standards and procedures for sanitization (i.e., clearing, purging, or destroying) information system storage media, memory devices, and other hardware will include the following—

   a. Procedures for the handling and control of media, electronic devices, and hardware prior to clearing, purging, or destruction will be documented.

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

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

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

   e. Completed purging processes will be verified as follows—

      (1) No fewer than 5 percent of the purged media are sampled on a random basis to verify that the purging process has been successfully completed.

      (2) The verification is conducted by individuals other than those performing the purging processes. Additionally, these individuals must have a DOE clearance appropriate for the highest level and classification of information that he/she may view as a result of purging activities.

      (3) The completion and verification of the purging process are documented.

   f. The requirements for removing information from storage media, memory devices, and related hardware will be included in the awareness program and reviewed with all users.

   g. Process, sanitization, and quality control documentation will be maintained as records in accordance with DOE Records Schedule.

2. PROCEDURES FOR MEDIA CLEARING, PURGING, AND DESTRUCTION.

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

(1) 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 for technology and media used in classified processing. Refer to www.nsa.gov.

(2) 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 for technology and media used in unclassified processing. Refer to www.nist.gov.

(3) Technologies and media types not listed in the tables or references are referred to the DOE Chief Information Officer (CIO) for defining minimum clearing, purging, and destroying requirements and processes.

b. Unclassified Storage Media Processes.

(1) Storage media that is no longer in use, has been used for sensitive unclassified information (SUI) processing, and is not protected with Federal Information Processing Standard (FIPS) 140-2 Level 1 or higher encryption will be tracked and controlled until it is destroyed or all locations are overwritten with a pseudorandom pattern twice and followed by overwriting with a known pattern.

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

(3) Storage media that is no longer in use, has been used in SUI processing, and is not protected with FIPS 140-2 Level 1 or higher encryption will be tracked and destroyed if the unclassified information is located in bad sectors and the storage media cannot be purged or overwritten with a pseudorandom pattern twice and followed by overwriting with a known pattern.

(4) In addition to the clearing processes listed in Tables 1 through 3, processes to clear unclassified storage media will include the following:

(a) Storage media hosting DOE/ Government information will be cleared if it will be reused by a potential user who has a different authority for access, including need-to-know.

(b) Only overwriting software and hardware that are compatible with the media to be overwritten (i.e., matched to the media, considering the make, model, and manufacturing date) will be used.

Vertical line denotes change.

(c) One-pass overwrites with a pseudorandom pattern are sufficient for clearing storage media that does not contain SUI.[1]

(d) Individuals performing storage media clearing containing SUI that has not been protected with FIPS 140-2 Level 1 or higher encryption will certify and document successful completion of the process in accordance with DAA approved procedures by affixing a label to the storage media. The label will uniquely identify the storage media. At a minimum, the documentation will include—

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

2 information type with the highest confidentiality impact hosted on the media prior to clearing;

3 purpose of clearing (e.g. reuse, release, etc.);

4 procedure used; and

5 date, printed name, and signature of the certifying individual.

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

(a) Unclassified storage media will be reviewed, and approved for public release, in accordance with Senior DOE Management or operating unit procedures or purged if the media is to be released to the public without review.

(b) Unclassified storage media will be purged prior to reuse on a system containing information that has a security category (confidentiality impact) less than its current use.

(c) Individuals performing storage media purging will certify and document that the purging process has been successfully completed in accordance with the DAA approved procedure by affixing a label to the storage media. The label will uniquely identify the storage media. At a minimum, the documentation will include—

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

[1] For SUI: Overwrite all locations with a pseudorandom pattern twice and then with a known pattern.

2 information type with the highest confidentiality impact hosted on the media prior to clearing;

3 purpose of purging;

4 procedure used; and

5 date, printed name, and signature of the certifying individual.

(d) Storage media that cannot be purged will be destroyed.

c. Classified Storage Media Processes.

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

(2) Decision and handling processes regarding reuse of classified storage media at lower classification levels will include formal risk and cost analyses and testing and will be documented. Justification will be provided to describe the operational need for usage at a lower classification level.

(3) In addition to the clearing processes listed in Tables 1 through 3, processes to clear classified storage media will include the following—

(a) 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 will be cleared.

(b) Only overwriting software and hardware that are compatible with media (i.e., matched to the media, considering the make, model, and manufacturing date) to be overwritten will be used.

(c) Individuals performing storage media clearing will certify and document that the clearing process has been successfully completed in accordance with the DAA approved procedure by affixing a label to the storage media. The label will uniquely identify the storage media. At a minimum, the documentation will include—

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

2 most restrictive information group hosted prior to clearing;

Vertical line denotes change.

3 purpose for clearing;

4 procedure used; and

5 date, printed name, and signature of the certifying individual.

(4) In addition to the purging processes listed in Tables 1 through 3, processes to purge classified storage media will include the following—

(a) Classified storage media will be purged prior to reuse at a less restrictive information group or in an unclassified environment.

(b) Classified storage media that contains data in bad sectors or cannot be purged will be destroyed.

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

(d) Individuals performing classified storage media purging will certify and document that the purging process has been successfully completed in accordance with DAA approve procedure by affixing a label to the storage media. The label will uniquely identify the storage media. At a minimum, the documentation will include—

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 procedure used; and

5 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 (0-350 Oersteds)	1, 2, or 3	1, 2, 3, or 4	5
Type II (351-750 Oersteds)	1, 2, or 3	2, 3, or 4	5
Type IIA (751-1000 Oersteds)	2 or 3	3 or 4	5
Type III (1001-1700 Oersteds)	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.

§All degaussing products used to clear or purge media will 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.* The degaussing product must have a higher coercivity than the media being cleared or sanitized in it.

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.

Note: Degaussing any current generation hard disk will render the drive permanently unusable.

Vertical line denotes change.

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 electronic memory devices	X	X	9

‡Numbers in the table refer to the processes listed.

§All degaussing products used to clear or purge media will 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*. The degaussing product must have a higher coercivity than the media being cleared or sanitized in it.

Processes: ‡

1. Degauss with a NSA approved Type 3 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	X	X	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 then 3	X	5
Personal Digital Assistant (PDA) (Palm, Pocket PC, etc)	6 then 3	X	5
Routers/ Copy machines	6 then 3	X	5
All other hardware	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 devices/equipment 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. Note: All copies printed for clearing and purging purposes will be destroyed as classified waste.
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. No process authorized.

3. REUSING CLASSIFIED STORAGE MEDIA IN AN UNCLASSIFIED ENVIRONMENT.

a. Reuse of classified storage media and associated risk mitigation strategies will be identified in the system security plan (SSP) of the system where the media is being reused and the media will be tracked/controlled until it is destroyed.

b. The classified storage media will be purged by overwriting the entire storage media, at a minimum, using the three-pass overwrite process described in Table 1, Process 4.

Vertical line denotes change.

(1) The software used for purging will provide information about sectors overwritten and bad sectors that cannot be overwritten.

(2) Quality controls will be documented and deployed for review of overwrite process results and verification that all the classified information was completely overwritten.

(3) The classified storage media will be destroyed if any sectors on the storage media cannot be purged (i.e. bad sectors exist).

c. Individuals performing classified storage media purging will certify and document that the purging process has been successfully completed in accordance with DAA- approved procedures by affixing a label to the storage media. The label will uniquely identify the storage media. At a minimum, the documentation will include—

(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) procedure used; and

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

4. EQUIVALENCIES AND EXEMPTIONS. Requests for equivalencies and exemptions from the requirements of this Manual must be supported with a risk assessment that identifies the risks to be accepted, compensatory measures, and alternative controls to be implemented.

a. Equivalencies. Equivalencies are approved conditions that technically differ from a requirement in this Manual but afford DAA-approved equivalent levels of protection either with or without compensatory measures.

(1) Equivalency requests must be submitted in writing to the cognizant DAA and include detailed description of the requirement(s) and rationale for the equivalency. The equivalency documentation will be included or referenced in the system security plan (SSP).

(2) The cognizant DAA will review and approve or disapprove the equivalency with comments and recommendations in writing.

(3) Equivalencies will be approved for no longer than 3 years, can be extended through request resubmission and must be documented or referenced in the SSP.

b. Exemptions. Exemptions are approved deviations from a requirement in this Manual that may create a security vulnerability. Exemptions will be approved only when correction of the condition is not feasible or cost effective and compensatory measures are inadequate to preclude the acceptance of risk.

(1) Requests for exemptions and supporting documentation must be submitted in writing by the DAA to the cognizant Senior DOE Management for review and approval. Documentation supporting the exemption request and DAA's acceptance of associated residual risk must identify the requirements that cannot be met, compensatory measures implemented, and compensatory measures performance testing to validate the compensatory measures.

(2) The cognizant Senior DOE Management will review and approve or disapprove the exemption request and provide a final decision in writing to the DAA. A copy of the approved exemption will be provided to the DOE CIO.

(3) Approved exemptions will remain in effect no longer than 3 years and must be documented or referenced in the SSP.

Vertical line denotes change.

CHAPTER II. ROLES AND RESPONSIBILITIES

1. DOE UNDER SECRETARIES, INCLUDING THE NNSA ADMINISTRATOR.

   a. Ensure the implementation of this Manual by the operating units under their purview for all DOE Information Systems.

   b. Determine the need for and develop any additional requirements to this Manual for the operating units under their purview and ensure that the operating units implement those requirements.

   c. Ensure that contracting officers are notified to incorporate the CRD into affected contracts.

2. HEADS OF DEPARTMENTAL ELEMENTS (OTHER THAN UNDER SECRETARIES).

   a. Ensure the implementation of this Manual by the operating units under their purview for all DOE Information Systems.

   b. Determine the need for and develop any additional requirements to this Manual for the operating units under their purview and ensure that the operating units implement those requirements.

   c. Ensure that contracting officers are notified to incorporate the CRD into affected contracts.

   d. Review procurement requests for new non-site/facility management contracts that involve DOE Information Systems and contain DEAR clause 952.204-2, *Security Requirements*. If appropriate, ensure that the requirements of the CRD of this Manual are included in the contract.

3. OPERATING UNIT MANAGERS.

   a. Develop any requirements in addition to this Manual as well as any additional requirements imposed by Senior DOE Management and ensure that those requirements are implemented on all DOE Information Systems under their cognizance.

   b. Ensure the implementation of this Manual by all organizations, including contractors, under their purview.

   c. Ensure that the contracting officers are notified to incorporate the CRD into affected contracts.

4. DOE CHIEF INFORMATION OFFICER. In addition to the responsibilities as a Senior DOE Manager, as described in paragraph 2 above—

a. Complete an annual review of this Manual and update as necessary.

b. Define clearing, purging, and destroying processes for technologies and media types not listed in the tables or references of this Manual, that have been referred to the DOE CIO.

5. CONTRACTING OFFICER.

a. Once notified of contractor applicability, incorporate the CRD into affected contracts.

b. Assist originators of procurement requests who want to incorporate the requirements of the CRD of this Manual in new non-site/facility management contracts, as appropriate.

Vertical line denotes change.

CONTRACTOR REQUIREMENTS DOCUMENT
DOE M 205.1-6, *MEDIA SANITIZATION MANUAL*

This contractor requirements document (CRD) establishes the requirements for Department of Energy (DOE) contractors whose contracts involve DOE Information Systems that collect, process, store, display, create, disseminate, or transmit information.

Regardless of the performer of the work, the contractor is responsible for implementing and complying with the requirements of this CRD and the applicable Senior DOE Management Program Cyber Security Plan (PCSP).

The contractor is responsible for 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.

Contractor managers or system owners may specify and implement additional requirements to address specific risks, vulnerabilities, or threats within its operating unit/ systems.

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

ADMIN CHANGE

DOE M 205.1-6 Chg 1

Approved: 12-23-08
Admin Chg 1: 9-1-09

SUBJECT: MEDIA SANITIZATION MANUAL

1. PURPOSE. To transmit the revised page to DOE M 205.1-6, *Media Sanitization Manual,* dated 12-23-08.

2. EXPLANATION OF CHANGES. This change amends the date for Senior DOE Management Program Security Plans to require their operating units to implement and maintain at least the minimum requirements of the Manual for information systems operated by or on behalf of the Department.

3. LOCATION OF CHANGE.

Page	Paragraph
ii	4.b.

After filing the attached pages, this transmittal may be discarded.

BY ORDER OF THE SECRETARY OF ENERGY:

KEVIN T. HAGERTY
Director
Office of Information Resources
Office of Management

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

ADMIN CHANGE

DOE M 205.1-6 Chg 2

Approved: 12-23-08
Admin Chg 1: 9-1-09
Admin Chg 2: 12-22-09

SUBJECT: MEDIA SANITIZATION MANUAL

1. PURPOSE. To transmit the revised page to DOE M 205.1-6, *Media Sanitization Manual,* dated 12-23-08.

2. EXPLANATION OF CHANGES. This change amends the date to facilitate the orderly transition to an improved Departmental cyber security governance structure following the cyber security management direction memorandum signed by the Deputy Secretary on December 7, 2009.

3. LOCATION OF CHANGE.

Page	Paragraph
ii	4.b.

After filing the attached pages, this transmittal may be discarded.

BY ORDER OF THE SECRETARY OF ENERGY:

KEVIN T. HAGERTY
Director
Office of Information Resources
Office of Management