DEPARTMENT OF THE NAVY
NAVAL INFORMATION SYSTEMS
MANAGEMENT CENTER

NAVSO P-5239-26
SEPTEMBER 1993

REMANENCE SECURITY

GUIDEBOOK

MODULE 26

INFORMATION SYSTEMS SECURITY
(INFOSEC)
PROGRAM GUIDELINES

0515-LP-208-8345

Distribution: Submit requests for placement on distribution (including supporting justification), or amendment to the existing distribution, to:

Commanding Officer
Naval Electronic Systems Security Engineering Center
Code 011C
3801 Nebraska Avenue, N.W.
Washington, DC 20393-45454
Commercial (202) 282-0538
DSN 292-0538

Stocked: Additional copies of NAVSO P-5239-26 can be obtained from the Navy Aviation Supply Office (Code 03415), 5801 Tabor Avenue, Philadelphia PA 18120-5099, through normal supply channels in accordance with NPFC PUB 2002D, NAVSUP P-437 or NAVSUP P-485, using AUTODIN, DAMES, or MILSTRIP message format to DAAS, Dayton, OH.

Cite stock number 0515-LP-208-8345.

DEPARTMENT OF THE NAVY

NAVAL INFORMATION SYSTEMS MANAGEMENT CENTER
WASHINGTON, D.C. 20360-5000

NAVSO P-5239-26
SEPTEMBER 1993

FOREWORD

This publication, Navy Staff Office Publication (NAVSO Pub) 5239, "Information Systems Security (INFOSEC) Program Guidelines" is issued by the Naval Information Systems Management Center. This publication consists of a series of modules providing procedural, technical, administrative and/or supplemental guidance for all information systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data. Each module will focus on a distinct program element, and will establish a standard methodology for planning, implementing and executing the INFOSEC program within the Department of the Navy (DON).

This module, "Remanence Security Guidebook", provides the Information Systems Security Manager (ISSM)/Automated Data Processing Security Officer (ADPSO) with expanded guidance and procedures to supplement DoD 5200.28-M and OPNAVINST 5510.1. During the lifecycle of an Automated Information System (AIS), its data storage media are shared among a variety of users at many different clearance levels. At all times, the data must be protected against unauthorized disclosure. The recommendations contained in this guidebook allow the Designated Approving Authority to make intelligent decisions as to the risks involved in clearing, purging, and destroying AIS data storage media.

Instructions herein are issued for the information and compliance of all persons in the DON and are effective upon receipt.

/s/
J. G. HEKMAN
Rear Admiral, SC, USN

THIS PAGE INTENTIONALLY BLANK

TABLE OF CONTENTS

CHAPTER 1

GENERAL INFORMATION

1. **Introduction**. This guidebook addresses Department of the Navy (DON) Automated Information System (AIS) remanence security requirements. Remanence refers to traces of information remaining on data storage media after the use of insufficient purging procedures. In some cases, these remanent traces can be used to reconstruct the original information. Remanence security provides a set of procedures to prevent the unintentional disclosure of information from remanence.

2. **Applicability and Scope**.

a. The guidance and procedures in this document pertain to the handling and control of magnetic and non-magnetic data storage media containing General Service (GENSER) classified, and/or unclassified but sensitive information. The guidance does not apply to Special Compartmented Information (SCI), Cryptographic (CRYPTO), cryptologic, Special Access Program (SAP), Single Integrated Operation Plan - Extremely Sensitive Information (SIOP-ESI), or North Atlantic Treaty Organization (NATO) data.

b. These guidelines were developed from past research, policy, and accepted practices. Current research into remanence properties of new types of data storage media will add to the future development of guidelines. Specifically, this guidebook provides:

(1) Responsibilities of the Designated Approving Authority (DAA) and the Information Systems Security (INFOSEC) support personnel concerning remanence.

(2) Procedures for clear ing and purging data storage media for later reuse.

(3) Acceptable methods of destroying data storage media.

(4) Guidance for removal of external markings from data storage media.

3. **Objective**. Remanence security provides methods and procedures to prevent disclosure of classified, and/or unclassified but sensitive, information to persons who do not have the proper clearance and need-to-know for that information.

4. **Explanation of Terms**.

a. Caveats and handling restrictions. Controls on the dissemination of information (e.g., For Official Use Only (FOUO), Privacy Act of 1974, Contract Sensitive, Company Proprietary, NATO, and No Contractor).

b. Classification. The determination that official information requires, in the interest of national security, a specific degree of protection against unauthorized disclosure, coupled with a designation signifying that such a determination has been made. Executive Order 12356 defines the following levels: Top Secret, Secret, Confidential, and Unclassified.

c. Clearing. Rendering stored information unrecoverable by keyboard attack.

d. Coercivity. The strength of an applied magnetic field which will demagnetize a magnetic material. Demagnetizing the magnetic material of magnetic data storage media removes remanence.

e. Declassification. Declassification is the determination that classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification designation. Declassification does not constitute authority for public release. Declassification may be accomplished only under the rules contained in OPNAVINST 5510.1.

f. Erasing. Ambiguous term which can refer to purging, clearing, or removing file allocation.

g. Keyboard attack. Extracting information from data storage media by executing software utilities, keystrokes, or other system resources executed from a keyboard. For example, disk and file recovery utilities and memory scavenging procedures can be used to carry out keyboard attacks. A countermeasure to keyboard attack is: to overwrite or remove data storage media, thereby making information unavailable to users employing normal system capabilities.

h. Laboratory attack. Using sophisticated signal recovery equipment, in a laboratory environment, to recover stored information from data storage media. A countermeasure to laboratory attack is: to purge data storage media, rendering data unrecoverable by an effort commensurate with its sensitivity.

i. Memory Scavenging. Searching through data storage to collect residue thereby acquiring data. Data storage may be records, blocks, pages, segments, files,

directories, words, bytes, fields, or peripheral devices such as printers or video displays or others.

j. Operating Condition. Refers to whether equipment is in working order.

k. Overwriting. Writing data in the same storage location currently occupied by other data.

l. Purging. Rendering stored information unrecover able by laboratory attack.

m. Remanence. Residual information remaining on data storage media after use of insufficient purging procedures.

n. Removal of External Marking. The removal of external markings is a physical and administrative process applied to computer data storage media after classified, and/or sensitive but unclassified, information has been purged or declassified.

o. Sensitivity. Classification level plus caveats and handling restrictions.

p. Unclassified but Sensitive Information. FOUO, Privacy Act of 1974, or Contract Sensitive information.

5. **Responsibilities**. All INFOSEC personnel must be knowledgeable about the retention properties of data storage media under their control, the known risks of clearing, purging, and releasing data storage media, and the use of approved security procedures to help prevent accidental disclosure of classified, or unclassified but sensitive information. Implementation of approved security procedures is especially important during a lifecycle upgrade, and replacement of system memory and other storage components. The following paragraphs provide expanded guidance on the responsibilities established in SECNAVINST 5239.2.

a. The **Designated Approving Authority (DAA)** is responsible for the following: determining the acceptable level of data remanence risk for each system that will be accredited, approving software programs and equipment used for clearing and purging data storage media, and approving procedures for removal of external markings from data storage media. Only those persons having DAA cognizance over a particular system or medium have authority to approve purging or clearing procedures.

b. The **Information Systems Security Manager (ISSM)**:

(1) Develops and maintains plans for clearing, purging, destroying, removing external markings, and disposing of computer data storage media.

(2) Provides adequate information on data remanence for users, operations personnel, and other security personnel to make sound decisions concerning risks, requirements, and procedures.

(3) After ensuring that classified information has been properly purged, approves removal of external markings from computer data storage media where the DAA determined level of risk is acceptable and within guidelines.

(4) Coordinates with activity security manager on matters of common concern.

c. **Information Systems Security Officer (ISSO), Terminal Area Security Officer (TASO), or User**, as appropriate:

(1) Maintains proper control of equipment and information.

(2) Marks removable computer data storage media appropriately for sensitivity level and architecture (e.g., drive architecture or data storage media coercivity).

(3) Marks equipment such as computer terminals or stand alone personal computers, which contain non-removable computer data storage media (e.g., non-removable hard disk drives), appropriately for sensitivity level.

(4) Maintains awareness of the risks associated with storing and processing classified, and/or unclassified but sensitive, information on computers.

d. **Security Manager** serves as the Commanding Officer's advisor and direct representative in matters pertaining to the security of classified information and personnel security and coordinates with the command ISSM on matters of common concern. Performs duties specified by CNO (N09N) or CMC (ARAB).

(1) Develops and provides command personnel security procedures.

(2) Coordinates with the physical security officer on physical security measures for protection of classified information.

(3) Administers the command's cla ssification management program including: declassification, downgrading of classified information, and maintenance of records of removal of external markings from computer equipment and data storage media.

CHAPTER 2

DATA REMANENCE GUIDELINES

6. **Remanence Guidelines**. This document provides guidance on clearing, purging, and destruction of data storage media to an acceptable level of risk with regard to currently available technical information. Current Department of the Navy policy requires the DAA to accept the residual risk, provided that the user follows these procedures.

7. **Explanation of Purging and Clearing Computer Storage**. Purging removes classified, and/or unclassified but sensitive, information from data storage media to an extent that gives assurance, proportional to the sensitivity of the data, that the information is unrecoverable by laboratory attack. Clearing removes classified, and/or unclassified but sensitive, information from data storage media to an extent that renders the information unrecoverable by keyboard attack, but not to a degree sufficient to deny a laboratory attack. Routines such as file deletion and high level formatting, that only remove pointers and leave data intact, are not acceptable methods of clearing or purging data storage media.

8. **Guidance for Handling Data Storage Media**.

a. Clear operational data storage media that contained unclassified but sensitive information before reutilization or release from Government control. (Note: When required by licensing agreements, clear data storage media containing commercial off-the-shelf application software before release).

b. Clear data storage media which: is in operating condition, will be reused at a different sensitivity level, and where future physical protection will be at the same or higher sensitivity level.

c. Clear memory, disks, and other non-removable data storage media when changing AIS security modes of operation or reducing classification level during periods processing. This prevents unauthorized disclosure of residual information. Protection and labeling of removable data storage media and output during a dedicated or system high period processing session is at the level of the session rather than at the system's highest authorized level.

d. Purge data storage media that contained classified information before reutilization at a lower level of physical protection, or release from Government control.

e. Protect data storage media according to the highest classification of information ever processed or recorded until all the information ever stored thereon is declassified or the classified information is purged and the external markings removed.

f. Destroy unuseable or unpurgeable data storage media which contain classified information.

9. **Analysis Procedures**. Tables 1, 2, and 3 should be consulted to determine the proper actions to be taken for clearing, purging, and destruction of data storage media. Before using the tables, complete the following steps:

a. Determine the sensitivity of the data storage media. Note: this document does not apply to Special Compartmented Information (SCI), Cryptologic, North Atlantic Treaty Organization (NATO), or Single Integrated Operational Plan (SIOP) categories.

b. Determine what type of data storage media you have, for example magnetic tape, hard disk, floppy disk or other. If a question exists as to data storage media type, consult the equipment manual, manufacturer's documentation, or parts lists, etc.

c. Determine whether the data storage media are in operating condition (are they defective?). If a hard disk can not be reliably written or read, it is not in operating condition. Unreadable and unwriteable data storage media may contain remanent data. Unwriteable data storage media cannot be cleared or purged through overwriting.

d. Determine whether future users of the data storage media will have the clearance and need-to-know for the current data stored on the data storage media.

e. Determine whether future physical protection of the data storage media will be at the same, higher, or lower level of sensitivity of the information processed on the data storage media. For example, data storage media transferred from a Secret facility to an Unclassified facility will be physically protected at a lower level of sensitivity.

f. Consult Tables 1 and 2 for the following scenarios: data storage media are in operating condition and future physical protection will be at the same or higher sensitivity level; data storage media are in operating condition and future physical protection will be at a lower sensitivity level; or data storage media are not in

operating condition and therefore will be repaired or destroyed and future physical protection will be a lower sensitivity level.

10. **Procedures for Handling Data Storage Media**.

a. In order to inhibit signal analysis techniques used in laboratory attack, the following data storage media should be formatted or overwrittten with an unclassified data pattern prior to classified use: Electrically Erasable Programmable Read Only Memory (EEPROM), Electrically Alterable Read Only Memory (EAROM), and magnetic data storage media.

b. Protect data storage media as prescribed for the highest classification of information recorded on them until the data is purged or the data storage media are destroyed and the external marking removed. Evaluate all risk factors before removing classification labels from or releasing data storage media and do not remove external marking from data storage media if the remaining stored data has not been confirmed as unclassified. Do not remove the external marking or release from control, data storage media used for processing or storing classified information of any level without guidance from the ISSM or a declassification authority.

c. AIS data storage media are subject to the accountability, controls, safeguarding, and storage requirements established by CNO (i.e., OPNAVINST 5510.1). The granularity of the accountability may stop at the system level, for example, a personal computer with an integrated disk drive. Removal of a data storage device housing classified data storage media from an AIS for off-site maintenance or other release, however, requires that it be treated as a separate piece of equipment. For example, initiate a separate record for a disk drive containing non-removable sensitive data storage media, when the disk drive is taken out of a system and sent out for repair. The history record should include at minimum, positive identification of the component and any purging or destruction procedures employed before releasing the component.

d. Clearing and purging are especially important during AIS maintenance. For maintenance performed at the user's facility by uncleared personnel, clear data storage media or closely monitor the maintenance to preclude the disclosure of classified, and/or unclassified but sensitive information. Data storage media contained in AISs being serviced outside the user's facility, or data storage media that will be removed during service, should be purged before release. For example, when a classified, and/or unclassified but sensitive, AIS is serviced, the escort should not let the maintenance person walk off with a system board, disk, or other parts that may contain classified, or unclassified but sensitive data.

11. **Removal of External Marking from Data Storage Media**. The removal of an external marking is a physical and administrative procedure applied to computer data storage media after classified, and/or unclassified but sensitive, information has been purged. Some data storage media may contain information so sensitive that procedures within the scope of this guidebook may not meet the requirements of the cognizant security authority. In these cases, do not release the data storage media without approval from the applicable security authority.

Approval or disapproval of the procedures for removal of external marking should be based on established guidelines and procedures. If operational necessity or equipment costs warrant a decision that is outside the guidelines for acceptable risk, the ISSM will refer the information to the DAA for approval. Before considering removing the external marking from data storage media consider: the sensitivity of the data, the type of data storage media, its remanence potential, the purging procedures used, and any residual risks. Be certain that the information on the data storage media has been purged by an approved process, that the purging processes has been verified, and that the sensitivity of the purged information and the threats have been reviewed.

If required for record keeping purposes (see paragraph 2.5.c), a written statement should be submitted to the Security Manager, containing the following information:

a. The description of the data storage media (type, manufacturer, model, serial number, etc.).

b. The highest data classification ever processed or stored.

c. The purpose of the downgrade, declassification, or release.

d. An identification of the data owner.

e. A description of the purging procedures.

f. The individuals executing the purge, and verification of the results.

12. **Review of Purged Data Storage Media**. Review a statistical sample (nominal 90 percent confidence) of the overwritten data storage media for retention of data. A lower confidence value may be used for degaussers because of their inherently greater consistency and reliability. Accomplish this review by attempting to dump random short sectors, blocks, or memory contents to hard copy or a display for review. A person knowledgeable of the process should witness the data purge and certify in writing that the process was done properly and that review of the data storage media

revealed only the expected remanence. Someone in authority other than the person(s) purging the data storage media should maintain the record of the purging action. Data storage media that have features or malfunctions which might inhibit purging procedures should be dealt with on a case -by-case basis. Consult with the ISSM whenever there is any doubt about the success of the specific purging procedure.

13. **External Marking of Data Storage Media**.

a. Cleared data storage media retain their previous classification. They must retain external markings unless reused at a higher classification (in which case they should be marked at that higher classification level). Label them cleared and include the date and agency clearing the data storage media.

b. Purged data storage media retains their classification until they are administratively removed. Once the decision to remove the external marking is made and documented, remove all external markings and other labels which might identify the data storage media's previous sensitivity. Handle the data storage media as unclassified.

c. Data storage media leaving the Government inventory must not bear external markings showing previous classification and, if possible, ownership. Purge the information and remove the external markings.

THIS PAGE INTENTIONALLY BLANK

CHAPTER 3

CLEARING AND PURGING DATA STORAGE MEDIA

14. **Clearing and Purging Data Storage Media**. Clearing and purging data storage media are countermeasures to the threats of keyboard or laboratory attack, respectively. The difference in these threats and the sensitivity of the data, dictate that purging techniques be more rigorous than clearing techniques. Clearing and purging techniques also vary depending upon the data storage technology (e.g., magnetic, electrical, electrostatic, or thermal).

15. **Clearing Magnetic Data Storage Media by Overwriting**. The procedure for clearing magnetic data storage media by overwriting is to write a data pattern to all data storage locations on the media. The overwrite program should write to file allocation tables, directories, block maps, unassigned file space, active and inactive (unused) file space, and to the space between the end of a file and the end of the sector or block where it resides. NOTE: simply removing pointers to a file (as in the MS-DOS "delete" or "format" commands) does not prevent recovery of information. WARNING: MS-DOS, PC-DOS, and other similar operating systems have peculiarities which affect clearing and purging files by overwriting. Retrieving and editing a stored file, and then saving it may result in writing the file to a different location on the data storage media. Therefore, overwriting this file alone could leave older versions of it on the data storage media.

16. **Purging Magnetic Data Storage Media by Overwriting**. Some magnetic data storage media (See Tables 1-3 for applicability) may be purged by: overwriting all data storage locations first with a data pattern, then with the data pattern's compliment, then with a random pattern which will be subsequently verified (per DoD 5200.28-M). The procedure should force the magnetic fields at every addressable location on the data storage media to both polarities. The overwrite program should write to file allocation tables, directories, block maps, active and inactive (unused) file space, and to the space between the end of a file and the end of the sector or block where it resides. It should write to bad and spare sectors and tracks (including those removed from standard addressing). CAUTION: Ensure the read/write device hardware is functioning properly before beginning this procedure.

a. Where possible, use overwrite programs assessed by a recognized INFOSEC authority.

(1) When no evaluated or assessed program is available, the DAA may approve commercial programs designed to purge data storage media by overwriting, under the following guidelines.

(a) The performance of the program must be assessed. Systems programmers and analysts should carefully test and validate the performance of this software.

(b) The program documentation must fully explain all functions performed. The program should not perform any undocumented functions. Functions, outside overwriting must not create situations which either hinder overwriting or enable recovery of data.

(2) Where no commercial software is available or appropriate, systems programmers familiar with purging data storage media may develop computer programs or routines designed to overwrite computer memory or magnetic data storage media. The programs or routines must meet the requirements of this document and be tested as described.

(3) Only the DAA should approve the use of commercial or in -house programs or routines for purging computer storage. The ISSM should document the assessment of risk in using these programs to the appropriate DAA. It should be an attachment to the system's risk analysis or accreditation package.

b. Floppy disks and magnetic tapes. Because of the large variations in head to data storage media alignment and data formats, do not overwrite floppy disks to purge data; degauss them. Overwriting tapes is a far less efficient technique than using a degausser and should only be used if a degausser is unavailable. Magnetic tapes should be overwritten only if the overwriting software will provide a continuous stream of data that will overwrite existing inter-record gaps. The overwrite process should use the same bit density as in the original recording.

c. Hard Disks. Hard disks containing Confidential or Secret data may be overwritten to purge data. Disk controllers use a variety of encoding techniques to convert the computer data to a format suitable for the magnetic data storage media. Typically, ST506 style disk drives use Modified Frequency Modulation (MFM) encoding; Small Computer Systems Interface (SCSI) and AT Adapter (ATA)/Integrated Drive Electronics (IDE) drives use a Run Length Limited (RLL) encoding scheme (either 1,7 or 2,7). The patterns given below are designed to generate a specific bit sequence and its complement on the data storage media. Other patterns producing the same effect may also be used. If you are uncertain as to the drive encoding technique, use the RLL pattern. When doing verifications, read-

caching should be disabled. Note: The direction of head stepping motion (e.g., from inner to outer track) should alternate for each of the steps, (a) through (c), of the procedures listed below (3.3.c.(1) and 3.3.c.(2)).

(1) The preferred method for disk data storage media that may be purged by overwriting is to:

(a) Write all 1's to every block.

(b) MFM: Write a "1" in low order bit; a "0" in the next most significant bit; and "1"s in the remaining bits comprising the data block. RLL: Write "0010011111..1111" (least significant bit ... most significant bit) for 32 bits and repeat this pattern throughout the data block. Repeat the appropriate pattern for all addressable data blocks.

(c) Write a nonlinear pseudorandom bit sequence to all locations. This sequence is not predictable without knowledge of the generating algorithm. One such sequence is the output of an encrypting algorithm (e.g., Data Encryption Standard). In this application a biased algorithm (i.e., producing more zeros than ones (or vice versa)) is acceptable. The sequence should not repeat at the same offset on any two blocks on the disk drive. A different starting point for the pseudorandom bit sequence should be used for each disk drive.

(d) Verify the overwrite by reading the last data written to the data storage media. You should read nothing but the pseudorandom sequence.

(2) An alternate method when the required data patterns cannot be generated is to use the following simpler but less effective technique:

(a) Write a single character (e.g: hex EB) to all add ressable locations.

(b) Write the previous character's compliment (i.e., hex 14) to all addressable locations.

(c) Write a random character (e.g., hex 5C) to all addressable locations.

(d) Verify the overwrite by reading the last data written to the data storage media. You should read nothing but the random character.

d. SCSI and ATA/IDE drives. These disk drives are commonly used in personal computers, workstations, and file servers. They typically have a reserve spare capacity of one to two percent of their formatted volume. When areas (sectors or tracks) on the data storage media become defective, or difficult to access, the drive copies the data from the defective areas to spare areas and removes logical address pointers from the defective areas, rendering them subsequently inaccessible by logical addressing. As a result, the defective areas cannot later be overwritten during purging, or verified by reading after overwriting, by software that uses only logical addressing for overwriting. Subjecting the drive to laboratory examination can reveal the contents of defective areas and restore the deleted logical pointers. Sparing or grown defects (defects accruing after factory release of the media) should be considered when purging by overwriting. If the drive supports the function, the grown defect list should be retrieved and examined to determine its magnitude. If there is a large amount of sparing, the drive should not be purged by overwriting unless software utilities that overwrite the physical locations of defective areas is used.

17. **Purging Magnetic Data Storage Media by Degaussing**. Degaussing with approved degaussing equipment is a method for purging operational and non-operational magnetic data storage media, and is an alternative to physical destruction of magnetic data storage media. Refer to section 1.2.a of this document for applicability.

a. Magnetic Tape. Magnetic tapes are typed by coercivity, a measure of the strength of an external magnetic field needed for demagnetization sufficient to purge data. Type I magnetic tape coercivity is from 0 - 350 Oersteads (Oe), Type II magnetic tape coercivity is from 351 - 750 Oe, and Type III magnetic tape coercivity is above 750 Oe. Type I tape can be purged by Type I, II, or IIA degaussers. Type II tape can be purged by Type II or IIA degaussers. Currently, Type IIA degaussers are not approved for purging Type III magnetic tape above 900 Oe, but are approved for degaussing Type III tape that is below 900 Oe. Coercivity of magnetic tape cannot be determined by appearance, therefore mark or label the tape as to type upon receipt. Do not remove or cover markings until destruction or release of the tape. Before degaussing, determine the coercivity of the tape and ensure that it does not exceed the rating (Type I, II, or IIA) of the degausser. Table 3 lists the nominal coercivity of various data storage media.

b. Magnetic Disk. Type I degaussers are sufficient for purging all curren t magnetic floppy and hard disks including those with a coercivity over 350 Oe.

NOTE: Degaussing hard disks destroys timing information and often demagnetizes the permanent magnets of the spindle motor on sealed (Winchester) drives. Therefore, you should not degauss functioning sealed disk drives which you expect to reuse.

c. Approved permanent magnets may be used to degauss only Type I tapes and any magnetic computer floppy or hard disks. For fixed magnets, follow manufacturer's procedures. For hand-held magnets use a lint -free wiping cloth or a lintless tissue between the magnet and the recording surfaces to prevent damage to the data storage media. Wipe the entire surface at least three times, while slowly rotating it. Take care to expose all areas (tracks) to the hand -held magnet assembly.

e. Follow manufacturer's procedures for the proper use of electromagnetic degaussers. Adapters for degaussing different kinds of data storage media are available for most approved electromagnetic degaussers. Make sure data storage media are not encased in metal covers which will interfere with the degaussing magnetic field. Make certain the degaussing equipment is functioning properly. Someone in authority knowledgeable about the degaussing procedures, other than the person(s) executing the degaussing, should audit the entire procedure, verify in writing that the process was done properly, and verify that review of the data storage media revealed only the expected remanence. Review of the data storage media is achieved by examining a statistical sample of the degaussed data storage media for retention of data. Accomplish this by dumping short sectors, blocks, or memory contents to hard copy or a display for review.

f. Evaluated Degaussers: National Security Agency (NSA) evaluated degaussers may be used to purge magnetic data storage media containing classified information. Place special emphasis on degaussers used for data storage media containing Top Secret information. Type I degaussers cannot degauss Type II or above data storage media. NSA publishes the "Information Systems Security Products and Services Catalog", which contains a listing of evaluated degaussers called the Degausser Products List (DPL). The DPL lists degaussers evaluated against either the National Security Agency Specification L14 -4-75, or the later version, L14 -4-A. The Magnetic Tape Degausser Specifications include the applicable Federal Specifications and Military Standards. The Information Systems Security Products and Services Catalog is available from the Government Printing Office.

g. Non-evaluated Degaussers: Non-evaluated degaussers can be used for clearing Type I media, however purging Type I media with non-evaluated degaussers requires written approval from the cognizant DAA. The DAA should not approve non-evaluated degaussers for use on Type II or above data storage media. NOTE: Non-evaluated degaussers may not completely purge data storage media, therefore the

DAA must exercise caution when approving non-evaluated degaussers, especially for media containing Top Secret information. Users should initiate action to replace or augment non-evaluated degaussers with those listed on the DPL. Advise the DAA of the kind of degausser (for example, fixed, paddle, bar permanent magnet, electromagnet, etc.), brand, model, serial number, field strength (include the method used to determine the field strength), and the highest classification being degaussed. For approval of Type I data storage media and magnetic computer disks the following minimum criteria must be met:

(1) The degausser must have a minimum field strength of 1500 Gauss at the degaussing platform. Measure the field strength with a gauss meter.

(2) If measurement of field strength is not possible, manufacturer's specifications must state that the minimum field strength is at least 1500 Gauss.

h. Procure only degaussers listed on the DPL, or which are evaluated. If you cannot obtain an evaluated degausser and must buy a non-evaluated degausser, your DAA must approve it. Test the proposed degausser under NSA/CSS Specification L14-4-A, Magnetic Tape Degausser, dated 31 Oct 85 (or superseding specifications). Data supporting the request must include all of the information required under this specification, testing agency, test results, and a statement telling why an evaluated degausser is not adequate or available. Degaussers not listed on the DPL, or which have not been formally evaluated under NSA/CSS Specification L14-4-A will not be approved for use with Type II magnetic computer or video tape.

i. Contact the degausser vendor or a degausser repair service any time the degausser is suspected of not performing properly. After repair, certify that the degausser operates within the limits established by NSA/CSS Specification L14-4-A before using it to degauss classified data storage media.

18. **Purging EEPROM and EAROM**. Purge EEPROMs and EAROMs using the procedures given in Tables 1 and 2. If practical, retain data storage media under Government control for four hours after purging. Government control may be cleared or uncleared personnel.

19. **Purging Random Access Memory (RAM)/Battery Backed RAM/Static RAM (SRAM)**. RAM, battery backed RAM and static RAM are volatile semiconductor memory. Purge them by removing power for at least 30 seconds. CAUTION: Static RAM (SRAM) chips may retain power after the system is powered down through either filter capacitors or batteries. SRAM is volatile, but the user must remove all power to purge it.

20. **Clearing Optical Disks**. There are three types of optical data storage media. These are Read Only Optical Disks (commonly called CD -ROM), Write Once Read Many Optical Disks (WORM), and Erasable magnetic or non-magnetic Optical Disks. Only the Erasable Optical Disks, which can be repeatedly read from and written to, can be cleared. (No optical disks can be purged.) Clear Erasable Optical Disks by writing a pattern to all locations. NOTE: The disk must remain classified at the same level as the highest level of classified data which was recorded. Protect it appropriately. Label it to indicate that it was cleared. Retain external markings for the highest classification level on the storage medium.

CHAPTER 4

DATA STORAGE MEDIA DESTRUCTION TECHNIQUES

21. **Data Storage Media Destruction**. Destroy data storage media that stored classified, and/or unclassified but sensitive, information when the data storage media is no longer usable and **cannot** be purged. Remove all external markings indicating previous use or classification from the data storage media.

22. **Magnetic Data Storage Media Destruction**. Destroy magnetic data storage media when it is defective or cannot be economically purged for reuse. Use one of the following destruction methods:

a. Incinerate or disintegrate tapes, magnetic cards and floppy disks. WARNING: Do not destroy magnetic tapes on aluminum reels or disks in a sodium nitrate incendiary device such as M3 or M4 destructor drum or the M4 file destroyer. The combination of iron and aluminum in a sodium nitrate fire creates a danger of explosion.

b. Degauss magnetic media by the degaussing methods in Chapter 3 of this document.

c. Destroy hard disks and drums at an approved metal destruction facility.

d. Completely remove the entire recordin g surface of disks or drums using an emery wheel, disk sander, belt sander, or sand blaster.

e. Trained personnel can remove (that is, chemically destroy) gamma ferric oxide disk surfaces by the application of concentrated hydriodic acid (55 to 58 percent solution).

f. Remove the drum or disk recording surface by applying acid activator Dubais Race A (NSN 8010-00-181-7171) with stripper Dubais Race B (NSN 8010-00-181-7170). After removing the recording surface apply technical acetone (NSN 6810-00-184-4796) to remove any residue from the drum surface.

23. **Semiconductor Memory Destruction**. Destroy unusable or unpurgeable semiconductor memory which contained classified information. Destroy semiconductor memory by pulverizing, incinerating or disintegration. The following are some authorized ways to destroy semiconductors.

a. Wafers/Chips (unmounted).

(1) Brinkman Instruments Model ZM -1 Centrifugal Grinding Mill equipped with 0.12 mm pore -size sieve (75 microns o r less), or

(2) Molten Sodium Hydroxide (600 degrees Centigrade), or

(3) Hydrofluoric and Nitric acid (HF and HNO3) in 1:1 ratio. CAUTION: This procedure must be done in a well ventilated area and personnel must wear eye protection and protective clothing.

b. Packaged Circuits.

(1) Molten Sodium Hydroxide (600 degrees Centigrade), or

(2) Hydrochloric and Nitric acid (HCL and HNO3) in 1.5:1 ratio, then HF and HNO3 in 1:1 ratio. CAUTION: This procedure must be done in a well ventilated space and personnel must wear eye protection and protective clothing.

24. **Optical Disk Destruction**. The methods of destruction of optical disk, in order of preference are: smelting, incinerating in an approved facility, or by pulverizing into chip sizes smaller than 0.5 mm. Early model CD-ROMs containing elements such as selenium and tellurium generate hazardous gas or dust when heated or pulverized. Before destroying a disk obtain evidence from the disk manufacturer that the disk does not contain these elements. If this evidence is unavailable, or if these elements are present, retain the disk in secure storage until an environmentally approved destruction facility is available.

25. **Other Media Destruction**.

a. Paper Materials. Destroy by burning, pulverizing, or crosscut shredding. Residue of pulverized products must not exceed pieces 5 mm in size. Residue of shredded products must not exceed pieces 3/64 inches wide by 1/2 inches long in size. Reduce residue of burned products to white ash.

b. Platens, Ribbons. Remove printer platens and ribbons from all printers before releasing them to a vendor or DoD property disposal channels. Destroy platens

(remove only the rubber surface for destruction) and ribbons by burning, pulverizing, or chemical means.

c. Glass Masks (Emulsion). Destroy in 5% Sodium Hypochlorite (common household bleach) by total immersion.

d. Glass Masks (Chrome). Smelt at 1040 degrees Centigrade.

e. Cathode Ray Tube (CRT) . Consider a CRT unclassified if visual inspection reveals no classified information etched into the CRT phosphor. If there is any doubt after inspection of the screen, highlight the CRT surface by filling the screen with vectors. This creates a raster effect and lights up the entire screen. Vary the brightness of the raster with the intensity control. You can then easily detect any burns or uneven illumination of the phosphor coating that could be compromising. Random burns on the CRT do not require automatic classification. Should any area of the CRT contain classified information, the CRT becomes classified at the highest level of residual information. Destroy the CRT if it becomes defective and contains classified data. See Table 1 for destruction procedures.

26. **Equipment**. Physically examine card punches, card readers, printers, optical character readers, FAX transceivers, etc., during clearing. Include visual examination of the normal card/paper path through the equipment. To detect the possible presence of unprocessed punched cards, operate the card punch/reader for three or more cycles with the hopper empty. If the equipment malfunctions, search the locations where a card or page of paper could become lodged. Remove or open equipment access panels and other removable components to perform the visual inspection. If the equipment contains buffer memory, registers, or other data storage media, clear them according to the appropriate procedures.

THIS PAGE INTENTIONALLY BLANK

TABLE 1. MANAGEMENT OF DATA STORAGE MEDIA CONTAINING CLASSIFIED DATA.

DATA STORAGE MEDIA TYPE	Data Storage Media are in operating condition and future physical protection will be at the same or higher sensitivity level (clear).	Data Storage Media are in operating condition and future physical protection will be at a lower sensitivity level (purge).	Data Storage Media are not in operating condition, and will be repaired or destroyed. Future physical protection will be at a lower sensitivity level (purge or destroy).
Magnetic Bubble Memory, Magnetic Core Memory, or Magnetic Plated Wire Memory	**Overwrite all locations with any pattern.**	**Degauss with Type I, II, or IIA degausser.**	**Degauss with Type I, II, or IIA degausser; or smelt, incinerate, disintegrate, or pulverize.**
Magnetic Resistive Memory	**Overwrite all locations with any pattern.**	**Smelt, incinerate, disintegrate, or pulverize.**	**Smelt, incinerate, disintegrate, or pulverize.**
Magnetic Tape (Type I)	**Degauss with Type I, II, or IIA degausser or use manufacturers erase.**	**Degauss with Type I, II, or IIA degausser.**	**Degauss with Type I, II, or IIA degausser or smelt, incinerate, disintegrate, or pulverize.**
Magnetic Tape (Type II)	**Degauss with Type I, II, or IIA degausser or use manufacturers erase.**	**Degauss with Type II or IIA degausser.**	**Degauss with Type II or IIA degausser; or smelt, incinerate, disintegrate, or pulverize.**
Magnetic tape (Type III)	**Degauss with Type I, II, or IIA degausser or use manufacturers erase.**	**See 3.4.A or Smelt, incinerate, disintegrate, or pulverize.**	**See 3.4.a or Smelt, incinerate, disintegrate, or pulverize.**
Magnetic Floppy Disk or Magnetic Bernoulli Disk	**Overwrite all locations with any pattern or degauss with Type I,II, or IIA degausser.**	**Degauss with Type I, II, or IIA degausser.**	**Degauss with Type I, II, or IIA degausser or smelt, incinerate, disintegrate, or pulverize.**

Magnetic removable or non-removable Hard Disk	**Overwrite all locations with any pattern or degauss with Type I,II, or IIA degausser.**	**TOP SECRET: Degauss with Type I, II, or IIA degausser. (This may damage the disk drive).**	**Degauss with Type I, II, or IIA degausser; or smelt, incinerate, disintegrate, or pulverize.**
		SECRET/CONFIDENTIAL: degauss with Type I, II, or IIA degausser (may damage disk) or overwrite as per paragraph 3.3.c	
Magneto-Optical Read Many, Write Many Disk	**Overwrite all locations with any pattern.**	**Smelt, incinerate, disintegrate, pulverize.(see 4.4)**	**Smelt, incinerate, disintegrate, or pulverize.(see 4.4)**
Magneto-Optical Read Only (ROM) Disk, Write Once Read Many (WORM) Disk, Non-Magnetic Read Only (ROM), or Programmable (PROM) Memory.	**Smelt, incinerate, disintegrate, pulverize. (see 4.4)**	**Smelt, incinerate, disintegrate, pulverize. (see 4.4)**	**Smelt, incinerate, disintegrate, or pulverize. (see 4.4)**
Non-Magnetic Random Access Memory (RAM)	**Overwrite all locations with any pattern or power off for at least 30 seconds.**	**Power off for at least 30 seconds.**	**Power off for at least 30 seconds or smelt, incinerate, disintegrate, or pulverize.**
Non-Magnetic Erasable PROM (UV PROM/ EPROM)	**Perform an ultraviolet erase according to manufacturer's recommendations.**	**Perform an ultraviolet erase three times according to manufacturer's recommendations and overwrite all locations with a random pattern and verify that pattern.**	**Perform ultraviolet erase three times according to manufacturer's recommendations and overwrite all locations with a random pattern and verify that pattern. Or, smelt, incinerate, disintegrate, pulverize.**
Non-Magnetic Electrically Alterable PROM (EAROM), Non-Magnetic Electrically Erasable PROM (EEPROM)	**See manufacturer's specification.**	**TOP SECRET: Preferred method: Erase, program all locations with a random pattern, wait 2 minutes, erase, program all locations with another random pattern, verify the random pattern.**	**Smelt, incinerate, disintegrate, pulverize.**

		SECRET or CONFIDENTIAL: Preferred method: Erase, program all locations with a random pattern, verify the random pattern.	
		Alternate method: perform above steps, but substitute the compliment of the erase pattern for the random pattern.	
Cathode Ray Tube (CRT) Note: Test CRT as per paragraph 4.5.e.	**No action required**	**Not possible.**	**WARNING: The coating inside of the CRT may be extremely toxic. CAUTION: A trained technician should wear a full face shield or equivalent protection while performing the following destruction procedure: remove the CRT tube and place it face down in an empty CRT carton; with a screwdriver or probe, carefully break off the location pin from the tube base and break off the tip of the glass vacuum seal.**
Laser or LED Printer Drum	**No action required.**	**TOP SECRET: Print 9 pages of unclassified data with few blank or solid black areas.**	**Expose drum surface to strong infrared source or sunlight for 20 seconds or crush drum. See 4.2.f.**
		SECRET: Print 3 pages of unclassified data with few blank or solid black areas.	
		CONFIDENTIAL: Print 1 page of unclassified data with few blank or solid black areas.	

Printer or FAX with Hard Disk, Floppy Disk, EEPROM, or other data storage media.	**Treat components per table.**	**Treat components per table.**	**Treat components per table.**
Printer Ribbons	**No action required.**	**Overwrite 5 times with unclassified data.**	**Incinerate, disintegrate, pulverize**

TABLE 2. MANAGEMENT OF DATA STORAGE MEDIA CONTAINING UNCLASSIFIED BUT SENSITIVE DATA.

DATA STORAGE MEDIA TYPE	Data Storage Media are in operating condition and future physical protection will be at the same or higher sensitivity level (clear).	Data Storage Media are not in operating condition, and will be repaired or destroyed. Future physical protection will be at a lower sensitivity level (purge or destroy).
Magnetic Bubble Memory, Magnetic Core Memory, Magnetic Plated wire Memory, or Magnetic Resistive Memory	**Overwrite all locations with any pattern.**	**No action required.**
Magnetic Tape Type I, Magnetic Tape Type II, or Magnetic Tape Type III	**Degauss with Type I, II, or other degausser (see 3.4)**	**If unreadable, no action required. Otherwise:degauss with Type I, II or other degausser (see 3.4); or cut or crush media surface or otherwise render unreadable.**
Magnetic Floppy Disk, Magnetic Bernoulli Disk, Magnetic removable Hard Disk, or Magnetic non-removable Hard Disk	**Overwrite all locations with any pattern or degauss with Type I, II, or other degausser (see 3.4).**	**If unreadable, no action required. Otherwise:degauss with Type I, II or other degausser (see 3.4); or cut or crush media surface or otherwise render unreadable.**
Magneto-Optical Read Many, Write Many Disk	**Overwrite all locations with any pattern.**	**If unreadable, no action required; otherwise, break into several pieces of various sizes.**
Magneto-Optical Read Only (ROM) Disk, Magneto-Optical Write Once Read Many (WORM) Disk, Non-Magnetic Programmable ROM (PROM), or Non-Magnetic Read Only Memory (ROM)	**Break into several pieces of various sizes.**	**No action required.**

Non-Magnetic Random Access Memory (RAM)	**Overwrite all locations with any pattern or power off for at least 30 seconds.**	**Power off for at least 30 seconds.**
Non-Magnetic Erasable PROM (UV PROM/ EPROM)	**Perform an ultraviolet erase according to manufacturer's recommendations.**	**Perform an ultraviolet erase according to manufacturer's recommendations or break or cut leads.**
Non-Magnetic Electrically Alterable PROM (EAROM) or Non-Magnetic Electrically Erasable PROM (EEPROM)	**See manufacturer's specifications.**	**No action required.**
Cathode Ray Tube (CRT)	**No action required.**	**No action required.**
Laser or LED Printer Drum	**No action required.**	**No action required.**
Printer or FAX with Hard Disk, Floppy Disk, EEPROM, or other data storage media.	**Treat components per table.**	**No action required.**
Printer Ribbons	**No action required.**	**No action required.**

TABLE 3. NOMINAL COERCIVITY OF VARIOUS DATA STORAGE MEDIA

This table contains the nominal coercivity for the kinds and brands of magnetic data storage media listed. It is a compilation of the information available at the time of publication and is not all inclusive. It is intended to aid in determining degaussing requirements. The guidance given in the notes column is valid for that storage medium.

Model/Brand	Medium	Kind	Coercivity (Oe)	Notes
3-1/2 Inch Rigid Disk	Disk	Computer	630	4
5-1/4 Inch Floppy Disk (360 K)	Disk	Computer	320	4
5-1/4 Inch Floppy Disk (High Density)	Disk	Computer	640	4
8 Inch Floppy Disk (High Density)	Disk	Computer	640	4
4 mm	Tape	Computer	1450	3
8 mm	Tape	Computer	1450	3
8 mm	Tape	Video	1450	3
196, Ampex	Tape	Video	650	2
721, Ampex	Tape	Instrument	700	2
777, 3M	Tape	Computer	295	1
795, Ampex	Tape	Instrument	310	1
797, Ampex	Tape	Instrument	310	1
799, Ampex	Tape	Instrument	310	1
895, Memorex	Tape	Instrument	310	1
897, Memorex	Tape	Instrument	310	1
5198, 3M	Tape	Instrument	700	2
6250 CPI (7,8,9 Track)	Tape	Computer	295	1
A-10 Cartridge, Bernoulli	Disk	Computer	600	4
A-20 Cartridge, Bernoulli	Disk	Computer	600	4
Analog Video Adaptations	Tape	Instrument	650	2
B-5 Cartridge, Bernoulli	Disk	Computer	600	4
B-20 Cartridge, Bernoulli	Disk	Computer	600	4
B-44 Cartridge, Bernoulli	Disk	Computer	750	4
Beta, Sony	Tape	Video	700	2
Betacam, Sony	Tape	Video	680	2
Betacam SP, Sony	Tape	Video	1500	3
Blackwatch 1/2 In Cartridge, 3M	Tape	Computer	520	2
C-Format	Tape	Video	650	2

Model/Brand	Medium	Kind	Coercivity (Oe)	Notes
3-1/2 Inch Rigid Disk	Disk	Computer	630	4
D1	Tape	Video	900	3
D2	Tape	Video	1500	3
DC 100, 3M	Tape	Computer	310	1
DC 300, 3M	Tape	Computer	310	1
DC 600, 3M	Tape	Computer	550	2
DC 615, 3M	Tape	Computer	550	2
DC 1000, 3M	Tape	Computer	550	2
DC 2000, 3M	Tape	Computer	550	2
ED-Beta	Tape	Video	900	3
IBM 3480	Tape	Computer	520	2
ID1	Tape	Instrument	900	3
ID2	Tape	Instrument	1500	3
M II (Metal Particle), Panasonic	Tape	Video	1500	3
MDC 750 Megatape	Tape	Computer	650	2
Phillips-type (High Bias)	Tape	Computer	600	2
Phillips-type (Standard)	Tape	Computer	300	1
Quadraplex	Tape	Video	295	1
SVHS	Tape	Video	900	3
SQ 100 Cartridge, Syquest	Disk	Computer	800	3
SQ 200 Cartridge, Syquest	Disk	Computer	800	3
SQ-400 Cartridge, Syquest	Disk	Computer	950	3
TK 50	Tape	Computer	520	2
TK 70	Tape	Computer	520	2
U Matic	Tape	Video	650	2
U Matic SP 3/4 Inch	Tape	Video	720	2
VHS	Tape	Video	700	2

Notes:
1. Type I Media.
2. Type II Media.
3. Above Type II Media.
4. See 3.4.b.