National Nuclear Security Administration

**Policy Letter: NAP-14.16**
**Date: August 9, 2006**

TITLE: Clearing, Sanitizing, And Destroying Information System Storage Media, Memory Devices, And Other Related Hardware

1. OBJECTIVES. To establish National Nuclear Security Administration (NNSA) policy requirements and responsibilities for clearing, sanitizing, and destroying NNSA information system storage media, memory devices, and other related hardware hereafter referred to as storage media.

   a. To provide instructions for clearing, sanitizing, and destroying storage media to preserve the confidentiality of the stored information.

   b. To provide instructions for handling classified storage media that will be reused in controlled environments.

   c. To provide instructions for sanitizing storage media that has become contaminated with classified or unclassified sensitive information.

   d. To ensure that no unauthorized information can be retrieved from unclassified NNSA and DOE computer equipment and storage media that is to be transferred or declared surplus.

   e. To ensure that all NNSA element personnel are made aware of requirements for clearing, sanitizing, and destroying information system storage media, memory devices, and related hardware.

2. CANCELLATIONS. None. This policy is NNSA's implementation of DOE M 205.1-2, *Clearing, Sanitizing, and Destroying Federal Information System Storage Media, Memory Devices, and Other Hardware*, 6-26-05

3. APPLICABILITY. Except for the exclusions in paragraph 3e, this NNSA Policy (NAP) applies to all entities, Federal or contractor, that collect, create, process, transmit, store, and disseminate information for the NNSA.

a. NNSA Elements. NNSA Headquarters Organizations, Service Center, Site Offices, NNSA contractors, and subcontractors are, hereafter, referred to as NNSA elements.

b. Information System. This NAP applies to any information system that collects, creates, processes, transmits, stores, and disseminates unclassified or classified NNSA information. This NAP applies to any information system life cycle, including the development of new information systems, the incorporation of information systems into an infrastructure, the incorporation of information systems outside the infrastructure, the development of prototype information systems, the reconfiguration or upgrade of existing systems, and legacy systems. In this document, the term(s) "information system," Target of Evaluation (TOE), or "system" are used to mean any information system or network that is used to collect, create, process, transmit, store, or disseminate data owned by, for, or on behalf of NNSA or DOE.

c. Deviations. Deviations from the requirements prescribed in this NAP must be processed in accordance with the requirements in NAP 14.1-B, *NNSA Cyber Security Program.*

d. Site/Facility Management Contractors. Except for the exclusions in paragraph 3e, the Contractor Requirements Document (CRD), Attachment 1, sets forth requirements of this NAP 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 NNSA information systems.

(2) As the laws, regulations, and DOE and NNSA Directives clause of site/facility management contracts states, regardless of the perfomer 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—

i. Ensure that they and their subcontractors comply with the requirements of the CRD; and

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

e. Exclusions.

(1) The Deputy Administrator for Naval Reactors shall, in accordance with the responsibilities and authorities assigned by Executive Order 12344 (set forth in Public Law 106-65 of October 5, 1999 [50 U.S.C. 2406]) and to ensure consistency throughout the joint Navy and DOE Organization of the Naval Reactors Propulsion Program, implement and oversee all requirements and practices pertaining to this Order for activities under the Deputy Administrators cognizance.

(2) The requirements set forth in this Manual are not applicable to storage 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 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 the Government program security officer as promulgated in program security manuals.

4. IMPLEMENTATION. A plan for the implementation of this NAP must be completed within 60 days after modification of the site's contract to include this NAP. A plan for the implementation of this NAP within an NNSA federal organization must be completed within 60 days after issuance of this NAP.

5. REQUIREMENTS.

a. Implement the processes described in Attachment 1 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 or unclassified information.

b. Decisions to clear, sanitize, or destroy information system storage media, memory, and other related hardware must be based on the Consequence of Loss of confidentiality of the most sensitive information ever recorded on the storage media.

6. RESPONSIBILITIES. Roles and responsibilities for all activities in the NNSA PCSP are described in NAP 14.1-B, *NNSA Cyber Security Program.*

7. DEFINITIONS. See Attachment 2.

8. 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. Committee on National Security Systems Instruction No. 4009, *National Information Assurance Glossary*, revised May 2003

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

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

   g. DOE M 205.1-2, *Clearing, Sanitization, and Destruction of Information System Storage Media, Memory Devices, and Related Hardware Manual*, dated 6-26-05.

9. CONTACT. Questions concerning this Notice should be directed to the NNSA Cyber Security Program Manager, through the cognizant Cyber Security Office Manager, at 301-903-2425.

BY ORDER OF THE ADMINISTRATOR:

Linton Brooks

Administrator

Attachments

# ATTACHMENT 1

## CONTRACTOR REQUIREMENTS DOCUMENT

This Contractor Requirements Document (CRD) establishes the requirements for National Nuclear Security Administration (NNSA) contractors, with information systems that provide access to DOE/NNSA information. Contractors must comply with the requirements listed in the CRD.

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 processes in this CRD are to be used for clearing, sanitizing, and destroying information system storage media, memory, and other related hardware capable of recording information hereafter referred to as storage media. Processes for special circumstances for storage media are also identified. The processes set forth in this CRD are not applicable to storage media that have been used to process Special Access Program information or Sensitive Compartmented Information.

Any storage media used in classified or unclassified sensitive processing that will be released from a NNSA-controlled environment to a controlled environment within DOE or another agency that meets the NNSA requirements for protection of the information residing on the storage media must be transferred using the DOE Classified Matter and Protection Control processes for handling classified matter or DOE processes for the transmission of sensitive information.

1. CLEARING STORAGE MEDIA USED IN CLASSIFIED PROCESSING. Storage media has been used in classified processing and will be reused at the same or more restrictive Information Group, but by a user with a different Need-to-Know, must be cleared prior to reuse. The processes to clear storage media are described in Appendix A. Additionally:

    a. Only overwriting software that is compatible with the specific hardware intended for overwriting and approved by the cognizant Designated Approving Authority

(DAA) will be used. Use of such software will be coordinated in advance with the data steward.

b. Cleared storage media that has been used in classified processing must be protected by measures commensurate with the highest level and category of information it has ever contained.

c. Individuals involved in clearing storage media as listed in Appendix A, must also certify that the process has been successfully completed by documenting the following:

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

(2) Most restrictive Information Group prior to clearing;

(3) Purpose for clearing;

(4) The procedure used; and

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

2. SANITIZING STORAGE MEDIA USED IN CLASSIFIED PROCESSING. The processes to sanitize storage media that has been used in classified processing are described in Appendix A. Additionally:

a. Any storage media that will be reused at a less restrictive Information Group must be sanitized. Until sanitization is complete, classified storage media must remain in a physical environment suitable to protect the Information Group. Paragraph 5 below describes special circumstances for certain types of storage media.

b. Any storage media that has been used in classified processing must be tracked/ controlled until it is destroyed.

c. Classified storage media that has been sanitized may not be donated, sold, etc. (released from the DOE/NNSA environment) to outside organizations.

d. Storage media must be handled in accordance with classified matter or sensitive information processes and procedures until sanitized as directed in Appendix A.

e. Individuals involved in sanitizing storage media, as listed in Appendix A, 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 document:

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

(2) Most restrictive Information Group prior to sanitizing;

(3) Purpose for sanitizing;

(4) Provide a statement indicating that the equipment has been sanitized or contains no information that is not within the Open, Public, Unrestricted Access Information Group in accordance with this Policy;

(5) The cognizant DAA approved procedure used; and

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

f. The certifier must prepare separate documentation recording the same information and submit it to the cognizant authority defined in the site's Cyber Security Program Plan (CSPP) and retain this documentation for a minimum of 5 years.

3. DESTROYING STORAGE MEDIA USED IN CLASSIFIED PROCESSING. The processes to destroy storage media are described in Appendix A. Additionally:

a. Storage media that is no longer being used or needed for archiving and that has been used in classified processing must be destroyed.

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

c. Storage media must be handled in accordance with classified matter processes and procedures until destroyed as directed in Appendix A. Storage media that cannot be sanitized must be destroyed.

d. Methods for destroying storage media include pulverizing, smelting, incinerating, disintegrating, applying acid solutions, grinding, etc., as approved by the cognizant DAA.

4. APPROVED PROCESSES. NNSA-approved processes for clearing, sanitizing, and destroying information system storage media, memory devices, and related hardware that have been used to process, store, or contain unclassified or 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 must be based on the Consequence of Loss of confidentiality of the most sensitive information ever recorded on the storage media. The implementation of these processes and plans for clearing, sanitizing, and destroying information system storage media must be documented in the appropriate CSPPs, including the requirement for documented methods for independently verifying the clearing/sanitizing results.

5. SPECIAL CIRCUMSTANCES. The use of storage media in a lower classification or unclassified environment is described below.

   a. Reusing Classified Storage Media.

      (1) Reuse of storage media must be identified in the System Security Plan (SSP).

      (2) The storage media must be sanitized.

      (3) The decision to reuse storage 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. The testing, risk and cost analysis procedures must be documented in the Site's approved CSPP. Storage media are to be sanitized by overwriting the entire storage media using the three-pass process described in Appendix A of this CRD.

         (a) Sanitizing software must provide information about sectors overwritten and bad sectors that cannot be overwritten. If classified information is located in bad sectors, the storage media must be destroyed.

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

      (4) Storage media that has been used in classified processing, designated for reuse by local site management, must be sanitized. The Cyber Security Site Manager (CSSM) or designee must use a DAA-approved overwrite method, review the results of overwrites to verify that the method used completely overwrote all classified information, and document the review.

   b. Sanitizing Partially Contaminated Storage Media.

---

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

The NNSA Information Assurance Response Center (IARC)– Cyber Forensics Center, at no charge, to assist with the verification of sanitization of media.

(1) If non-removable storage media operated in unclassified environments (e.g. the TOE is accredited for any of the unclassified Information Groups) become contaminated with relatively small amounts of classified information (less than 20 megabytes of information and less than 0.001 percent of the capacity of the non-removable storage media), the affected areas may be sanitized using the three-pass process described in Appendix A of this CRD.

(2) If non-removable storage media operated in classified environments become contaminated with relatively small amounts of information from a more restrictive Information Group (less than 0.1 percent of the capacity of the non-removable storage media), the affected areas may be sanitized using the three-pass process described in Appendix A of this CRD.

(3) If non-removable storage media operated in the Open or Unclassified Protected environment become contaminated with relatively small amounts of Mandatory Protected information (less than 0.1 percent of the capacity of the non-removable storage media), the affected areas may be sanitized using the three-pass process described in Appendix A of this CRD.

(4) The cognizant DAA must approve all software used to perform overwrites.

(5) The cognizant CSSM or designee must approve the overwrite method, review the results of overwrites to verify that the method used completely overwrote all classified information, and document the review.

(6) The programs used to overwrite contaminated storage media must overwrite all contaminated locations, including temporary data file locations, file slack, free space, and directories, provide confirmation of overwrite of specified areas and of successful completion, and provide information about sectors overwritten and bad sectors that cannot be overwritten. If information from an Information Group containing classified information or the Unclassified Mandatory Protection Information Group is located in bad sectors or the storage media cannot be sanitized, the storage media must be destroyed.

## 6. CLEARING AND SANITIZING UNCLASSIFIED STORAGE MEDIA

a. CLEARING. Storage media that will be reused at the same or more restrictive Information Group, but by a user with a different Need-to-Know, must be cleared prior to reuse. The processes to clear storage media are described in Appendix A. Additionally:

(1) Only overwriting software that is compatible with the specific hardware intended for overwriting and approved by the cognizant DAA will be used. Use of such software will be coordinated in advance with the data steward.

(2) Before any NNSA- or DOE-owned or managed hard disks or systems containing hard disks are transferred internally to a recipient who does not have the same Need-to-Know, they must be cleared. This requirement also applies to equipment used for NNSA support.

(3) One-pass overwrites are sufficient for clearing unclassified computer storage media not containing information from the Unclassified Mandatory Protection Information Group.

(4) Individuals involved in clearing computer equipment must also certify that the process has been successfully completed by documenting the following:

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

(d) Most restrictive Information Group prior to clearing;

(e) Purpose for clearing;

(f) The procedure used; and

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

b. SANITIZING. The processes to sanitize storage media are described in Appendix A. Additionally:

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

(2) A minimum of three-pass overwrites are required for sanitizing unclassified computer storage media that contained Unclassified Mandatory Protection Information Group information.

(3) Individuals involved in 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 document:

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

(b) Most restrictive Information Group prior to sanitizing;

(c) Purpose for sanitizing;

(d) Provide a statement indicating that the equipment has been sanitized or contains no information that is not within the Open, Public, Unrestricted Access Information Group in accordance with this Policy;

(e) The cognizant DAA approved procedure used; and

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

c. DESTROYING UNCLASSIFIED STORAGE MEDIA The processes to destroy storage media are described in Appendix A. Additionally, storage media that is no longer being used or needed for archiving and that contains or did contain Unclassified Mandatory Protection or Unclassified Protected Information Group information must be destroyed if it cannot be sanitized.

(1) Storage media must be handled in accordance with the Information Group it contains until destroyed as directed in Appendix A.

(2) Methods for destroying storage media include pulverizing, smelting, incinerating, disintegrating, applying acid solutions, grinding, etc., as approved by the cognizant DAA

d. DONATED OR SURPLUS SYSTEMS. Systems or equipment declared surplus or donated to outside (civilian or non-DOE/NNSA) organizations must have their storage media sanitized.

(1) Prior to donation or surplus/disposal, cleared or sanitized hard drives intended for disposal or donation must be sampled, as documented in the CSPP, to validate that clearing or sanitization processes have been successfully completed.

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

(3) No fewer than 20 percent of all overwritten hard drives will be examined in the sampling process.

(4) Requirements for training, sampling, and verifying that the overwrite process is successful must be described in the CSPP.

7. TRAINING, EDUCATION, AND AWARENESS. Requirements for training personnel in clearing, sanitizing and destruction procedures; sampling procedures for

cleared and sanitized hard drives; and verification of the clearing and sanitizing process must be established in the site's CSPP.

a. All 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 at least annually.

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

# APPENDIX A

## TABLE 1. APPROVED PROCESSES 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 |
| Non-removable 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 | X | X | 4 |
| **Other** | | | |
| Floptical | X | X | 4 |
| Helical-scan Tapes | X | X | 4 |
| Cartridges | X | X | 4 |
| Optical | X | X | 4 |
| CD-R, -RW, -ROM | X | X | 4 or 6 |
| DVD | X | X | 4 or 6 |

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

†NNSA is responsible for developing cleaning, sanitizing, and destroying processes for media types not listed.

‡Numbers in the table refer to the processes listed.

# Acceptable for PII information also.

§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*.

**Processes:** †

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 with a known pattern..

4. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media arephysically destroyed.
5. Remove the entire recording surfaces by sanding or applying acid.
6. Grind surface of CD or DVD to ensure the entire recording surface is removed. Only NSA Group D equipment and associated processes approved for the specific media may be used.

X. No process authorized.

## TABLE 2. APPROVED PROCESSES FOR CLEARING, 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 |

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

†NNSA is responsible for developing clearing, sanitizing, and destroying processes for media types not listed.

‡Numbers in the table refer to the processes 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*.

**Processes:**‡

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 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 CSSO to determine whether additional processes 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.

X. No process authorized.

## TABLE 3. APPROVED PROCESSES FOR CLEARING, SANITIZING, AND DESTROYING HARDWARE*

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

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

†NNSA is responsible for developing cleaning, sanitizing, and destroying processes for media types not listed.

‡Numbers in the table refer to the processes listed.

**Processes:** †

1. Chemically clean so no visible trace of data remains.
2. Print at least five pages of randomly generated unclassified data. The pages should not include any blank spaces or solid black areas.
3. Print three blank copies. If unable to get a clean output, print an undassified test pattern or black copy; then run three blank copies.
4. For fax machines that have memory and other storage media incorporated, treat each component per processes listed in tables 1 and 2 of this appendix.
5. 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.
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.

# ATTACHMENT 2

## DEFINITIONS

**Clearing** Removal of data from an Information System, its 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); however, the data may be reconstructed using laboratory methods.

**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.

**NNSA-controlled environment**

An area within NNSA-controlled premises or within NNSA contractor-controlled premises.

**Non-removable media**

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

**Overwriting** A process to destroy data from storage media by recording patterns of meaningless data over that which is stored on the media. The approved overwrite process is to overwrite all locations three times—twice with a pseudorandom pattern and then a known pattern.

**PII** Any information about an individual maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace and individual's identity, such as their name, social security numbers, data and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or likable to an individual.

**Personal Computer**

A computer built around a microprocessor for use by an individual, as in an office or at home or school, without the need to be connected to a larger computer.

**Pseudorandom Number**

Of, relating to, or being a consistent, characteristic form of random numbers generated by a definite, nonrandom computational process.

**Removable media**

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

**Sanitization** The process of removing data from storage media such that data recovery is not possible.