U.S. Customs and Border Protection

Attachment Y

Media Sanitization Procedures

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version Number	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release is based solely on existing 1400-05C, Version 2.1 appendices which were found to be unrelated to existing DHS 4300A, Version 6.1.1 attachments. The policy content of this attachment is exactly the same as the 1400-05C, Version 2.1 appendix. It is now presented in the attachment format.
2.0	December 21, 2010	No changes

CONTENTS

This section addresses media procedures for Sensitive-But-Unclassified (SBU) data only. The sanitization of classified media storage devices is not covered within the scope of this document. Please refer to the *CBP National Security Systems Handbook* for procedures relating to classified media.

1.0 Destination of Released Media

There is an increased risk of compromise of sensitive data when magnetic storage media are released outside of the CBP environment. If improperly cleansed, magnetic media falls into hostile possession, methods could be employed to recover data from the media.

2.0 Mechanical Storage Device Equipment Failure

The effectiveness of overwrite procedures may be reduced because of equipment failure or mechanical faults, such as misalignment of read/write heads. Hardware preventive maintenance procedures must be performed on schedule and records must be maintained in an effort to prevent this problem.

3.0 Storage Device Segments Not Receptive to Overwrite

A compromise of sensitive data may occur when an addressable segment of a storage device (e.g., a disk drive) is not receptive to overwrite. A disk platter may have bad tracks or sectors marked for no read/write operation, but data may have been previously recorded in these areas (before the areas were marked bad). In this situation, the platter must be destroyed to ensure removal of the information.

4.0 Computer Programs Designed to Overwrite

Overwrite programs must be designed and developed by competent systems programmers familiar with the rules for declassification. To ensure strict compliance with procedures, engineers must test such programs in a laboratory environment.

5.0 Security Inspection and Release Authority

Sanitizing and releasing IT equipment (e.g., workstations, hard drives, and laptops) containing sensitive-but-unclassified information are auditable events. This is to ensure that proper procedures have been followed before releasing magnetic storage media. This improves the chance of preventing the inadvertent release of sensitive information.

In order to initiate the excessing or releasing of any magnetic storage media, the owner of the equipment must notify the Local Property Officer (LPO). All excessing/disposal of personal property must be coordinated through the LPO. The LPO must complete a disposal package to ensure that the disposal of the asset is properly documented.

In order to initiate the disposal process, the LPO completes the Standard Form SF120 – *Report of Excess Personal Property* that documents the property being released. A Helpdesk ticket may then be entered to document that the Automated Data Processing (ADP) equipment was sanitized by an official LAN administrator or an email may be generated to document that the LAN

administrator properly sanitized the equipment. This documentation is attached to the disposal package. Proper sanitization requires that the LAN administrator use an approved utility that is part of the CBP Technical Reference Model (TRM). A CBP Form 7610, *Certification of Retirement – CBP Excess of Personal Property* must be completed by the LPO and attached to the SF120 as another part of the disposal package.

There is a box on the CBP Form 7610 that requires the LPO to document that the ADP equipment listed on the SF120 was sanitized. The CBP Form 2001 documenting that the media is ready for excessing/disposal is no longer required. The LPO retires the equipment in SAP, which means the record remains in SAP, but does not appear on active inventories. The CBP Form 7610 is used to document the release of components, sub-components and the formal release of a complete system. The releasing LPO at the site must retain the completed disposal package for a period of at least three years after the release date of the property. For more information, see Chapter 9 of the *Personal Property Management Handbook*, CIS HB 5200-13A.

Oversight of the sanitization of ADP equipment is the responsibility of the Information Systems Security Officer (ISSO) assigned to the General Support System (GSS). The actual records of the clearing, sanitization, and disposition of sensitive storage media are maintained by the LPO, but the ISSO should have access to the sanitization documentation as required.

6.0 How to Cleanse, Release, and Ship

All storage media must be processed in accordance with Table J.6, Rule-Based Table for Disposal and Shipment of Components before being considered for release within CBP or to other non-CBP users or to salvage. The rule-based procedures defined in Table J.6 are the decision rules for cleansing, sanitizing, destroying, overwriting, releasing and shipping actions.

CAUTION

If the item being cleansed, sanitized or released is not in Table J.6, do not assume it does not require processing. Contact the STP Branch (b)(6) (b)(7)(C) for further directions. Use the rule-based procedures contained in Table J.6 for all cleansing, sanitizing, and releasing decisions.

Table J.6: Disposal and Shipping of Storage Devices

Media Type	Destroy	Overwrite	Release
Magnetic Tape	Rule 1	N/A	N/A
Floppy Disk	Rule 1	N/A	N/A
Optical Disk (CD-ROMs)	Rule 15	N/A	N/A
Removable Hard Disks	Rule 4	N/A	N/A
Disk Packs	Rule 4	Rule 2	Rule 15
Removable Hard Drive	Rule 6	Rule 5	Rule 15
Fixed Hard Drive	Rule 6	Rule 5	Rule 15
Solid State (Volatile)	Rule 3	Rule 3	Rule 15
Solid State (Non-Volatile)	Rule 3	Rule 3	Rule 15
Mag Drum	Rule 8	Rule 2	Rule 15
Bubble Memory	Rule 7	Rule 2	Rule 15
Mag Core	Rule 9	Rule 9	Rule 15
Thin Film	Rule 10	Rule 2	Rule 15
Platens	Rule 12	N/A	N/A
Ribbons	Rule 1	N/A	N/A
Laser Toner Cartridge	Rule 13	N/A	N/A
Cassette/Magnetic Card	Rule 1	N/A	N/A
CRT	Rule 11	N/A	N/A
PDAs/PEDs	Rule 16	Rule 16	Rule 16

7.0 Rules for Cleansing, Releasing and Shipping

Rule 1. Destruction of Expendable Items

Expendable items (e.g., floppy diskettes or other portable storage media) cannot be released for reuse outside of CBP. Rather than jeopardize security, destroy the item if it is damaged or no longer deemed usable. Remove the recording media (e.g., magnetic Mylar, film, ribbons) from any outside container (e.g., reels, casings, hard cases or soft cases, envelopes). Dispose of the outside container in a regular trash receptacle. Cut the recording media into pieces and then dispose of it in a regular trash receptacle. A crosscut chipper/shredder may be used to cut the media into pieces, if such is available. When cost prohibitive to manually destroy individually, use of an authorized vendor to dispose expendable recording media by shredding following policy in Rule 1 is permissible. If an authorized vendor is used, the designated ISSO will have oversight responsibility to ensure that the approved destruction of expendable items procedures are followed.

Rule 2. Overwrite and Overwrite Verification Procedures for Storage Media

To overwrite vendor-supplied programs such as the FDISK utility program for MS-DOS, remove any partitions that may be on the media. Next, reformat the storage media using a vendor-supplied program such as the MS-DOS FORMAT program. Overwrite all possible storage locations on the media a minimum of three times. Overwrite the media completely with binary "1"s on the first overwrite, with binary "0"s on the second overwrite and with random characters on the third overwrite. Perform a second FORMAT of the storage media after the last overwrite. This entire overwrite procedure must be performed or supervised by the LAN administrator. The ISSO has oversight responsibility. In many cases, multiple overwrite of the drive shall be sufficient to allow transfer.

Rule 3. Power-Down Procedure for Release of Solid State Memory Media

For any storage media containing integrated electronic components, execute the overwrite and verification procedure then remove all batteries and power. If capacitances discharge time is known for the particular storage unit, power down the unit for twice the time it takes the unit to drop to ten percent of its total required electrical power. (For example, if a unit normally operates at 110 volts and it takes 5 seconds for the unit to drop to 11 volts after shutdown, double the 5 seconds and the required time is 10 seconds.) If the discharge time is not known, power down the storage media for a minimum of one hour. If the device cannot be overwritten, verified, and/or subjected to power up/down, the device cannot be considered for declassification or release.

If the overwrite and verification procedures as stated cannot be accomplished for any reason, then power the unit up and down for three times with one minute in between each "ON" and each "OFF," then remove all batteries and power down the storage media for a minimum of 72 hours prior to release. If damage to the end item could result from application of the power up/down procedure above, a bench power supply may be used to apply and remove power. If unable to power a defective component, competent authority must consider the risk.

Rule 4. Destruction of Removable Hard Disks and Disks Packs

Removable hard disks are expendable items and cannot be released for reuse outside of CBP. Because of the costs, disk packs may be released if the item is required for further use. Removable hard disks, if damaged or no longer deemed usable, must be destroyed. If the platter(s) of a defective unit can be removed, do so if the removal is cost-effective. Destruction of a removable hard disk consists of dismantling the exterior case and removing the platter from the case. Place the exterior case in a normal trash disposal. Local destruction of the platter no longer requires removing the magnetic surface by sanding. It is now acceptable for the use of approved electromagnetic degausser to be used to sanitized broken hard drives as referenced in DHS 4300B National Security Systems Handbook, Attachment U Media Reuse and Disposition. When either the cost of the approved electromagnetic degausser or a high number of broken hard-drives for the FTO to manually destruct make it cost-prohibitive, sending the broken-hard-drives to National Security Agency / Classified Material Conversion (NSA/CMC) is an acceptable alternate solution when following the approved documented procedures located at http://www.nsa.gov/cmc/.

Rule 5. Reuse of Operative Fixed Hard Disk Drives

Hard disk drives are not expendable items and depending upon their sensitivity or classification level, they may not be authorized for release or reuse outside of CBP. Each fixed hard disk drive is considered categorized to the highest level of data stored or processed on the system in which it was used. If the hard disk drive processed sensitive information and it is to be released for reuse, follow the overwrite procedure described in Rule 2 and release the unit intact as unclassified using a SF120 and coordinating with the Local Property Officer (LPO) while referencing the "Property Management Handbook." If the unit processed sensitive information and it is not being released for reuse, treat it as broken and process it for release using Rule 6.

Rule 6. Release of Broken Disk Drives

Disk drives may be released for service or repair after removing the storage media and completing the power-down procedure as stated in Rule 4. Hard disk drives, fixed or removable, are expendable items. However, because they contain storage media, broken drives they may not be authorized for release for reuse outside of CBP. Each hard disk drive shall be protected to the highest level of data stored or processed on the system in which it was used.

Rule 7. Sanitizing and Release of Magnetic Bubble Memory Modules

If the storage media are operable, the LAN administrator will perform or oversee the procedure described in Rule 3. The ISSO will ensure the procedure was completed. An alternate procedure for bubble memory modules, with a built-in bias voltage control is to raise the bias voltage to a level that will cause the collapse of all magnetic bubbles. If the memory was designed with a bias control, the vendor can supply the bias voltage level required to cause the collapse of all of the magnetic bubbles. This procedure must be executed and verified in the same manner as the Overwrite and Overwrite Verification Procedures described in Rule 2.

Rule 8. Sanitizing and Release of Magnetic Drums

If the storage media are operable, the LAN administrator must perform or oversee the procedure described in Rule 3. The ISSO will ensure the procedure was completed.

Rule 9. Sanitizing and Release of Magnetic Core

The LAN Administrator or ISSO will use a modified Rule 3 to ensure that magnetic core memory is overwritten a minimum of three times. Use a random character the first time, a special character the second time, and the third time use the complement of the character used the second time.

Rule 10. Sanitizing and Release of Thin Film Memory

If the storage media are operable, Rule 3 applies.

Rule 11. Sanitizing and Release of Cathode Ray Tubes

A Cathode Ray Tube (CRT) can be considered sanitized if visual inspection reveals that no legible sensitive information has been etched into the CRT phosphor. If the CRT is defective and cannot be purged of sensitive information, a trained technician should remove and destroy the tube and break its vacuum seal.

Rule 12. Sanitizing and Release of Printer Platens

Before a printer that has processed sensitive information is released to any property disposal channel, remove its platen (the roller in a computer printer against which the print head strikes). Remove the rubber surface of the platen by carving, scraping, sanding, or other feasible methods and then place it in a regular trash receptacle

Rule 13. Disposal of Laser Toner Cartridges

Destruction of laser toner cartridges is not authorized. Each cartridge must be recycled.

Rule 14. Disposal of Optical Disks (CD-ROMs)

When no longer needed, optical disks that were created within CBP containing any form of CBP information must be smashed, broken, rendered useless, and dropped into regular trash. To avoid copyright violations, the same rule applies to optical disks that contain obsolete commercial-off-the-shelf software.

Rule 15. Shipping

For sensitive and unclassified material, use First Class Mail of the United States Postal Service to any location.

Rule 16. Sanitization of Handheld devices

All known information, i.e., address book, to-do list, email, etc will be manually deleted. Any removable mass storage media must be removed from the device. The PDA/PED will be reset to a default factory state. The LAN Admin will have to contact the specific vendor for specific procedures. Before the handheld device is reissued by the Local Property Officer (LPO), the sanitization must be confirmed. In the event it is not possible to reset the model to a default factory state, the PDA/PED will be destroyed.

8.0 Cleansing Storage Media at a Commercial Recovery Facility

Storage Media used in a commercial recovery facility shall be cleansed in accordance with the procedures detailed in this section.

Cleansing removes sensitive information from information system storage media in a manner that renders it unrecoverable by normal system utilities or non-technical means. Routines that only remove pointers and leave data intact (i.e., delete or format) are not acceptable methods of cleansing storage media. Media can be cleansed for reuse within the same information system and environment where the media is reused.

Commercial Recovery Facility Physical Environment

The physical environment must be constructed to meet the requirements of CIS HB 1400-02A Physical Security Handbook and controlled by personnel with a BI 24/7/365 to the equivalency of a CBP Level 1 facility with the addition of a monitored alarm system 24/7. Provision of storage devices is necessary for the continued operation at the Commercial Recovery Facility.

Personnel with continuous access (i.e. maintenance, guard force, alarm system monitors, and facility maintenance personnel) must have successfully undergone a Background Investigation (BI) by government security services.

Procedures for Cleansing

1. **Magnetic Tapes** - Although magnetic tapes can be overwritten (reel and cassette formats), this method of cleansing is not preferred because it is time consuming and inter-record gaps may preclude proper cleansing. The preferred method for cleansing tapes is to degauss them with a Type I or Type II degausser. If degaussers are not available, overwrite tapes to cleanse them. Select the highest density available for the tape transport and the largest blocking factor supported by the equipment. Verify overwrites by randomly reading media to ensure nothing other than the overwrite character is present.

2. **Floppy Disks, Diskettes, and Magnetic Cards** - Cleanse flexible magnetic media and cards by overwriting or degaussing. Overwrite all addressable locations at least one time with a single character. Degauss flexible media using either a Type I or hand-held degaussing wand.

3. **Sealed Disk Drives[1], Hard Disks, Hard Drive Assemblies (HDAs), Removable Cartridge Drives, and PC (Memory) Cards** - These devices are widely used for storage of digital information. Functioning sealed drives may be cleansed by employing an overwrite procedure as below:

    a. Functioning sealed drives and removable cartridge drives may be cleansed by overwriting all addressable locations with binary zeros (i.e., 0000 0000) then binary ones (i.e., 1111 1111). Then, overwrite all addressable locations with any character (i.e., "a").

    b. Verify the overwrite procedure by randomly re-reading (recommend 10%) the overwritten information to confirm that only the overwrite characters can be recovered.

    c. This media may also be cleansed using a Type II degausser.

    d. For sanitization of non-functioning classified drives see rules listed in Table J.6.

4. **Removable Disk Packs** - Removable disk packs may be cleansed by means of an overwrite cycle, in accordance with procedures described for sealed disk drives. An alternative method to cleanse disk packs is to degauss the recording surfaces of all platters with an approved large cavity degausser or a hand-held degaussing wand.

5. **Magnetic Drums** - Cleanse according to established procedures for sealed disk drives.

[5] Unlike magnetic tape and floppy disks, where the read/write heads come in direct contact with the recording media, sealed disk drives contain rigid magnetic media and implement a "flying head" arrangement where the read/write head is designed to float above the surface of the recording media. A "head crash" means that the heads have contacted the media, resulting in catastrophic system failure and permanent damage to both the heads and the recording media