ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE

June 4, 2001

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Disposition of Unclassified DoD Computer Hard Drives

References: (a) Deputy Secretary of Defense Memorandum, "Destruction of DoD Computer Hard Drives Prior to Disposal," dated January 8, 2001
(b) Deputy Secretary of Defense Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," dated May 29, 2001

Reference (a) directed that immediate steps be taken to ensure that all hard drives of unclassified computer equipment being disposed of outside the Department of Defense (DoD) be removed and destroyed. Reference (b) directed that the January 8, 2001 guidance be amended to provide Department-wide procedures, methods and specifications regarding the disposition of unclassified hard drives, to include allowing hard drives to be overwritten before leaving DoD custody or control. However, while meaningful information cannot be recovered from a hard drive that has been properly overwritten with qualified software, there may be situations where the nature of the unclassified information (e.g., law enforcement) is such that the preferred course of action is to degauss or destroy the hard drive in question.

Attachment 1 specifies methods and procedures for santization and provides guidance on disposition of hard drives, depending on ownership. Attachment 2 provides specifications for overwriting, degaussing or destruction. Attachments 3 and 4 provide definitions and examples of verification labels and destruction records, respectively.

Components are to take immediate steps to implement the guidance in the attachments, including arranging for required training and certification of personnel. All contracts for computer support initiated after September 30, 2001 must comply with the guidance. This office will examine the feasibility of enterprise licensing of qualified overwriting software.

Additional guidance regarding this subject will be issued as necessary. Questions concerning this memorandum or the attachments may be directed to Mr. Donald Jones, OASD(C3I), at (703) 614-6640.

Linton Wells II
Acting

Attachments

Disposition of Unclassified DoD Computer Hard Drives

Sanitization and Disposition of Unclassified Computer Hard Drives

1. Purpose: This attachment provides specific guidance on methods, processes and procedures to ensure no data remains on unclassified computer hard drives that are to be permanently removed from DoD custody. It addresses disposition of hard drives in three cases:

- DoD owned computers;
- Leased computers; and,
- Warranty repair or replacement (DoD owned or leased computers)

The attachment outlines specific procedures and steps for hard drive sanitization in the three cases, including consideration of whether the storage device is operable or inoperable and cost effectiveness, as appropriate. Attachment 2 provides detailed specifications and guidance to support sanitization by overwriting, degaussing, or destruction. The term "user" herein refers to the DoD organization with effective ownership or control of a hard drive, not an individual using a computer.

2. Methods and procedures for hard drive sanitization and clearing:

2.1. Overwriting is the process of replacing information (data) with meaningless data in such a way that meaningful information cannot be recovered from a hard drive. Software meeting the specifications are outlined in Attachment 2, paragraph 2.1., Overwriting Software Specifications, will be used to overwrite all DoD owned or controlled hard drives. The individual performing the overwriting must be properly trained and will be responsible for certifying that the process has been successfully completed. Once overwriting has been certified, a signed label verifying that the drive has been purged will be affixed to the hard drive or the computer housing the hard drive, as appropriate. The certifier will maintain separate documentation recording the same information for a minimum of five years. Overwritten hard drives will also be sampled on a random basis by a trained individual other than the one who performed the overwrite process to verify that the overwriting process has been successfully completed. No fewer than 20% of all overwritten hard drives will be examined in the sampling process. See Attachment 4 for examples of an acceptable verification label and required documentation.

2.2. Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux of a medium to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable. For specific instructions on degaussing procedures and where to obtain a listing of approved degaussing products, see Attachment 2, paragraph 3, Degaussing Procedures. Individuals performing degaussing will certify that the process has been completed by affixing a

signed verification label to the hard drive or the computer housing the hard drive, as appropriate, indicating the date and degaussing product used for the procedure. Persons performing the degaussing function must be properly trained and certified. Separate documentation recording the same information will be maintained for a minimum of five years. Supervisory personnel should closely monitor the degaussing process.

2.3. Destruction of a hard drive is the process of physically damaging a medium so that it is not usable in a computer and so that no known exploitation method can retrieve data from it. For acceptable methods of destruction, refer to Attachment 2, paragraph 4., Physical Destruction Procedures. Destruction of hard drives will be certified by affixing a signed label to the computer indicating the date and method of destruction. The certifier will maintain separate documentation recording the same information for a minimum of five years.

2.4. Clearing data (deleting files) removes information from storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by technical means, it is not an acceptable method of sanitizing DoD owned or controlled unclassified hard disk storage media.

3. Disposition: Hard drives may be scheduled for reuse, repair, replacement, or removal from service for a variety of reasons and disposed of in various ways as described below.

3.1. Government-owned hard drives:

3.1.1. Operable hard drives that will be reused must be overwritten in accordance with (IAW) the procedures in paragraph 2.1. above, prior to transfer. If the operable hard drives are to be removed from service completely for any reason, they should also be destroyed or degaussed IAW paragraph 2.2. or 2.3. above. Figure 3.1-1. highlights the process flow for the disposition of operable Government-owned hard drives.

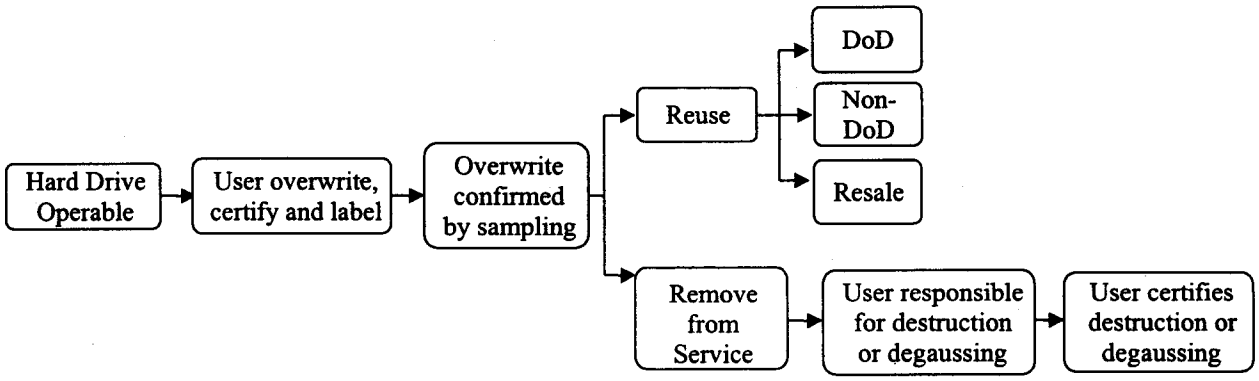

Figure 3.1-1. Purging an Operable DoD-Owned Hard Drive

3.1.2. If the hard drive is inoperable and has reached the end of its useful life, it will be destroyed or degaussed IAW paragraph 2.2. or 2.3. above. Figure 3.1-2. highlights the process flow for the disposition of inoperable Government-owned hard drives.

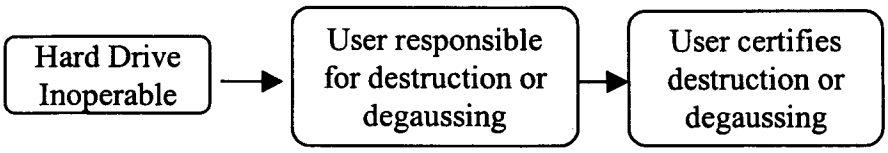

Figure 3.1-2. Purging an Inoperable DoD-Owned Hard Drive

3.2. Leased computers, including assets provided under service level agreements:

3.2.1. If the leased hard drive is operable, and is simply being relocated within a contract umbrella (i.e., it will remain under the authority of the DoD leasing agent or seat manager), overwrite is not required. However, if the hard drive is to be redirected from the contract umbrella, then the leasing agent/seat manager will overwrite, certify, and label the hard drive IAW paragraph 2.1. above.

3.2.2. If the leased hard drive is inoperable, the contractor will make a determination as to whether the hard drive is repairable or should be removed from service.

3.2.2.1. Repaired leased hard drives that are returned to the user need not be overwritten. If the hard drive is not returned to the user specified in the contract, the contractor will certify to the DoD leasing agent/seat manager that the hard drive has been overwritten using an approved DoD process and product.

3.2.2.2. If the hard drive is determined to be not repairable and is to be removed from service, the contractor may degauss or destroy the hard drive, or return the drive to DoD for degaussing or destruction, depending on the terms of the lease agreement. If the contractor is responsible for the destruction or degaussing of the drives, the contractor will certify in writing that this process has been completed IAW one of the methods specified in Attachment 2. If the inoperable hard drive is returned to DoD for destruction, the procedures outlined in paragraph 3.1.2. above will be followed.

3.2.3. Figure 3-2.1. highlights the process flow for the disposition of hard drives which have been leased or provided under a service level agreement:

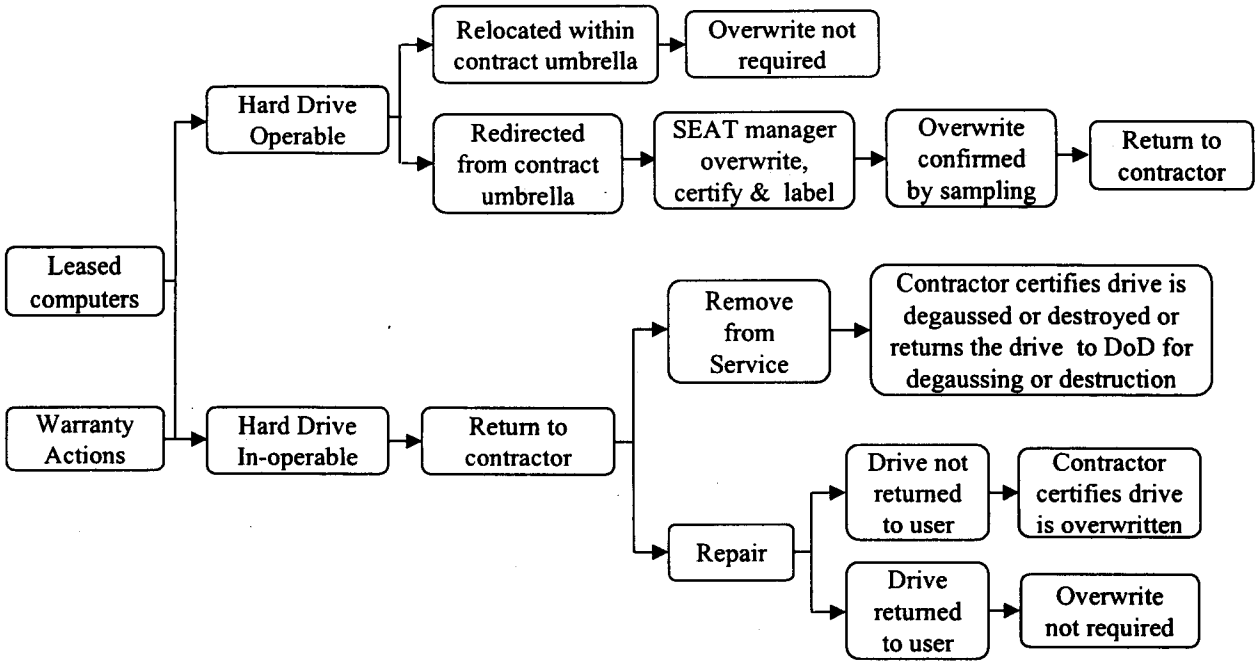

Figure 3.2-1. Purging Hard Drives That Have Been Leased and Warranty Actions.

3.2.4. All new contracts initiated after September 30, 2001 must accommodate the requirements in paragraphs 3.2.1. and 3.2.2.

3.3. Warranty Actions: The warrantor will make a determination as to whether the hard drive is to be repaired and returned to the original Government user, repaired but redirected to another user, or permanently removed from service. The processes and procedures for handling inoperable hard drives that are returned for warranty action are exactly the same as those for inoperable hard drives that are returned to the contractor under lease agreements as shown in Figure 3.2-1.

4. Certain storage technologies are such that data are saved across an array of hard drives in a manner that results in no intelligible information being recoverable from any single drive (i.e., each byte is spread among different drives on the array). In these situations, where individual drives are removed from an array for repair or replacement, there is no requirement to overwrite, degauss, or destroy the drive in question.

Disposition of Unclassified DoD Computer Hard Drives

Specifications For Sanitization Of Hard Drives

1. Purpose: This attachment provides guidance on sanitization by overwriting, degaussing and destruction of unclassified hard drives. Components may supplement these specifications to meet their operational needs. System users will ensure supplemental instructions to this policy meet with the approval of the responsible Designated Approving Authority (DAA). Sanitization removes sensitive information from storage media in a manner that gives assurance that the information cannot be recovered by keyboard or laboratory attack. Before the sanitization process begins, the computer should be disconnected from any external network to prevent accidental damage to the network operating system (OS) or other files on the network. In addition, users should audit the sanitizing process to ensure data is no longer retrievable. This means a trained knowledgeable person should witness the sanitization process and verify that the hard drive was sanitized.

2. Overwriting Hard Drives for Sanitization: Overwriting is an approved method for sanitization of hard disk storage media containing unclassified data. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable, but the process must be correctly understood and carefully implemented. Overwriting consists of recording data onto magnetic media by writing a pattern of fluxes or pole changes that represent binary ones (1) and zeros (0). These patterns can then be read back and interpreted as individual bits, 8 of which are used to represent a byte or character. If the data is properly overwritten with a pattern (e.g., "11111111" followed by "00000000") the magnetic fluxes will be physically changed and the drives read/write heads will only detect the new pattern and the previous data will be effectively erased. To purge the hard drive, the DoD requires overwriting with a pattern, and then its complement, and finally with another pattern (e.g., overwrite first with "00110101", followed by "11001010", then "10010111"). Sanitization is not complete until all six passes of the three cycles are completed.

2.1. Overwriting Software Specifications: The software specifications discussed below are the minimum that Components must apply to overwriting hard drives. Software products and applications not meeting the minimum stated specifications are not acceptable for sanitizing unclassified hard drives. Overwriting software that merely reformats or repartitions a hard drive is not accepted within the scope of this policy. Further, some software products may not run on systems with lower end central processing unit (CPU) chipsets, and may require a minimum of a 386 or greater processor. Software users should verify the compatibility of selected software products

with the particular hard disk being sanitized. In addition, some software product versions may not have the capability to remove the OS during the overwriting process. To ensure the integrity of the sanitization process, overwriting software must have the following functions and capabilities:

2.1.1. The ability to purge all data or information, including the OS, from the physical or virtual drives, thereby making it impossible to recover any meaningful data by keyboard or laboratory attack.

2.1.2. A compatibility with, or capability to run independent of, the OS loaded on the hard drive.

2.1.3. A compatibility with, or capability to run independent of, the type of hard drive being sanitized (e.g., ATA/IDE or SCSI type hard drives).

2.1.4. A capability to overwrite the entire hard disk drive independent of any BIOS or firmware capacity limitation that the system may have.

2.1.5. A capability to overwrite using a minimum of three cycles (six passes) of data patterns on all sectors, blocks, tracks, and slack or unused disk space on the entire hard disk medium.

2.1.6. A method to verify that all data has been removed from the entire hard drive and to view the overwrite pattern.

2.1.7. Although not mandatory, selected software should also:

2.7.1.1. Provide the user with a validation certificate indicating that the overwriting procedure was completed properly.

2.7.1.2. Provide a defects log, or listing of any bad sectors, that could not be overwritten by the software.

2.2. Software Available for Overwriting: Listed below are products and manufacturers that produce overwriting software tools. These products are currently in use by DoD Components and are considered to meet the minimum standards called out in this policy. Note: This listing is not all-inclusive and there may be other products that meet the required specifications in addition to the products listed below.

2.2.1. Product Name: "No Trace"
Communication Technologies, Inc.,
14151 Newbrook Drive, Suite 400, Herndon, VA 20170
Tel: (703) 961-9080
Fax: (703) 961-1330
Web: www.comtechnologies.com

2.2.2. Product Name: "DataEraser"
ONTRACK Data International, Inc.
9023 Columbine Road, Eden Prairie, MN 55347
Toll Free: 1 (800)-872-2599
Tel: 1 (952) 937-5161
Fax: 1 (952) 937-5750
Web: www.ontrack.com
Technical Support: 1 (952) 937-2121

2.2.3. Product Name: "UniShred Pro"
Los Altos Technologies,
1381 Kildaire Farm Road, Suite 415, Cary, NC 27511
Toll Free: 1 (800) 999-8649
Tel: 1 (919) 233-9889
Fax: 1 (919) 233-6761
Web: www.lat.com
Technical Support: 1 (919) 223-9889

2.2.4. Product Name: "CleanDrive"
Access Data Corporation
2500 North University Ave., Suite 200, Provo, UT 84604-3864
Toll Free: 1 (800) 574-5199
Tel: 1 (801) 377-5410
Fax: 1 (801) 377-5426
Web: www.accessdata.com
Technical Support: 1 (800) 489-5199

2.2.5. Product Name: "Sanitizer" D 4.01
Infraworks
6207 Bee Cave Road Austin, TX 78746
Tel: 1 (512) 583-5000
Fax: 1 (512) 583-5075
Web: www.infraworks.com/products/santizer.html

2.3. Damaged Hard Disks: A hard disk platter may develop damaged or unusable tracks and sectors. However, sensitive data may have been recorded in areas of the disk that should be purged. If features or malfunctions of the storage media inhibit overwriting, the storage media should be degaussed or destroyed.

3. Degaussing Hard Drives for Sanitization: Degaussing is a process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack.

3.1. Degaussing hard drives often destroys the drive's timing tracks and servo motors, and usually demagnetizes the permanent magnets of the spindle motor on sealed (e.g., Winchester) drives, thus they can seldom be used after degaussing. In addition, the process of removing the hard drives from the computer, taking off the hard drive's housing, degaussing and placing the hard drive back into the computer, and testing to ensure it still operates and no longer contains its original data, may make reutilization after degaussing cost ineffective.

3.2. Each type of magnetic media is distinguished by the rate of coercivity required to ensure the medium is brought back to its zero state. Due to the variation of media formats and their corresponding magnetic densities, a correct and effective degaussing process is often difficult to achieve, and it is essential that DoD Components utilize a degausser with the right coercivity specifications to degauss the target media. Coercivity strength of an applied magnetic field determines which type of degausser should be applied to the particular magnetic media being targeted for sanitization. Higher coercivity rates are usually required to degauss hard disk storage media and many degaussers designed for commercial uses do not have the magnetic energy required to erase media with a higher coercivity rate.

3.3. Degaussing standards and procedures:

3.3.1. Degaussers used on DoD hard drives must have a nominal rating of at least 1700 Oersted.

3.3.2. Degaussers must be operated at their full magnetic field strength.

3.3.3. Follow the product manufacturer's directions carefully. Deviations from an approved method or rate of coercivity could leave significant portions of data remaining on a hard drive.

3.3.4. All shielding materials (e.g., castings, cabinets, and mounting brackets), which may interfere with the degausser's magnetic field, must be removed from the hard drive before degaussing.

3.3.5. Hard disk platters must be in a horizontal direction during the degaussing process.

3.3.6. For degaussing hard drives with very high coercivity ratings, it may be necessary to remove the magnetic platters from the hard drive's housing.

3.4. Degaussing products should be acquired from the National Security Agency's (NSA) Degausser Products List which can be obtained by contacting:

National Security Agency
Attn: S7 Media Technology Center
9800 Savage Road, Ft. George G. Meade, MD 20755-6877
Tel: 1 (800) 688-6115 (Option #3) or 1 (410) 854-7661
Fax: 1 (410) 854-7668

4. Physical Destruction Procedures: Hard drives should be destroyed when they are defective or cannot be economically repaired or sanitized for reuse. As an added security measure, when practical, operable hard drives no longer deemed economically viable should be overwritten or degaussed prior to destruction. Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive. The following are acceptable means for destruction of hard disk storage media:

4.1. Physical destruction/impairment beyond reasonable use: Remove the hard drive from the chassis or cabinet. Remove any steel shielding materials, mounting brackets, and cut any electrical connection to the hard drive unit. In a suitable facility with individuals wearing appropriate safety equipment, subject the hard drive to physical force (e.g., pounding with a sledgehammer) that will disfigure, bend, mangle, or otherwise mutilate the hard drive so that it cannot be re-inserted into a functioning computer. Sufficient force should be used directly on top of the hard drive unit to cause shock/damage to the disk surfaces. In addition, any connectors that interface into the computer must be mangled, bent, or otherwise damaged to the point that the hard drive could not be re-connected without significant rework

4.2. Destruction at an approved metal destruction facility, i.e., smelting, disintegration, or pulverization.

4.3. Application of an abrasive substance (emery wheel or disk sander) to a magnetic disk or drum recording surface. Make certain that the entire recording surface is completely removed. Ensure proper safety measures to include protection from inhaling abraded dust and use of protective eyewear.

44. Application of concentrated hydriodic acid (55% to 58% solution) to a gamma ferric oxide disk surface. Acid solution use should be done in a well-ventilated area, and personnel must wear eye protection.

4.5. Application of acid activator Dubais Race A (NSN 8010 181 7171) and stripper Dubais Race B (NSN 8010 181 7170) to a magnetic drum recording surface. Technical acetone (NSN 6810 184 4796) should then be applied to remove residue from the drum surface. The above should be done in a well-ventilated area, and personnel must wear eye protection.

NOTE: Extreme caution must be observed when handling acid solutions. The application of chemical substances to remove data should be accomplished only by qualified and approved personnel.

Disposition of Unclassified DoD Computer Hard Drives

Definitions

Clearing – Rendering stored information unrecoverable unless special utility software or techniques are used.

Coercivity – Defines the magnetic field necessary to reduce a magnetically saturated material's magnetization to zero. Coercivity strength of an applied magnetic field determines which type of degausser may be applied to a particular type of magnetic material. Demagnetizing the magnetic material of data storage media removes data remanence.

Degaussing – Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used as a method of sanitization.

Erasing – An ambiguous term which can refer to purging, clearing, or removing file allocation.

Keyboard attack – Extracting information from data storage media by executing software utilities, keystrokes, or other system resource executed from a keyboard. For example, disk and file recovery utilities and memory scavenging procedures can be used to carry out keyboard attacks.

Laboratory attack – Using sophisticated signal recovery equipment in a laboratory environment to recover stored information from data storage media.

Media – Short for storage media. Physical objects on which data can be stored, such as hard drives, floppy disks, CD-ROMs, and tapes.

Memory Scavenging – Searching through data storage to collect residue thereby acquiring data. Data may be stored on records, blocks, pages, segments, files, directories, words, bytes, fields, or peripheral devices, such as printers or video displays.

Overwriting – Process of writing patterns of data on top of the data stored on a magnetic medium.

Oersted – A unit of magnetic field strength.

Remanence – Residual information remaining on data storage media after clearing.

Sanitize – To expunge data from storage media (e.g., diskettes, CD-ROMs, and tapes) so that data recovery is impossible. Sanitizing includes overwriting, degaussing and destruction. Clearing data does not constitute sanitizing.

Sensitive Information – "Sensitive" information is any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (The Privacy Act), but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information in routine DoD payroll, finance, logistics, and personnel management systems. (Certain information that the disclosure of which would constitute an unwarranted invasion of personal privacy is exempt from mandatory disclosure under the Freedom of Information Act of 1974.)

User – The DoD organization with effective ownership or control of a hard drive, not an individual using a computer.

Disposition of DoD Computer Hard Drives

Sanitization/Destruction Verification Labels and Records

1. Figure A-3.1. provides a suggested label format to be attached to a hard drive or computer housing, as appropriate. At a minimum the label should include the following information:

Certification of Hard Drive Disposition

This certifies this hard drive,

Serial Number _____,

Make and Model_____

Was Overwritten/Degaussed/Destroyed in accordance with DOD Memorandum XXX on ___(date)_____

(Manufacturer, Product Version, Date Used)_____

Software or Degausser Used

- or -

(e.g., Approved Metal Destruction Facility)_____

Method of Destruction

_____

Printed Name and Rank/Grade

_____ _____

Signature Date

Figure A-3.1. Format for Sanitization/Destruction Validation Label

Attachment 4

2. Below is an example format letter for verifying that a hard drive was overwritten, degaussed, and/or destroyed.

(Date)

1. The following listed hard drives were overwritten in accordance with Attachment 2, DoD Memorandum "Disposition of Unclassified DoD Hard Drives," dated April 2001, using the following software: (Manufacturer, Product Version).

- or-

The following listed hard drives were degaussed in accordance with Attachment 2, DoD Memorandum "Disposition of Unclassified DoD Hard Drives," dated April 2001, using the following degausser: (Manufacturer, Product Version).

- or -

The following listed hard drives were destroyed in accordance with Attachment 2, DoD Memorandum "Disposition of Unclassified DoD Hard Drives," dated April 2001, using the following method: (Smelting, Disintegration, Pulverization, Abrasion, or Acid Application, etc.).

2. (Hard Drive Make, Model, and Serial Number).

   (Hard Drive Make, Model, and Serial Number).

   (Hard Drive Make, Model, and Serial Number).

   (Hard Drive Make, Model, and Serial Number).

3. The sanitization/destruction process was performed by (Name and Rank/Grade).

Verifying Official
(Name, Rank/Grade, and Organization)

Figure A-3.2.1. DoD Verification of Sanitization/Destruction of DoD Hard Drives