A Guide to Understanding Data Remanence in Automated Information Systems

Table of Contents

FOREWORD

The National Computer Security Center is issuing A Guide to Understanding Data Remanence in Automated Information Systems as part of the "Rainbow Series" of documents our Technical Guidelines Program produces. In the Rainbow Series, we discuss in detail the features of the Department of Defense Trusted Computer System Evaluation Criteria (DoD 5200.28-STD) and provide guidance for meeting each requirement. The National Computer Security Center, through its Trusted Product Evaluation Program, evaluates the security features of commercially-produced computer systems. Together, these programs ensure that organizations are capable of protecting their important data with trusted computer systems. While data remanence is not a directly evaluated criterion of trusted computing systems, it is an issue critical to the safeguarding of information used by trusted computing systems.

A Guide to Understanding Data Remanence in Automated Information Systems is intended for use by personnel responsible for the secure handling of sensitive or classified automated information system memory and secondary storage media. It is important that they be aware of the retentive properties of such media, the known risks in attempting to erase and release it, and the approved security procedures that will help prevent disclosure of sensitive or classified information. This version supersedes CSC-STD-005-85, Department of Defense Magnetic Remanence Security Guideline, dated 15 November 1985.

As the Director, National Computer Security Center, I invite your suggestions for revising this document. We plan to review this document as the need arises.

Patrick R. Gallagher, JR — September 1991
Director
National Computer Security Center

ACKNOWLEDGMENTS

The National Computer Security Center extends recognition to Captain James K. Goldston, United States Air Force, for providing engineering support and as primary author and preparer of this guideline. We thank the many people involved in preparing this document. Their careful review and input were invaluable. The National Computer Security Center extends recognition to Dr. Bane W. Burnham and David N. Kreft, without whom this revision could not have taken place. Other reviewers that provided much needed input are Carole S. Jordan, Lawrence M. Sudduth, and Kim Johnson-Braun and George L. Cipra.

1 INTRODUCTION

Data remanence is the residual physical representation of data that has been in some way erased. After storage media is erased there may be some physical characteristics that allow data to be reconstructed. This document discusses the role data remanence plays when storage media is erased for the purposes of reuse or release.

Various documents have been published that detail procedures for clearing, purging, declassifying, or destroying automated information system (AIS) storage media. [1,2,4, 5, 6, 8,9,13 and 16] The Department of Defense (DoD) published DoD Directive 5200.28, Security Requirements for Automated Information Systems, [17] and its corresponding security manual DoD 5200.28-M, Automated Data Processing Security Manual, [1] in 1972 and 1973, respectively. These two documents were amended in 1979, in response to the Defense Science Board Task Force recommendation to establish uniform DoD policy for computer security requirements, controls, and measures. The directive was again revised in March 1988, and efforts are underway to revise the manual.

DoD 5200.28-M addresses DoD requirements for the secure handling and disposal of memory and secondary storage media. While the Department of Defense requires the use of DoD Directive 5200.28 and DoD 5200.28-M by DoD components, the heads of DoD components may augment these requirements to meet their needs by prescribing more detailed guidelines and instructions provided they are consistent with these policies. DoD contractors and subcontractors who participate in the Defense Industrial Security Program (DISP) are required to comply with DoD 5220.22-M, Industrial Security Manual for Safeguarding Classified Information. [8] The Defense Investigative Service is responsible for the promulgation of the policy reflected in DoD 5220.22-M. Unlike these policy documents, A Guide To Understanding Data Remanence In Automated Information Systems does not provide requirements.

Sometime during the life cycle of an AIS, its primary and secondary storage may need to be reused, declassified, destroyed, or released. It is important that security officers, computer operators, and other users or guardians of AS resources be informed of the risks involving the reuse, declassification, destruction, and release of AIS storage media. They also should be knowledgeable of the risks inherent in changing the sensitivity level of AS storage media or of moving media from an installation with a specific security posture tone that is less secure. They should use proper procedures to prevent a possible disclosure of sensitive information contained on such media. ("Sensitive" in this document refers to classified and sensitive but unclassified information.) The procedures and guidelines in this document are based on research, investigation, current policy, and standard practice.

This guideline is divided as follows: Section 2 provides information on using this guideline and introduces DoD terminology. Section 3 discusses the use of degaussers and references the Degausser Products List (DPL), a listing of DoD evaluated degaussers. Section 4, "Risk Considerations," has information similar to that found in version 1 of this document, except for the modification of Section 4.2, "Effects of Heat and Age," and the addition of information on overwriting and degaussing. Section 5 addresses DoD endorsed erasure standards. Recently developed storage technologies and disk exercisers

are discussed in Section 6. Section 7 addresses areas needing further investigation and provides references to additional information on the science of magnetics, as it pertains to magnetic remanence.

1.1 PURPOSE

The purpose of this publication is to provide information to personnel responsible for the secure handling of sensitive AIS memory and secondary storage media. (However, this guidance applies to any electronic or magnetic storage media, e.g., instrumentation tape.) This guideline provides information relating to the clearing, purging, declassification, destruction, and release of most AIS storage media. While data remanence is not a directly evaluated criterion of trusted computing systems, it is an issue critical to the safeguarding of information used by trusted computing systems and, as such, is addressed in thA5 National Computer Security Center (NCSC) guideline. The NCSC publishes this document because the community using trusted computing systems has expressed the desire for this information. Additionally, readers should note that this is a guideline only and they should not use it in lieu of policy.

1.2 HISTORY

As early as 1960 the problem caused by the retentive properties of AIS storage media (i.e., data remanence) was recognized. It was known that without the application of data removal procedures, inadvertent disclosure of sensitive information was possible should the storage media be released into an uncontrolled environment. Degaussing, overwriting, data encryption, and media destruction are some of the methods that have been employed to safeguard against disclosure of sensitive information. Over a period of time, certain practices have been accepted for the clearing and purging of AIS storage media.

A series of research studies were contracted by the DoD to the Illinois Institute of Technology, Research Institute and completed in 1981 and 1982. They have confirmed the validity of the degaussing practices as applied to magnetic tape media. [19] Additional research conducted at the Carnegie-Mellon University using communication theory and magnetic modeling experiments designed to detect digital information from erased disks has provided test data on the erasability of magnetic disks. [11, 21, and 22] This work, along with DoD research that has not yet been released, provides the basis for the disk degaussing standard. More studies are planned or underway to ensure the adequacy of DoD degaussing standards.

On 2 January 1981, the Director of the National Security Agency assumed responsibility for computer security within the Department of Defense. As a result, the Department of Defense Computer Security Center (DoDCSC), officially chartered by DoD Directive 5215.1, was established at the National Security Agency. (3] The DoDCSC Division of Standards (now Division of Standards, Criteria, and Guidelines) was subsequently formed and tasked to support a broad range of computer security related subjects. The DoDCSC became the NCSC in 1985, as amended in National Security Decision Directive 145. [15] As part of its mission to provide information useful for the secure operation of AISs, the NCSC published the Department of Defense Magnetic Remanence Security Guideline, which is version 1 of this guideline.

2 GENERAL INFORMATION

An AIS and its storage media should be safeguarded in the manner prescribed for the highest classification of information ever processed by the AIS. That is, until the AIS and its associated storage media are subjected to an approved purging procedure and administratively declassified. There should be continuous assurance that sensitive information is protected and not allowed to be placed in a circumstance wherein a possible compromise can occur. There are two primary levels of threat that the protector of information must guard against: keyboard attack (information scavenging through system software capabilities) and laboratory attack (information scavenging through laboratory means). Procedures should be implemented to address these threats before the AIS is procured, and the procedures should be continued throughout the life cycle of the AIS.

2.1 USE OF THIS GUIDELINE

Designated Approving Authorities and Information System Security Officers (ISSOs) may refer to this guideline when selecting or evaluating specific methods to clear, purge, declassify, or destroy AIS storage media. DoD components may include the information provided in this guideline in their security training and awareness program; however, they should not use this guideline in lieu of existing policies.

Guidelines in this document have two degrees of emphasis. Those that are most important to the secure handling of AIS storage media have such wording as "the ISSO should . . . ." Guidance of lesser criticality has such wording as "it is good practice" or "it may be." Thus, the word "may" denotes less emphasis or concern than the word "should."

2.2 IMPORTANT DEFINITIONS

This section provides definitions and their amplification critical to understanding the issues in remanence. A comprehensive glossary follows Section 7.

Clearing: The removal of sensitive data from an AIS at the end of a period of processing, including from AIS storage devices and other peripheral devices with storage capacity, in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed using normal system capabilities, i.e., through the keyboard. (This may include use of advanced diagnostic utilities.) An AS need not be disconnected from any external network before a clear. [1, draft version]

Clearing can be used when the secured physical environment (where the media was used) is maintained. In other words, the media is reused within the same AIS and environment previously used.

In an operational computer, clearing can usually be accomplished by an overwrite of unassigned system storage space, provided the system can be trusted to provide separation of the storage space and unauthorized users. For example, a single overwrite of a file or all system storage, if the circumstance warrants such an action, is adequate to ensure that previous

information cannot be reconstructed through a keyboard attack. Note: Simply removing pointers to a file, which can occur when a file is simply deleted in some systems, will not generally render the previous information unrecoverable through normal system capabilities (i.e., diagnostic routines).

Purging: The removal of sensitive data from an AIS at the end of a period of processing, including from AIS storage devices and other peripheral devices with storage capacity, in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed through open-ended laboratory techniques. An AIS must be disconnected from any external network before a purge. [17]

Purging must be used when the secured physical environment (where the media was used) will not be maintained. In other words, media scheduled to be released from a secure facility to a non-cleared maintenance facility or similar non-secure environment must be purged.

Note: The purging definition allows a hierarchy of data eradication procedures, although current standards do not take advantage of this. That is, removing data with "assurance, proportional to the sensitivity of the data, that the data may not be reconstructed" implies that standards can be developed to be applied hierarchically. For example, a standard could be developed that allowed a security officer to degauss CONFIDENTIAL tapes by 80 db, SECRET tapes by 90 db, etc. Practice has shown, however, that this is not a feasible approach. Authorized clearing and purging procedures are detailed in DoD 5200.28-M and sometimes further amplified in DoD component regulations.

Declassification: A procedure and an administrative action to remove the security classification of the subject media. The procedural aspect of declassification is the actual purging of the media and removal of any labels denoting classification, possibly replacing them with labels denoting that the storage media is unclassified. The administrative aspect is realized through the submission to the appropriate authority of a decision memorandum to declassify the storage media.

Whether declassifying or downgrading the storage media, the memorandum should include the following:

a. A description of the media (type, manufacturer, model, and serial number).
b. The media's classification and requested reclassification as a result of this action.
c. A description of the purging procedures to include the make, model number, and serial number of the degausser used and the date of the last degausser test if degaussing is done; or the accreditation statement of the software if overwriting is done; or the description of and authorization to use the purging procedure if the purging procedure is different from the preceding procedures.
d. The names of the people executing the procedures and verifying the results.
e. The reason for the downgrade, declassification, or release.
f. The concurrence of the data owner that the action is necessary.
g. The intended recipient or destination of the AIS and storage media.

Coercivity: Measured in oersteds (Oe), is a property of magnetic material used as a measure of the amount of applied magnetic field (of opposite polarity) required to reduce magnetic induction to zero from its remanent state, i.e., taking the media from a recorded state to an unrecorded state. Coercivity values are available from the manufacturer or vendor.

Type I Tape: Magnetic tape with coercivity not exceeding 350 Oe (also known as low-energy tape), for example, iron oxide coated tape. Note: The maximum coercivity level has changed from 325 Oe to 350 Oe.

Magnetic disks, i.e., oxide particles on a metal substrate, also have varying coercivity levels. Research has shown, however, that the physical remanence properties of disks are easier to address. Because of this, disks are treated as Type I media and are discussed in more detail later.

Type II Tape: Magnetic tape with coercivity ranging from 351 to 750 Oe (also known as high-energy tape), for example, chromium dioxide coated tape.

The determination of the Types l and II definitions was largely a result of the tape manufacturing industry. Low-energy tapes were developed first, and they have coercivities around 300 Oe + 10%. The next generation tape was high-energy tape, whose coercivity is around 650 Oe + 10%. There have been no naturally occurring plateaus for which to define a Type Ill tape. As a practical matter, there are no degaussers that can yet meet the requirements of National Security Agency/Central Security Service (NSA/CSS) Specification L14-4-A for tapes above Type II. [13]

Type III Tape: Magnetic tape with coercivity above 750 Oe, for example, cobalt-modified iron oxide coated tape and metallic particle coated tape. This definition is provided so these media may be discussed.

Degausser: A device that can generate a magnetic field for degaussing magnetic storage media. A Type l degausser can purge Type I tapes and all magnetic disks. A Type II degausser can purge both Types I and II tapes. There are, at present, no Type III degaussers. Currently, all Type I, II, and III tapes may be cleared with a Type I degausser. However, Type III tapes with higher than the current maximum coercivity may be developed that would not be clearable with a Type I degausser. Refer to the DPL for Type III degausser availability. Section 3 discusses degaussers further.

Permanent Magnet Degausser: A hand-held permanent magnet that has satisfied the requirement to degauss floppy disks, disk platters, magnetic drum surfaces, bubble memory chips, and thin film memory modules. It is not used to degauss magnetic tape.

2.3 OBJECT REUSE AND DATA REMANENCE

The issue of data scavenging on multiuser systems was recognized to be an area of concern long before the DoD 5200.28-STD, Trusted Computer System Evaluation Criteria (TCSEC), [20] became the metric with which to evaluate trusted systems. The TCSEC reflects this concern with its requirement that a Trusted Computing Base (TCB) have a mechanism that enforces an object reuse policy. This mechanism must ensure that no user can use the TCB interface to recover

another user's data from recycled storage media (e.g., memory or disk pages). Object reuse in trusted computing systems is comparable (in most respects) to "clearing."

Object reuse can be implemented so that the address space that contained the object (file) is cleared upon deallocation (the net result is that unallocated address space is cleared) or upon allocation (the net result is that unallocated address space may contain data residue). (Note: There are other ways to implement object reuse which do not involve clearing.) Information from a common data storage pool cannot normally be retrieved through the keyboard.

Some comparisons have been made between trusted systems that satisfy the object reuse requirement and overwrite programs that do only clearing or purging; however, it should be noted that overwrite programs cannot be trusted in the same sense as trusted systems. This is primarily because of the environment in which overwrite programs must operate.

Trusted systems are designed with an object reuse mechanism that is protected and supported by the TCB, substantiating the degree of trust placed in the object reuse mechanism. Commercially available overwrite programs are usually designed to operate on several different systems and are not evaluated with the same rigor as trusted systems; however, any overwrite program should be protected from unauthorized modification. These two security features provide a similar aspect of data confidentiality but satisfy different computer security requirements.

3 DEGAUSSERS

DoD 5200.28-M requires that degaussing equipment be tested and approved by a laboratory of a DoD component or a commercial testing laboratory where the evaluation tests may be certified. Test methods and performance criteria are promulgated in DoD 5200.28-M. National Security Agency/Central Security Service (NSA/CSS) Specification L14-4-A, Magnetic Tape Degausser, [13] is an updated version of DoD 5200.28-M degausser testing requirements. The NSA/CSS has ensured that degausser testing criteria are current by publishing NSA/CSS Specification L14-4-A.

3.1 A PRIMER

Data are stored in magnetic media by making very small areas called magnetic domains change their magnetic alignment to be in the direction of an applied magnetic field. This phenomena occurs in much the same way that a compass needle points in the direction of the earth's magnetic field. Degaussing, commonly called erasure, leaves the domains in random patterns with no preference to orientation, thereby rendering previous data unrecoverable. There are some domains whose magnetic alignment is not randomized after degaussing. The information that these domains represent is commonly called magnetic remanence. Proper degaussing will ensure that there is insufficient magnetic remanence to reconstruct the data.

Erasure via degaussing may be accomplished in two ways: in AC erasure, the media is degaussed by applying an alternating field that is reduced in amplitude over time from an initial high value (i.e., AC powered); in D

erasure, the media is saturated by applying a unidirectional field (i.e., DC powered or by employing a permanent magnet).

3.2 DEGAUSSER TESTING

The DoD has adopted the National Security Agency security standard for degaussing equipment, which requires degaussers to reduce a special worst-case analog test signal by 90 decibels (db). More simply stated, degaussing must reduce the test signal to one billionth (1 part in 109) of its original strength. However, the signals recorded on magnetic media are easier to erase than the worst-case test signal. This signal is a test signal that magnetically saturates a tape and is set forth in references 1 and 13. After the test signal is recorded on the tape, the tape is degaussed and the residual signal is evaluated against the 90 db standard. This quantifies degausser effectiveness.

3.3 LABELING TAPES

It is difficult to distinguish the different types of magnetic tape from appearance alone. For this reason, it is recommended that responsible personnel ensure that type labels (i.e., Type I, II, or III) are applied to the tape reels upon initial use. The label should remain on the reel until the tape is cut from the reel or the reel is destroyed.

In some cases, adding another label to the tape could introduce the possibility of operator error in shops where the reel is already crowded with labels. Some facilities require the security officer to use the manufacturer's label to determine tape coercivity. In any case, strict inventory controls should be in place to ensure that tapes can be identified by type so the correct purge procedure is used.

3.4 DEGAUSSER PRODUCTS LIST (DPL)

The list of magnetic degaussers that satisfy the requirements in NSA/CSS Specification L14-4-A is included in the NSA's Information Systems Security Products and Services Catalogue [10] as the DPL. The catalogue is updated quarterly and is available through the U.S. Government Printing Office.

3.5 DEGAUSSING EQUIPMENT FAILURE

Because of the possibility of equipment failure, degaussing equipment should be periodically tested to verify correct operation throughout the life cycle of the equipment. Preventive maintenance should be done on a regular schedule to preclude mechanical or electrical problems. Some manufacturers have maintenance contracts and recommended maintenance schedules to ensure the integrity of the degaussing procedure.

To provide a rough estimate of degausser effectiveness, an on-site test of generated magnetic field strength may be done by using a gaussmeter for some models of Type I degaussers. (Some Type I degaussers cannot be tested in this manner because the degaussing field is not accessible.) However, a more extensive test is required to maintain an adequate degree of assurance that the degausser is operating correctly.

Both Type I and II degaussers may be periodically tested more extensively by testing against the 90 db test signal strength reduction requirement in NSA/CSS Specification L14-4-A using the following procedure: have the tape prerecorded with the specified test signal (in a testing laboratory), degauss the tape, then return the tape to the laboratory where it can be tested for the remanent signal level. [13] Check with local authorities or engineering personnel to determine if such a service is available to your organization. There are two companies listed in the DPL, Integra Technologies Corporation and Data Security, Incorporated, that can test an installed degausser's effectiveness.

Although this periodic test is not a DoD requirement, it is highly recommended. After a degausser is installed, it should be tested periodically (approximately every six months) for its first two years of operation. This data can be used to develop a histogram of the degausser's operation. Based on this information, an informed decision can be made about extending the interval between testing, e.g., every 9 months, yearly, every 18 months, etc.

Note that it is erroneous to assume that even a newly installed degausser, let alone a degausser several years old, is providing sufficient erasure. It is not prudent to rely upon one DoD evaluation of the degausser manufacturer's product line because of possible product failure.

4 RISK CONSIDERATIONS

Many risks should be considered when reuse or release of AIS storage media is anticipated. AIS security personnel, operations personnel, users, and other designated responsible persons should be aware of these risks before attempting to declassify or make any decision to release storage media.

4.1 DESTINATION OF RELEASED MEDIA

The risk of compromise of sensitive data increases when AIS storage media is released for any reason outside of the controlled environment. Personnel should consider the media's destination when evaluating this risk.

4.2 EFFECTS OF HEAT AND AGE

Version 1 of this document reported that magnetic media stored for either an extended period of time or under high temperature conditions (120 degrees Fahrenheit or greater) becomes more difficult to degauss or erase. Additional research is in progress to validate the effects of heat and age on the erasure process. [14]

4.3 MECHANICAL STORAGE DEVICE EQUIPMENT FAILURE

Some of the early disk drives required manual alignment of read/write heads. The effectiveness of an overwrite on this technology base may be reduced because of equipment failure or mechanical faults, such as misalignment of read/write heads. Hardware preventive maintenance procedures should be done on schedule, and records should be maintained in an effort to prevent this problem.

4.4 STORAGE DEVICE SEGMENTS NOT RECEPTIVE TO OVERWRITE

A compromise of sensitive data may occur if media is released when an addressable segment of a storage device (such as unusable or "bad" tracks in a disk drive or inter-record gaps in tapes) is not receptive to an overwrite. As an example, a disk platter may develop unusable tracks or sectors; however, sensitive data may have been previously recorded in these areas. It may be difficult to overwrite these unusable tracks. Before sensitive information is written to a disk, all unusable tracks, sectors, or blocks should be identified (mapped). During the life cycle of a disk, additional unusable areas may be identified. If this occurs and these tracks cannot be overwritten, then sensitive information may remain on these tracks. In this case, overwriting is not an acceptable purging method and the media should be degaussed or destroyed.

4.5 OVERWRITE SOFTWARE AND CLEARING

Overwriting is an effective method of clearing data. In an operational system, an overwrite of unassigned system storage space can usually accomplish this, provided the system can be trusted to provide separation of system resources and unauthorized users. For example, a single overwrite of a file (or all system storage, if the circumstance warrants such an action) is adequate to ensure that previous information cannot be reconstructed through a keyboard attack. Note: Simply removing pointers to the file will not generally render the previous information unrecoverable. Software used for clearing should be under strict configuration controls. See A Guide to Understanding Configuration Management in Trusted Systems for additional information on this subject. [7]

4.6 OVERWRITE SOFTWARE AND PURGING

The DoD has approved overwriting and degaussing for purging data, although the effectiveness of overwriting cannot be guaranteed without examining each application. If overwriting is to be used in a specific application, software developers must design the software such that the software continues to write to all addressable locations on the media, in spite of intermediate errors. All such errors in usable sectors should be reported with a listing of current content. In addition, unusable sectors must be completely overwritten, because the unusable sector list will not show whether the sector ever contained any sensitive data. If any errors occur while overwriting or if any unusable sector could not be overwritten, then degaussing is required.

There are additional risks to trusting overwrite software to purge disks. The environment in which the software must operate is difficult to constrain. For this reason, care must be exercised during software development to ensure the software cannot be subverted. The overwrite software should be protected at the level of the media it purges, and strict configuration controls should be in place on both the operating system the software must run under and the software itself. The overwrite software must be protected from unauthorized modification. [7]

4.7 CONTRACTUAL OBLIGATION

Leased equipment containing non-removable magnetic storage media should not be

returned to the vendor unless the media is declassified using an approved procedure. Problems may be encountered obtaining warranty repair service or returning the equipment at termination of lease. Contractual maintenance agreements should address the issue of degaussed media and its effect on equipment warranties.

4.8 MAINTENANCE

Proper purging is especially important in relation to maintenance, whether routine or not. Purge procedures should be conducted and the device declassified before uncleared personnel undertake maintenance actions. If purging is impractical, prohibitively expensive, or could destroy the device, then precautions should be taken to reduce the threat to sensitive information on the device. Maintenance actions should be observed by an individual who has been provided with guidance so that improper actions can be discerned and unauthorized disclosure can be prevented.

If test and diagnostic equipment (T & DE) is used on an AIS that has not been purged, there is a possibility that the T & DE can capture sensitive information. To prevent unauthorized disclosure, the T & DE should either be purged after use or remain safeguarded at the highest level of information resident on the AIS.

For example, if a sensitive disk drive is serviced, the escort official should know that the maintenance person is not allowed to remove the damaged disk from the facility. The escort also should be capable of identifying when a maintenance person has altered the protective characteristics of the device.

4.9 DATA SENSITIVITY

AIS storage media may have contained information so sensitive that authorities decided to never allow declassification of the AIS or its storage media. Examples of such sensitive information are communications security (COMSEC) information marked CRYPTO or Single Integrated Operational Plan (SIOP) information. In these cases, the holder of the media should not attempt to declassify or release the media except as directed by proper organizational approving authorities. [9] Destruction may be the only alternative to indefinite storage of such highly sensitive media.

4.10 DEGAUSSING

Although degaussing is the best method for purging most magnetic storage media, it is not without risk. Degaussers can be used improperly. For example, the media may be removed before the degaussing cycle is complete. Also, degaussers can fail or have a reduced capability over time. Good degausser design can alleviate much, but not all, of this risk. This risk can be mitigated by periodic testing (see Section 3.5, "Degaussing Equipment Failure").

Mistakenly using a Type I degausser to purge Type II tape is another risk. Type I degaussers cannot purge Type II tape. Magnetic tape should have a label applied to the reel that identifies the coercivity of the media, because coercivity cannot always be distinguished by physical appearance. Strict inventory controls should be in place to ensure tapes can be identified by

type so the correct purge procedure is used. If type labels are used, they should not be removed from the reel unless the tape is cut from the reel or the reel itself is destroyed. Labels that show classification should not be removed from the reel until the media is declassified. See Section 3.3, "Labeling Tapes," for more information about labels.

5 STANDARDS

5.1 GENERIC PROCEDURES

There are two primary procedures allowed by DoD policy for clearing and purging AIS memory and secondary storage media that have processed sensitive information: overwriting and degaussing. [1] Other procedures are media specific and this section details them where appropriate. The need for destruction arises when the media reaches the end of its useful life.

5.1.1 OVERWRITING

Overwriting is a process whereby unclassified data are written to storage locations that previously held sensitive data. To satisfy the DoD clearing requirement, it is sufficient to write any character to all data locations in question. To purge the AIS storage media, the DoD requires overwriting with a pattern, then its complement, and finally with another pattern; e.g., overwrite first with 0011 0101, followed by 1100 1010, then 1001 0111. The number of times an overwrite must be accomplished depends on the storage media, sometimes on its sensitivity, and sometimes on differing DoD component requirements. In any case, a purge is not complete until a final overwrite is made using unclassified data.

5.1.2 DEGAUSSING

Degaussing is a process whereby the magnetic media is erased, i.e., returned to its initial virgin state. To satisfy the DoD requirement on degaussing a classified magnetic tape, the degausser must have met DoD testing requirements as discussed in Section 3, "Degaussers."

5.1.3 DESTRUCTION

It is good practice to purge media before submitting it for destruction. Media may generally be destroyed by one of the following methods. (Although approved methods, options d and e use acid, which is dangerous and excessive, to remove recording surfaces. Options a, b, and c are recommended over d and e.)

a. Destruction at an approved metal destruction facility, i.e., smelting, disintegration, or pulverization.
b. Incineration.
c. 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 before disposal. Also, ensure proper protection from inhaling the abraded dust.
d. Application of concentrated hydriodic acid (55% to 58% solution) to a gamma ferric oxide disk surface. Acid solutions should be used in a well-ventilated area only by qualified personnel.
e. Application of acid activator Dubais Race A (8010 181 7171) and

stripper Dubais Race B (8010 181 7170) to a magnetic drum recording surface. Technical acetone (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. Extreme caution must be observed when handling acid solutions. This procedure should be done only by qualified and approved personnel.

For additional information on destruction techniques and emergency destruction, see Institute for Defense Analyses (IDA) Report R-321, Emergency Destruction of Information Storing Media. [6]

5.2 SPECIFIC PROCEDURES

DoD 5200.28-M provides accepted DoD procedures to clear, purge, declassify, and destroy storage media. This section, "Standards," is a reflection of those procedures but does not provide the entire procedure (e.g., use three overwrites to purge disks). This is because these standards are evolving and this document, A Guide to Understanding Data Remanence in Automated Information Systems, is not to be construed as replacing policy.

5.2.1 MAGNETIC TAPES

Although overwriting can be used for clearing this media, the method is time consuming and generally never used. Also, inter-record gaps may preclude proper clearing. A better method for clearing Type I, II, and III tapes is degaussing with a

Type I or Type II degausser. This procedure is considered acceptable for clearing, but not purging, all types of tapes.

Degaussing with an appropriate degausser is the only method the DoD accepts for purging this media. Specifically, a Type I degausser can purge only Type I tapes, and Type II degaussers can purge Types I and II tapes. No degausser presently exists that is capable of purging Type III tapes in accordance with NSA/CSS Specification L14-4-A.

5.2.2 MAGNETIC HARD DISKS

The DoD has approved both overwriting and degaussing as methods to clear or purge this media. See Section 4, "Risk Considerations," and DoD 5200.28-M for additional information. Degaussed disks will generally require restoration of factory installed timing tracks. Type I degaussers and approved hand-held magnets can purge this media up to a coercivity level of 1100 oersteds. If hand-held magnets are used, then the magnet must be placed in almost direct contact with the disk, separated by only a tissue to prevent scratching the disk. Sometimes it is possible to insert the magnet between the platters without disassembling them. As a practical matter, if the drive must be disassembled, it is usually easier to destroy the platters than to degauss and then reinstall them.

Recently completed research has indicated that degaussing is an effective method to purge rigid disk media. Large cavity degaussing equipment can be used to erase the data from sealed disk packs and Winchester style hard disk drives while the platters remain in the drive. Care must be exercised to

ensure that the disk drive is not encased in a material that conducts a magnetic field. Research has shown that aluminum housings on Winchester disk drives attenuate the degaussing field by only about 2 db. Operational guidance is now being developed for the DoD.

5.2.3 MAGNETIC DRUMS

The DoD has approved both overwriting and degaussing as methods to clear or purge this media. See Section 4, "Risk Considerations," and DoD 5200.28-M for additional information. Type l degaussers and approved hand-held magnets can purge this media, with the latter being the only practical alternative.

5.2.4 MAGNETIC FLOPPY DISKS AND CARDS

The DoD has approved overwriting for clearing, but not purging, magnetic floppy disks. Degaussing is the preferred method. The technology of magnetic cards is old and not generally used. Degaussing with Type I degaussers or approved hand-held magnets is the only DoD accepted method of purging floppy disks and cards, regardless of their coercivity. See DoD 5200.28-M for additional information.

5.2.5 MAGNETIC CORE MEMORY

The DoD has approved both overwriting and degaussing as methods to clear or purge magnetic core memory. Type I degaussers and hand-held magnets can purge this media. See DoD 5200.28-M for additional information.

5.2.6 PLATED WIRE MEMORY

There are restrictions on overwriting magnetic plated wire memory based on the amount of time that information was resident in the same memory location. See DoD 5200.28-M for additional information.

5.2.7 THIN FILM MEMORY

The DoD has approved both overwriting and degaussing as methods to clear or purge thin film memory. Type l degaussers and approved hand-held magnets can purge this media.

5.2.8 MAGNETIC BUBBLE MEMORY

The DoD has approved both overwriting and degaussing as methods to clear or purge magnetic bubble memory. An alternative procedure for magnetic bubble memory modules that have been designed with a built-in bias voltage control is to adjust (i.e., raise) the bias voltage to a level that would cause the collapse of all the magnetic bubbles. On some bubble devices a chip erase is invoked by pulsing the z-coil. If the memory was designed with a bias control, information will be available from the vendor on the correct bias voltage level to apply to cause the collapse of all the magnetic bubbles. Type l degaussers and approved hand-held magnets can purge this media. Degaussed bubble memory will generally require re-initialization with programs available from the manufacturer. Bubble memory has not been shown to exhibit any magnetic remanence after application of any of these purging methods.

5.2.9 RANDOM ACCESS MEMORY (RAM)

The DoD has approved both overwriting and removal of power as methods to clear or purge RAM. See DoD 5200.28-M for additional information.

5.2.10 READ ONLY MEMORY (ROM)

Because data is permanently stored in ROM, clearing and purging this media has no relevance. See DoD 5200.28-M for additional information.

5.2.11 ERASABLE PROGRAMMABLE READ ONLY MEMORY (UVPROM)

The DoD has approved the use of ultraviolet light to clear or purge UVPROM. See DoD 5200.28-M for additional information.

5.2.12 ELECTRICALLY ERASABLE READ ONLY MEMORY (EEPROM)

The DoD has approved different forms of overwriting (e.g., single-step chip erase, individual overwriting, etc.) as methods to clear or purge EEPROM. See DoD 5200.28-M for additional information.

6 OTHER STORAGE AND OVERWRITE TECHNOLOGY

6.1 OPTICAL DISKS

The following are examples of optical disks: CD-ROM (Read-Only), WORM (Write-Once-Read-Many), and magneto-optical (Read-Many-Write-Many). Currently, no procedures exist that are considered adequate to ensure purging of these media. Magneto-optical disk technology uses a combination of laser optics and magnetics to obtain data densities far surpassing those of magnetic disks alone. Magneto-optical disks can be cleared by a single overwrite, although purging by overwrite is not considered adequate.

6.2 FERROMAGNETIC RAM

This technology couples magnetics with semiconductor random access memory to provide data retention after power is removed. There have been no standards published providing procedures to ensure clearing or purging of these media. However, consistency with all other types of storage media would dictate that a single overwrite is sufficient for clearing.

6.3 DISK EXERCISERS

As noted earlier in Section 4.6, "Overwrite Software and Purging," many drawbacks exist to using overwrite software for purging disks. Some of these drawbacks are not applicable to disk exercisers, which use a dedicated operating system. Winchester disk manufacturers use disk exercisers to do as their name implies-put Winchester disk drives through their paces. To purge a Winchester drive, the Winchester unit must be plugged into the disk exerciser. The disk exerciser is able to write to any part of a disk regardless of whether the operating system labeled the sector unusable. Some of these "exercisers" also have the capability of writing at different frequencies. This makes them a more effective alternative to overwrite software; however, their ability to purge disks has not been tested.

7 FUTURE DIRECTIONS

Several areas in data remanence can benefit from more investigation. After the adequacy of overwrites to ensure purging is determined, the use of disk exercisers for the purging of magnetic disks should be researched. Because of the increasing use of magneto-optical disks, research should be initiated on methods to purge this media also.

A good primer on magnetic coatings used for disks and tapes is Particulate Magnetic Recording: A Review, by Michael P. Sharrock. [18] For a discourse on future storage trends, see Data Storage in 2000-Trends in Data Storage Technologies, by Mark H. Kryder. [12] The IEEE Transactions on Magnetics provides a wealth of information on the field of magnetics, with entire sections devoted to engineering-level discussions related to magnetic remanence in AIS storage media.

Announcements concerning cavity degaussers should be forthcoming. See the Degausser Products List for these announcements and for announcements about decisions concerning magnetic media degaussing.

DoD policy, procedures, and guidance need continual refinement to keep pace with the evolving storage technologies. Although there is no focal point responsible for ensuring erasure standards are current, various agencies have sponsored research that has ensured our erasure standards provide an adequate degree of security. This has caused duplication of effort at times, but it has also provided additional validation of earlier work. However, a focal point would ensure research is duplicated only when necessary. As storage technology advances and clear and purge procedures are developed and refined, this guideline will be periodically updated to reflect the changes. DoD 5200.28-M should be updated also.

GLOSSARY

Automated Information System.
An assembly of computer hardware, firmware, and/or software configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.

AIS Storage Media.
The physical substance(s) used by an AS system upon which data are recorded.

Clearing AIS Storage Media.
Removal of sensitive data from an AS at the end of a period of processing, including from AIS storage devices and other peripheral devices with storage capacity, in such a way that there is assurance, proportional to the sensitivity of the data, that the data may not be reconstructed using normal system capabilities, i.e., through the keyboard. An AIS need not be disconnected from any external network before a clear.

Coercive Force.
A negative or reverse magnetic force applied for reducing magnetic induction to zero.

Coercivity.
The amount of applied magnetic field (of opposite polarity) required to reduce magnetic induction to zero. It is often used to represent the ease with which magnetic media can be degaussed.

Configuration Control.
The process of controlling modifications to the system's hardware, firmware, software, and documentation that provide sufficient assurance that the system is protected against the introduction of improper modifications before, during, and after system implementation. Compare "configuration management."

Configuration Management.
The management of security features and assurances through control of changes made to a system's hardware, software, firmware, documentation, test, test fixtures and test documentation throughout the development and operational life of the system. Compare "configuration control."

Data.
A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by humans or by an AIS.

Declassification of AIS Storage Media.
A procedure and an administrative decision to remove the security classification of the subject media.

Degausser.
A device that can generate a magnetic field for degaussing magnetic

storage media.

Degaussing.
To reduce magnetic induction to zero by applying a reverse magnetizing field. Also called "demagnetizing."

Degausser Products List (DPL).
A list of commercially produced degaussers that meet National Security Agency specifications as set forth in reference 13. The National Security Agency includes this list in their Information Systems Security Products and Services Catalogue.

Designated Approving Authority (DAA).
The official who has the authority to decide to accept the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards. The DAA must be at an organizational level such that he or she has the authority to evaluate the overall mission requirements of the AIS and provide definitive directions to AIS developers or owners relative to the risk in the security posture of the AIS.

Downgrade.
A procedure and an administrative decision to reduce the security classification of the subject media.

Erasure.
A process by which data recorded on storage media is removed.

Gauss.
A unit measure of the magnetic flux density produced by a magnetizing force.

Information System Security Officer (ISSO).
The person responsible to the DAA for ensuring that security is provided for and implemented throughout the life cycle of an AIS from the beginning of the system concept development phase through its design, development, operation, maintenance, and secure disposal.

Information Systems Security Products and Services Catalogue (INFOSEC Catalog).
A catalog issued quarterly by the National Security Agency to assist in the selection of products and services that will provide an appropriate level of information security. The National Security Agency issues the DPL in this publication, which is available through the Government Printing Office.

Inter-Record Gap.
The "area" between data records on a magnetic tape.

Keyboard Attack.
Data scavenging through resources available to normal system users, which may include advanced software diagnostic tools.

Laboratory Attack.
Data scavenging through the aid of what could be precise or elaborate equipment.

Magnetic Field Intensity.
The magnetic force required to produce a desired magnetic flux, given as the symbol H (see definition of "oersted").

Magnetic Flux.
Lines of force representing a magnetic field.

Magnetic Flux Density.
The representation of the strength of a magnetic field, given as the symbol B (see definition of "gauss").

Magnetic Remanence.
The magnetic flux density that remains in a magnetic circuit after the removal of an applied magnetic field. For discussion purposes, it is better to characterize magnetic remanence as the magnetic representation of residual information that remains on magnetic media after the media has been erased.

Magnetic Saturation.
The condition in which an increase in magnetizing force will produce little or no increase in magnetization.

Object Reuse.
The reassignment to some subject of a medium (e.g., page frame, disk sector, or magnetic tape) that contained one or more objects. To be securely reassigned, no residual data from the previously contained object(s) can be available to the new subject through standard system mechanisms.

Oersted.
A unit of magnetic field strength.

Overwrite Procedure.
A procedure to destroy data recorded on AIS storage media by recording patterns of unclassified data over the data stored on the media.

Permanent Magnet Degausser.
Hand-held permanent magnet that generates a magnetic field for degaussing magnetic storage media.

Purge.
The removal of sensitive data from an AIS at the end of a period of processing, including from AIS storage devices and. other peripheral devices with storage capacity, in such a way that there is assurance proportional to the sensitivity of the data that the data may not be reconstructed through open-ended laboratory techniques. An AIS must be disconnected from any external network before a purge.

Remanence.
The residual information that remains on storage media after erasure.

Scavenging.
Searching through object residue (file storage space) to acquire unauthorized data.

Trusted Computer System Evaluation Criteria (TCSEC).
A document published by the National Computer Security Center containing a uniform set of basic requirements and evaluation classes for assessing degrees of assurance in the effectiveness of hardware and software security controls built into systems. These criteria are intended for use in the design and evaluation of systems that will process and/or store sensitive or classified data. This document is DoD 5200.28-STD and is often called The Criteria or The Orange Book.

Trusted Computing Base (TCB).
The totality of protection mechanisms within a computer system, including hardware, firmware, and software, the combination of which is responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system. The ability of a TCB to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g., a user's clearance) related to the security policy.

Trusted Computing System.
A system that employs sufficient hardware and software integrity measures to allow its use for simultaneously processing a range of sensitive or classified information.

Type I Tape.
Magnetic tape whose coercivity does not exceed 350 oersteds (also known as low-energy tape).

Type II Tape.
Magnetic tape whose coercivity ranges from 351 oersteds up to 750 oersteds (also known as high-energy tape).

Type III Tape.
Magnetic tape whose coercivity exceeds 750 oersteds.

REFERENCES

[1]
Automated Data Processing Security Manual, Department of Defense Manual, DoD 5200.28-M, January 1973 with change pages in June 1979 (now under revision).

[2]
Care and Handling of Computer Magnetic Storage Media, Department of Commerce, National Bureau of Standards Special Publication 500-101, June 1983.

[3]
Computer Security Evaluation Center, Department of Defense Directive, DoDD 5215.1,25 October 1982.

[4]
Department of the Navy Automated Data Processing Security Program, Chief of Naval Operations Instruction, OPNAVINST 5239.1A with change 1, 3 August 1982.

[5]
Department of the Navy Automated Information System Security Program, Secretary of the Navy Instruction, SECNAVINST 5239.2, 1 November 1989.

[6]
"Emergency Destruction of Information Storing Media," Institute for Defense Analyses Report, R-321, December 1987.

[7]
A Guide to Understanding Configuration Management in Trusted Systems, National Computer Security Center Technical Guideline, NCSC-TG-006, Version 1,28 March 1988.

[8]
Industrial Security Manual for Safeguarding Classified Information, Department of Defense Manual, DoD 5220.22-M, June 1987.

[9]
Information Systems Security, Army Regulation, AR 380-19, 4 September 1990.

[10]
Information Systems Security Products and Services Catalogue, National Security Agency, quarterly publication.

[11]
Katti, Romney R., "Erasure in Magnetic Recording Media," doctoral dissertation, Carnegie-Mellon University, 12 April 1988.

[12]
Kryder, Mark H., "Data Storage in 2000-Trends in Data Storage Technologies," IEEE Transactions on Magnetics, Vol. 25, No. 6, November 1989.

[13]
Magnetic Tape Degausser, National Security Agency/Central Security Service (NSA/CSS) Specification L1 4-4-A, 31 October 1985.

[14]
Mountfield, K. R., and M. H. Kryder, "The Effect of Erasure in Particulate Disk Media," IEEE Transactions On Magnetics, Vol. 25, No. 5, September 1989.

[15]
National Policy on Telecommunications and Automated Information Systems Security, National Security Decision Directive, NSDD 145, 17 September

1984.

[16] Remanence Security, Air Force Systems Security Instruction, AFSSI 5020,15 April 1991.

[17] Security Requirements for Automated Information Systems, Department of Defense Directive, DoDD 5200.28, March 1988.

[18] Sharrock, Michael P., "Particulate Magnetic Recording: A Review," IEEE Transactions on Magnetics, Vol. 25, No. 6, November 1989.

[19] "Signal Processing Applications Techniques to Magnetic Erasure Data," Illinois Institute of Technology, Research Institute, Final Reports for Projects E06522, K06005, and K06051, February 1982, September 1982, and March 1984 respectively.

[20] Trusted Computer System Evaluation Criteria, Department of Defense Standard, DoD 5200.28-STD, December 1985.

[21] Veeravalli, Venugopal V., "Detection of Digital Information From Erased Magnetic Disks," masters thesis, Carnegie-Mellon University, 1987.

[22] Wiesen, Kurt, "Modeling of Magnetic Media," masters thesis, Carnegie-Mellon University, July 1986.