NSA/CSS STORAGE DEVICE DECLASSIFICATION MANUAL

(This Manual 9-12 supersedes NSA/CSS Manual 130-2, dated 10 November 2000.)

PROCEDURES

1. Guidance for the sanitization, declassification, and release of IS storage devices not covered by this document may be obtained by submitting all pertinent information to NSA/CSS (Attn: LL43 Media Technology Center, 301-688-1053).

MAGNETIC STORAGE DEVICES

2. Magnetic Tapes

a. Sanitization: Sanitize magnetic tapes in accordance with either of the following procedures. Remove all labels or markings that indicate previous use or classification.

1) *Degaussing*: Degauss using an NSA/CSS evaluated *degausser* per Reference a.

2) Incineration: Incinerate magnetic tape in a licensed incinerator in accordance with the procedures established for the controlled destruction of classified or sensitive materials.

b. Declassification: Declassify magnetic tapes only after approved verification and review procedures are completed per Reference b.

c. Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified magnetic tapes may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

3. Magnetic Disks: Magnetic disks include hard disk drives and diskettes.

a. Hard Disk Drives

1) Sanitization: Sanitize hard disk drives using one of the following procedures. Remove all labels or markings that indicate previous use or classification.

a) Sanitization with Automatic Degausser: (1) Remove the hard disk drive from the chassis or cabinet; (2) remove any steel shielding materials or mounting brackets which may interfere with magnetic fields; (3) place the hard disk drive in an NSA/CSS evaluated degausser per

Reference a and erase. Although not required, it is highly recommended that the hard disk drive be physically damaged prior to release.

NOTE – ERASURE OF HARD DISK DRIVES CAUSES PERMANENT DAMAGE THAT PROHIBITS THEIR CONTINUED USE.

b) Sanitization with Degaussing Wand: Sanitize hard disk drives by disassembling the device and erasing all surfaces of the enclosed platters with an NSA/CSS evaluated hand-held degaussing wand per Reference a. Although not required, it is highly recommended that the hard disk drive be physically damaged prior to release.

NOTE – ERASURE OF HARD DISK DRIVES CAUSES PERMANENT DAMAGE THAT PROHIBITS THEIR CONTINUED USE.

c) Sanitization by Incineration: Incinerate hard disk drives in a licensed incinerator in accordance with the procedures established for the controlled destruction of classified or sensitive materials.

2) Declassification: Declassify hard disk drives only after approved verification and review procedures are completed per Reference b.

3) Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified hard disk drives may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

b. Diskettes

1) Sanitization: Sanitize diskettes by degaussing, shredding, or incineration. Remove all labels or markings that indicate previous use or classification.

a) Sanitization by Degaussing: Degauss the diskettes in an NSA/CSS evaluated degausser per Reference a.

b) Sanitization by Shredding: Shred diskettes using an NSA/CSS evaluated high security crosscut paper shredder, per Reference e. Remove diskette cover and metal hub prior to shredding.

c) Sanitization by Disintegration: Disintegrate diskettes using an NSA/CSS evaluated high security disintegrator per Reference d.

d) Sanitization by Incineration: Incinerate diskettes in a licensed incinerator in accordance with the procedures established for the controlled destruction of classified or sensitive materials.

2) Declassification: Declassify diskettes only after approved verification and review procedures are completed per Reference b.

3) Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified diskettes may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

OPTICAL STORAGE DEVICES

4. Optical storage devices include Compact Disks (CD) and Digital Versatile Disks (DVD)

a. Sanitization: Sanitize optical storage devices using one of the following procedures. Remove all labels or markings that indicate previous use or classification.

1) Sanitization by Grinding: Use an NSA/CSS evaluated optical storage device grinder, per Reference c, to remove the information bearing layers of only CD storage devices. DVD’s cannot be sanitized by this method since the information bearing layers are sandwiched in the center.

2) Sanitization by Shredder or Disintegrator: Use an NSA/CSS evaluated optical storage device shredder per Reference c, or disintegrator per Reference d, to reduce CD and DVD storage devices into particles that have nominal edge dimensions of 5 millimeters or less and surface area of 25 square millimeters or less.

3) Sanitization by Embossing/Knurling: Use an NSA/CSS evaluated optical storage device embosser/knurler, per Reference c, for CD and DVD storage devices.

4) Sanitization by Incineration: Incinerate optical storage devices in a licensed incinerator in accordance with the procedures established for the controlled destruction of classified or sensitive materials. Material must be reduced to white ash.

b. Declassification: Declassify optical storage devices only after approved verification and review procedures are completed per Reference b.

c. Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified optical storage devices may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

SOLID STATE STORAGE DEVICES

5. Solid State Storage Devices include Random Access Memory (RAM), Read Only Memory (ROM), Field Programmable Gate Array (FPGA), Smart Cards, and Flash Memory.

a. Sanitization: Sanitize solid-state devices with the following procedures or sanitize by smelting in a licensed furnace at 1,600 degrees Celsius or higher or disintegrate into particles that are nominally 2 millimeter edge length in size using an NSA/CSS evaluated disintegrator per Reference d. Remove all labels or markings that indicate previous use or classification.

1) DRAM and SRAM: Sanitize DRAM and SRAM by removing the power. Once power is removed, sanitization is instantaneous. Or, sanitize functioning DRAM and SRAM by overwriting all locations with a known unclassified pattern. Verify the overwrite procedure by randomly re-reading the overwritten information to confirm that only the known pattern can be recovered.

2) Ferro-electric Random Access Memory (FRAM) and Magnetic Random Access Memory (MRAM) (Non-Volatile): Sanitize functioning FRAM and MRAM by overwriting all locations with a known unclassified pattern. Verify the overwrite procedure by randomly re-reading the overwritten information to confirm that only the known pattern can be recovered.

3) EPROM and UVEPROM: Sanitize EPROM and UVEPROM by performing an ultraviolet erase according to the manufacturer's recommendations, but increase the time requirement by a factor of three. Next, overwrite all bit locations with a known unclassified pattern.

4) EEPROM: Sanitize EEPROM by overwriting all locations with a known unclassified pattern. Verify the overwrite procedure by randomly re-reading the overwritten information to confirm that only the known pattern can be recovered.

5) PROM: Sanitize only by smelting.

6) FPGA (Non-Volatile): Sanitize FPGA by overwriting all locations with a known unclassified pattern. Verify the overwrite procedure by randomly re-reading the overwritten information to confirm that only the known pattern can be recovered.

7) FPGA (Volatile): Sanitize FPGA by removing the power. Once power is removed, sanitization is instantaneous.

8) Smart Cards: Sanitize Smart Cards by shredding with a strip shredder or with scissors.

a) Sanitization with a Strip Shredder: A strip shredder with a maximum width of 2 millimeters will destroy the microchip, barcode, magnetic strip and written information on the Smart Card. Smart Cards must be inserted diagonally into the strip shredder at a 45-degree angle for proper sanitization.

NOTE: A CROSS CUT SHREDDER WILL NOT SANITIZE SMART CARDS.

b) Sanitization with Scissors: Cut the Smart Card into strips diagonally at a 45-degree angle, insuring that the microchip is cut through the center. Insure that the barcode, magnetic strip, and written information are cut into several pieces and the written information is unreadable.

9) Flash Memory: Sanitize EEPROM by overwriting all locations with a known unclassified pattern. Verify the overwrite procedure by randomly re-reading the overwritten information to confirm that only the known pattern can be recovered.

b. Declassification: Declassify solid-state storage devices only after approved verification and review procedures are completed per Reference b.

c. Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified solid-state storage devices may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

HARD COPY STORAGE DEVICES

6. Hard Copy Storage Devices include paper, microforms, and monitors with *burn-in*.

a. Sanitization: Sanitize hard copy storage devices with the following procedures.

1) Sanitize paper by burning, chopping, crosscut shredding using an NSA/CSS evaluated crosscut shredder, per Reference e, pulverizing, or wet pulping. When burned, material residue must be reduced to white ash. When chopping, shredding, pulverizing, or wet pulping, material residue must be reduced to pieces 5 millimeters square or smaller.

2) Sanitize microforms (microfilm, microfiche, or other reduced image photo negatives) by burning or by chemical means, such as immersion in household bleach (i.e., sodium hypochlorite) for film masters and acetone or methylene chloride for diazo reproductions. When burned, material residue must be reduced to white ash.

3) Sanitize monitors exhibiting burn-in by destroying the surface of the monitor into pieces no larger than 5 centimeters square.

b. Declassification: Declassify hard copy storage devices only after approved verification and review procedures are completed per Reference b.

c. Release: Unless otherwise specified by the appropriate IS Security Officer (or equivalent), declassified hard copy storage devices may be released for disposal or recycling only after sanitization procedures and a declassification review have been completed.

RESPONSIBILITIES

7. Logistics Services Media Technology Center shall provide technical guidance for the sanitization, declassification, and release of IS storage devices.

8. NSA/CSS and all elements using this manual shall:

a. Protect classified or sensitive information, and make final decisions to declassify or release IS storage devices or refer to their IS security officer for guidance;

b. Establish and maintain a compilation of guidance and procedures for the sanitization, declassification, and release of classified or sensitive information on IS storage devices; and

c. Comply with the Director of Central Intelligence Directive (DCID) 6/3, "Protecting Sensitive Compartment Information Within Information Systems Manual," dated 11 December 2003 (Reference f).

REFERENCES

9. References:

a. NSA/CSS Degausser Evaluated Products List.

b. NSA/CSS Manual 130-1, Annex D, "Declassification & Release of NSA/CSS Information Storage Media".

c. NSA/CSS Specification 04-02, "Optical Media Destruction Devices," and EPL 04-02 Evaluated Products List.

d. NSA/CSS Specification 02-02, "High Security Disintegrators," and EPL 02-02 Evaluated Products List.

e. NSA/CSS Specification 02-01, "High Security Crosscut Paper Shredders".

f. Director of Central Intelligence Directive (DCID) 6/3, "Protecting Sensitive Compartment Information Within Information Systems Manual".

DEFINITIONS

10. Burn-In - A tendency for an image that is shown on a display over a long period of time to become permanently fixed on the display. This is most often seen in emissive displays such as Cathode Ray Tube (CRT) and Plasma, because chemical changes can occur in the phosphors when exposed repeatedly to the same electrical signals.

11. Coercive Force – A negative or reverse magnetic force applied for the purpose of reducing magnetic flux density.

12. Declassification - An administrative decision/action, based on a consideration of risk by the owner, whereby the classification of a properly sanitized storage device is downgraded to UNCLASSIFIED.

13. Degausser - An electrical device or permanent magnet assembly which generates a *coercive* magnetic *force* for the purpose of degaussing magnetic storage devices or other magnetic material.

14. Degaussing (or Demagnetizing) - Process for reducing the magnetization of a magnetic storage device to zero by applying a reverse (coercive) magnetizing force, rendering any previously stored data unreadable and unintelligible, and ensuring that it cannot be recovered by any technology known to exist.

15. Information System (IS) Storage Devices - The physical storage devices used by an IS upon which data is recorded.

16. Recycling – End state for IS storage devices processed in such a way as to make them ready for reuse, adapt them to a new use, or to reclaim constituent materials of value.

17. Sanitization - The removal of information from the storage device such that data recovery using any known technique or analysis is prevented. Sanitization includes the removal of data from the storage device, as well as the removal of all labels, markings, and activity logs. The method of sanitization varies depending upon the storage device in question, and may include degaussing, incineration, shredding, grinding, embossing, chemical immersion, etc.