Security, Remanence, and Sanitizing of Sensitive and Confidential Data

Hashim M. S. Alawadi
Systems Management Solutions, Austin, TX, USA
Joseph D. Mount and Khalid J. Elibiary
Tabernus, Austin, TX, USA

ABSTRACT

When information on an IT system is modified or erased, some or all of the original data may still be stored on the system in some form. This is an inherent characteristic of data storage systems and is referred to as data remanence. This data may then be recovered by unauthorized individuals or organizations using various tools, which may cause serious security risks and/or privacy issues.

Specialized processes and tools are needed to safely remove and secure sensitive and classified data from PCs, peripherals, and network components. This is valuable when the need arises for upgrading, decommissioning, reassigning, or discarding data storage components. Although physical destruction of storage media is required for some types of classified data, data bits may still be recovered by various means such as examining shredded hard drive platters with electron microscopy. Trends, best methods and recommendations are presented for use, even on physically destructed components, to ensure that sensitive/classified data cannot be recovered by unauthorized users. Applying the data overwriting method using an approved tool, in addition to destroying the storage media if called for by operational requirments, represents the most secure form of data sanitizing.

The following topics are discussed:

- Data storage characteristics, issues and risks of handling and decommissioning data.
- Trends and best methods in electronic data sanitizing.
- How to safely remove and secure sensitive and classified data.
- Processes and tools recommendations.

These tools are valuable for government data, bank records, financial data, corporate intellectual property, medical records, etc, and have been evaluated and are in use by major banks, information technology corporations and government agencies in the U.S. and around the world.

1. Introduction

The use of computers and information technology in modern life has become wide spread as more sophisticated systems become available commercially at ever decreasing cost. Computers are used in ever day life from simple communication systems to complicated management systems used by government agencies, businesses, banks, hospitals, etc. As a result, a phenomenon referred to as “Data Remanence” has become pervasive, although not widely understood or recognized.

A Massachusetts Institute of Technology study revealed that 90% of reassigned or recycled computer equipment had critical, useful, information still residing on computer hard drives [1]. Such a gap in data security can have severe consequences for government and commercial organizations. This data liability has forced the several world governments to enforce laws ensuring the security of data.

This paper aims to present the concepts of data remanence to the audience. We will explain how it occurs, the related security issues posed by it, and how to counter the unwanted results of this phenomenon. We will briefly survey how data remanence impacts different IT systems. We will present more focused information as it applies to magnetic storage media, such as tapes and hard drives. From a practical standpoint, magnetic media warrants more attention since it is the most widely used form of data storage in the market ranging from government and corporate data centers to personal computers.

1.1. When is Data Remanence an Issue?

Data remanence becomes a security issue when the need arises to decommission, discard, or reassign a storage device from one department, project or organization to another. Regardless of how data is created, it is stored in different formats on storage devices, such as a hard drive. Sooner or later and for various reasons, this storage device will be discarded, decommissioned, or moved from one use to another. PC equipment, network components, and storage devices may be decommissioned for different reasons such as:

- A device fails and has to be replaced (the device may be discarded or sent back to the manufacturer for warranty credit)
- A device is outdated and has to be upgraded.
- A device is recycled or moved from one agency or department to another (for example, as high end equipment is introduced to government agencies or corporations, older equipment may be moved to a department that may require less computing power, or donated to schools or charities).
- Equipment is re-sold because it still has high economic value.
- A drive has to be cleared of all stored data at the end of a classified project.

When such a storage device contains sensitive information, the device should be sanitized before it is moved or decommissioned to prevent unauthorized access to information. We will discuss why it is best to sanitize the data by the overwriting method at the place of use as a first step, even when other measures such as degaussing or device destruction is mandated. This process reduces risks associated with mishandling of drives while moving them from the point of use to the degauss or destruction facility.

Simply “deleting” a file or “reformatting” a hard drive does not ensure that the information is completely removed or is inaccessible by unauthorized users. There are numerous commercially

available tools that will allow one to view “deleted” files or “reformatted” drives. Thus, there is a need for more reliable techniques to completely remove sensitive information from storage devices. This process is called “Data Sanitizing”.

1.2. Who should be concerned?

If information is power, then IT data in the wrong hands can pose significant risk to national security as well as economic, corporate, and social security. Almost any type of data can be of value to someone somewhere, from breaching national security to corporate business espionage that can threaten the economic and social stability of a nation. Data remanence is of concern to any entity or agency that is concerned about the wrong person accessing its sensitive information when its storage equipment is decommissioned. Sensitive information can mean different things to different entities, from highly classified national secrets to valuable business information to personal private information.

- Government Agencies – sensitive government information including
  - Systems containing national security data bases
  - Intelligence information
  - Military secrets
  - Law enforcement information
  - Databases of national citizen identity and personal information records
  - Equipment installed at embassies, consulates, and various government offices abroad

- Financial Institutions
  - Bank records and management information
  - Customer account numbers, credit card numbers, ATM information (identity theft and credit card fraud are growing problems for consumers and financial institutions costing billions yearly as electronic commerce gains popularity)

- Corporations and Businesses
  - Trade secrets, Competitive information, Intellectual property – a competing company can recover confidential business information and use it to compete unfairly or destroy the competition.

- Medical and Health Services
  - Patient’s records can be compromised releasing patient confidential data that may be abused.
  - Medical records can be used for the purpose of insurance fraud.

- Home
  - Family pictures, emails, online banking information are all examples of private information that can be abused.

2. Data Storage and Remanence

To understand data remanence, it is important to understand how data is stored under typical operating systems such as Microsoft Windows, SunOS, HP-AIX, and Linux. Within an operating system there is a file management system, or file index, which allows users to store and retrieve data files (like documents, data files, pictures, etc.). In this example we will use the FAT (File Allocation Table) file system used by Microsoft. The FAT file system is characterized by the file allocation table that resides within the computer's hard drive and accessed by the operating system. The FAT is an indexing system that points to locations where individual files, containing user data, are stored. When a hard drive is initially formatted, a File Allocation Table is allocated in clusters. After which, when a file is created, an entry is created in the directory and the first cluster number containing data is established. Essentially, the FAT is a linked list of clusters that correspond to files (see figure 1). [3]

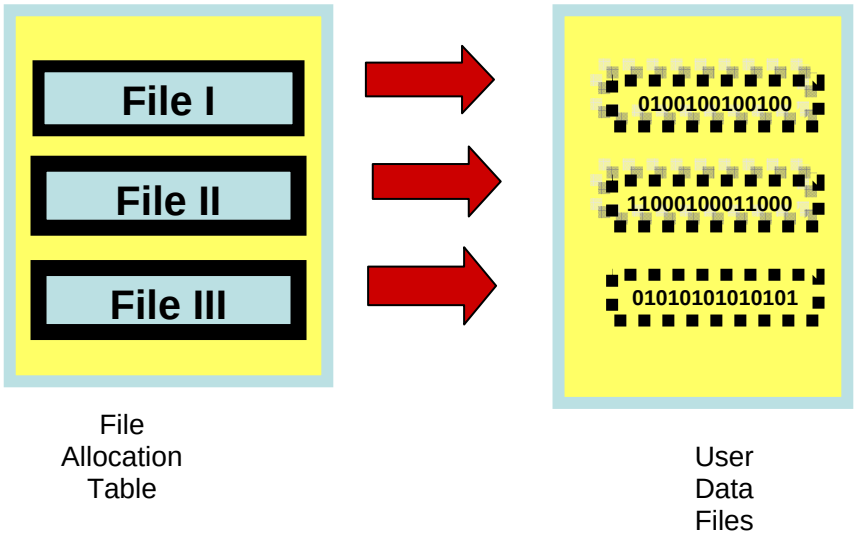


Figure 1: Representation of File Allocation Table

2.1. The Delete Command

Deleted files still reside within the storage system. When an operating system erases a file, two things happen to the file system. The filename is removed from the FAT allowing a file with a similar name to be created again and the clusters associated with the deleted file are released so that another file may use that space in the future. The actual data associated with the file still resides on the hard drive. Parts of a newly created file may or may not be stored in the original file location. Thus a new file may or may not overwrite the old information.

It is a very common misconception that when a user deletes a file or empties the Recycle Bin on their computer, that the actual file is removed from the hard drive. In reality the File Allocation Table has been updated to make the space available for possible use by new data, but the original user data is still

present, and can be easily recovered by third party software or the actual operating system itself (see figure 2).

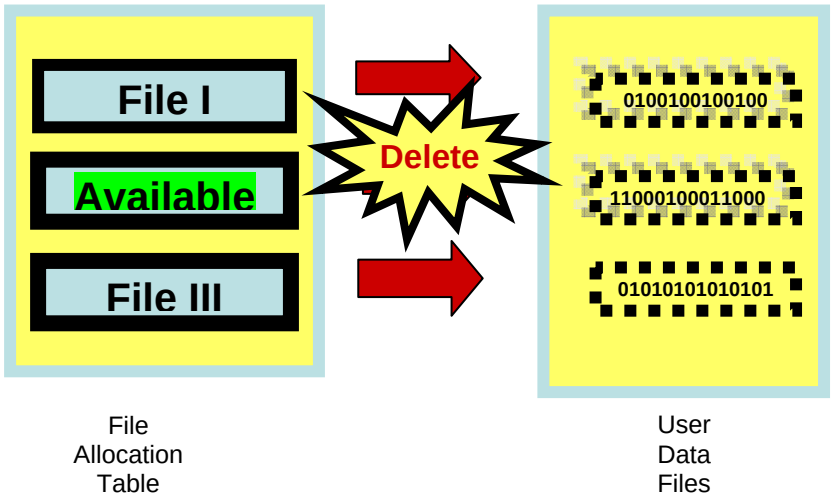


Figure 2: Representation of File Allocation Table after File Deletion: Although the file allocation table shows no record of File 2, the data still exists.

2.2. The Format Command

Another misconception is that formatting a hard drive renders all data unrecoverable. In fact the format command typically overwrites less than 1% of a hard drive. When a format command is issued the only data sectors that are manipulated are associated with the File Allocation Table, Boot Sectors, and base root directory. During the format command the entire hard drive is read in order to determine which blocks on the hard drive are bad and should not be used for file storage. This is what causes the format command to take a relatively long time, and give the wrong impression that all data is being overwritten.

3. Recovering Deleted or Formatted Data

As explained above, residual data remains stored on a storage device after deleting a file or re-formatting a drive. This data can be recovered and viewed easily using commercial tools such as Norton Utilities, and there are many freeware programs that enable you to examine data on hard drives. Even with more advanced data wiping techniques, there still remains a chance that data can be recovered using more sophisticated methods such as examining individual platters of a hard drive in specialized laboratories with advanced measurement tools.

3.1. Recovery Techniques

There are many procedures to recovering files and data which were simply deleted or formatted. Perhaps the easiest is simply to take a hard drive, with data of interest, attach it as a secondary drive to a computer with forensic or data recovery software installed. This will allow the user to see all files on the target drive.

Another technique would be to write a simple computer algorithm which scans a target drive looking for key phrases or numbers. Again, by attaching the storage device of interest to a working computer one could write a computer program that looks for 10 consecutive digits which may be credit card numbers, key words and phrases, or key domain names which could be important email messages.

A more sophisticated method of recovering data is using Magnetic Force Microscopy. This technique uses a sharp magnetic tip attached to a flexible cantilever placed close to the surface to be analyzed, where it interacts with the stray field emanating from the sample to produce a topographic view of the surface. The waveform from the topographic view can be analyzed by a computer to determine the binary state on the hard drive platters thus presenting the possibility if recovering the user data from the storage device [5] [6] [9].

4. Data Sanitizing Methods

As mentioned in section 3, formatting and deleting files are not adequate means of data sanitization, simply because of how easily data can be retrieved. In this section we will discuss various methods of sanitizing, their benefits, and their costs.

4.1. The Overwrite Method

Overwriting means that data blocks stored on a device are replaced with meaningless data blocks. If the overwriting procedure is implemented successfully, with the appropriate tool, the new data will completely cover the tracks of the original data so the original data cannot be recovered for all practical purposes (see figure 3). Overwrite can be accomplished both at a file level and at entire storage device level. When overwriting individual files, data still might not be secure because often operating systems make several copies of working files and store them in temporary directories.

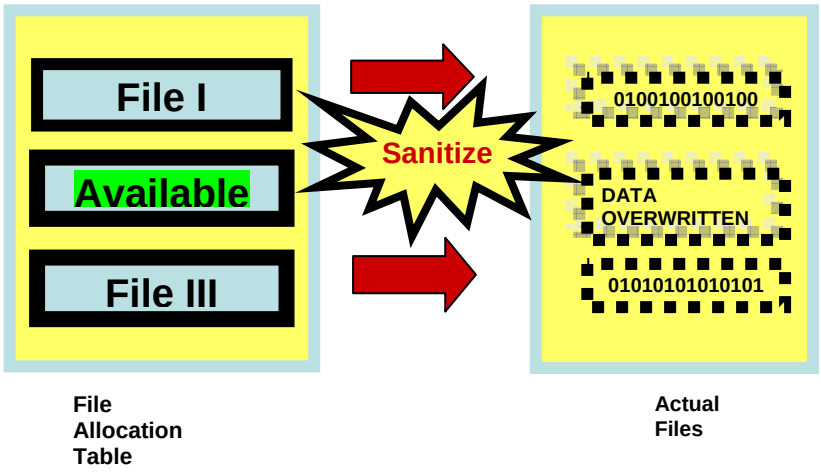


Figure 2: Representation of File After Overwrite Algorithm: the actual data is overwritten and original user data cannot be practically recovered.

4.1.1 Technical Discussion of Overwrite

To understand how this is accomplished, we need to understand how data is actually represented in digital format. Data is stored on a disk by writing tracks that contain binary patterns of 1'and 0's. Each character is represented by a byte, which is 8 individual binary bits of 1s and 0s. For example, the letter A may be represented by "01000001", the letter "B" is "01000010", the letter "C" as "01000011", etc. Meaningful information is represented by numerous bytes, and there are trillions of bytes on a typical hard drive.

When data is overwritten, the 1s and 0s are changed according to a predetermined or random pattern making it difficult, or practically impossible to read the original pattern and thus to recover the overwritten information. Theoretically, it is possible that not all magnetic tracks are 100% overwritten; this maybe true in older, low density drives, or in floppy drives that employ red/write heads that are not very precise. However, for all practical reasons, in modern higher capacity, higher density drives which employ highly tuned read/write heads, it is possible to overwrite all tracks, thus changing each bit according to a predetermined overwrite pattern. According to Feenberg, this is the case for all newer drives of 1.5Gb capacity or higher [7].

Various views have been presented in literature on this subject claiming that electron microscopy can be employed to recover traces of overwritten data. It is suggested that electron microscopy can be used to read bits that may have not been fully overwritten, or to predict what the overwritten data was originally. It is observed that the majority of studies are aimed at laboratory type testing to identify magnetic flux patterns that represent individual bits and test drive performance, and do not represent a practical or effective means of recovering overwritten information [6] [9].

Even if electron microscopy were employed to recover overwritten bits, since all data is represented in binary format (1s and 0s), you can at best recover 50% of individual bits correctly. This does not mean that you can recover 50% of the data. For example, a "10101010" byte may be recovered as "1?1010??". The mathematical probability of reconstructing the large number of bytes used to represent even the simplest information from this recovered pattern is infinitesimally small. When you consider a modern disk that contains billions to trillions of bits, the probability of recovering any useful information from an overwritten drive is practically nil.

It should be emphasized here that to minimize the chance of recovering any data from a disk by employing the overwriting method, the process should be understood and well implemented. One must select the appropriate tool that will ensure overwriting of all data on a drive. An appropriate overwrite pattern calls for 3 passes of overwrite with a character, its complement, and a random character, then 1 pass to read and verify that all data was overwritten correctly. We will discuss detailed criteria for effective overwriting tools below.

encountered during an erase process, should cause the software to fail the hard drive overwrite operation and flag the user for further action.

4.1.2 Advantages of Overwrite

There are several benefits to sanitizing storage devices by overwriting the data. First, overwriting offers the ability to securely erase user data. In addition, there is a feedback mechanism to ensure the drive is correctly sanitized. This is accomplished by reading every byte on the device to ensure it is of a certain value that matches the overwrite pattern. Overwrite allows traceability by generating a serialized log of each affected storage device. The overwrite software can read the drive serial number automatically and generate a log to verify the process. Additionally, a significant benefit, especially to businesses, is preserving the economic value of the device and the ability to reuse the equipment or re-sell it. The ability to reuse devices without compromising sensitive data can be a significant cost factor especially for large organizations.

4.1.3 Disadvantage of Overwrite

There are two disadvantages to sanitizing hard drives using the overwrite procedure. First it is time consuming. Overwriting hard drives will typically take 1 hour for every 20 Gigabytes of data, assuming a 3 pass overwrite with 1 pass verify. Secondly, bad sectors are bytes on the hard drive which quit working during the life of the drive. Most modern hard drives are smart enough to recognize when sectors are going bad and start to move data from bad sectors and into good sectors. However when a sector is bad it can no longer be able to read from or written to. Bad sectors have been a source of debate for overwrite software, in that if the sector is bad no data can be retrieved from it, is it a truly a security issue. This is a limitation of overwrite sanitizing software, any read and write errors.

4.2. Degaussing

Degaussing is the process of using an external device to alter the recorded magnetic flux patterns on the storage device. A degaussing device may be:

- A magnetic wand used to demagnetize the storage media.
- A powerful permanent magnet that imposes a static magnetic field.
- or an alternating current device that produces a strong fluctuating magnetic field that would alter the magnetic characteristics of a storage device to render it unreadable.

4.2.1 Technical Discussion of Degaussing

Degaussing is an appropriate method for sanitizing data. However, it is far more applicable for magnetic tape and floppy disks than for newer fixed disk drives. Older drives and disks were coated with gamma ferric oxides film, which can be demagnetized relatively easy. However modern high density disks use more sophisticated metal oxides and shielding that are meant to resist data degradation and stray magnetic fields to a certain degree. Thus they are more tricky to properly erase by degaussing. They require higher magnetic fields to degauss, which means bulky and expensive degauss equipment and proper isolation so other equipment (such as computers, phones, watches) in the vicinity is not damaged unintentionally. If using portable degaussers, the user may have to disassemble the drive enclosure and platters so they can be degaussed appropriately.

It should be noted that to erase recorded data, it is necessary for the strength of the degaussing field to be greater in value than the coercivity of the magnetic media. Coercivity is the intensity of the applied magnetic field required to reduce the magnetization of the storage device material to zero after the magnetization of the sample has been driven to saturation. Since different drives from different manufacturers may have different magnetic properties, there may not be a universal degausser suitable for all drives. This means the user has the added responsibility to ensure that the degausser being used matches the properties of the drive and the organizational requirements for acceptable demagnetization level. This could prove to be a difficult task for a large organization.

In addition to being cumbersome, an issue with degaussing is that depending on the orientation of the magnetic fields and manual process variations (preparation and placement of disk to be degaussed), complete demagnetizing of all data tracks may not be guaranteed. Also, after degaussing, the disk maybe damaged enough as to not allow verification of data erasure through common read/write processes despite the fact that some tracks may still contain sensitive data. Thus there is no easy way to ensure that a disk has been properly degaussed.

4.2.2 Advantages of Degaussing

Degaussing is relatively fast to implement and can work on any magnetic storage media whether it is functional or not.

4.2.3 Disadvantages of Degaussing

Degaussing equipment capable of erasing modern hard drives can be expensive, with the cost of an NSA approved degausser costing in excess of $25,000 USD. Another drawback to degaussing is the lack of feedback or verification that a device is completely wiped. There is no means to tell if all data has been removed from the storage media, and there is no way to verify which drive was degaussed when handling a large number of devices, since degaussers do not extract the device's serial number prior to sanitization. Additionally, degaussing causes damage to the drive read/write and rotation servos. This permanently destroys the drive mechanics and consequently the storage devices will lose any economic value for future re-use or warranty claims.

4.3. Physical Destruction

Physical destruction of storage devices is another means of making recorded data unrecoverable. This can be accomplished by physically shredding the device, incinerating it, or punching holes in it. Depending on the degree of destruction, data may still be recoverable in a laboratory environment if complete destruction is not accomplished.
Using Magnetic Force Microscopy discussed in section 4, parts of the hard drives magnetic platters can be examined and data might be accessed. Obviously there is an economic loss in physically destroying a hard drive which may be worth hundreds of dollars in actual resale dollars or not sharing the drive within an organization or corporation. In addition, the inability to obtain storage device serial numbers for records may lead to an unverifiable, insecure sanitization process.

5. Selecting the Appropriate Sanitizing Process

The decision on how to sanitize data on a storage device should be based on several factors:

- Assessing the sensitivity, security category, or economic value of the stored data
- Assessing the economic value of the assets or device under consideration, and determining whether it can be re-used, re-sold, has warranty credit, etc.
- Selecting the appropriate data sanitization type based on the information category
- Selecting the appropriate data sanitization method for the media
- Sanitizing the media
- Verifying the result
- Ability to maintain accurate history of which devices were sanitized.

The level of data sensitivity and security as well as economic value varies between organizations. For intelligence applications for example, security may be of utmost concern, while for a financial institution, both security and economics may be equal driving factors.

We have listed the sanitizing procedures recommended by the US Department of Defense for different media in Appendix A. Appendix B contains a table that shows the recommended processes for an extended list if media, based in part on United States Department of Defense recommendations and on industry expert recommendations.

An organization should assess the value of the stored information and the value of the equipment based on its operational and/or business requirements and guidelines. Then the most cost-effective technique for the media and sanitization type can be implemented. Cost considerations should include any loss of residual value from partial or complete destruction of a reusable data storage asset.

We believe that at a minimum, the appropriate overwriting method should be employed, even when other processes are to be followed. This ensures:

1. Verification of user data being wiped.

2. Traceability – drives are logged as they are overwritten with device serial numbers, security erasing standard used, and date of sanitization.

3. Reduced security risk during transportation since physical destruction often requires transportation of devices to specialized areas.

6. Required Criteria for an Effective Overwrite Tool

There are numerous overwrite tools offered in the market. Because modern high density high capacity disk drives contain many hidden sectors that contain drive format and control information, a trusted utility should be used to sanitize a drive. Such a utility should be capable of viewing ALL drive sectors and have access to overwrite/read each sector independent of the operating system. The following features are required for complete erasure of user data, and are required by the US Department of Defense and the UK MOD for software tool compliance:

- The ability to purge all data from the hard drive including the Operating System.

- Capability to run independent of the Operating System of the disposition drive.

- A compatibility with, or capability to run independent of, the type of hard drive being sanitized (e.g., Advanced Technology Attachment (ATA)/Integrated Drive Electronics (IDE) or Small Computer System Interface (SCSI) type hard drives).

- A capability to overwrite the entire hard disk drive independent of any Basic Input/Output System (BIOS) or firmware capacity limitation that the system may have. Older BIOSs can return an incorrect disk size when it is not compatible with a newer larger hard drive. This is

not noticed during normal operation as the flaw is automatically corrected by the operating system. However if the sanitizing product is not independent of the BIOS, then it will only remove the data from part of the hard drive as reported by the BIOS. This will result in data being left behind on the disk.

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

Although not mandatory, selected software should also:

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

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

In addition to these features identified by the US Department of Defense; overwrite software should provides additional robustness to allow it more usage versatility.

- The capability to work with the latest drive technology including SAS (Serial Attached SCSI) and SATA (Serial Advanced Technology Attachment) and Fiber Channel drives.

- The ability to remap and reallocate bad sectors in SCSI and Fiber Channel hard drives.

- The ability to physically view the data on each sector of the hard drive.

- The ability to allow configurable overwrite data patterns, both in number of patterns and the pattern itself, as different organization may require different overwrite patterns to satisfy internal requirements.

- The ability to configure the number of read / write retries to reduce the probability of an erroneous report of a bad sector. This increases the likelihood of a successful overwrite of all sectors.

- The ability to run the overwrite process locally from a CD, or remotely through a network connection.

7. Conclusions

Data remanence in the electronic age is pervasive and a major liability for individuals, businesses, and governments. Perhaps the main reason for data remanence is lack of awareness to the problem and misunderstanding of what actually happens when files are deleted or storage devices are formatted. Once there is proper awareness of the problem there are a variety of solutions to data remanence. The most secure, economic, and generally practiced procedure within governments and corporation involves data overwrite to some degree.

Overwriting storage devices with the appropriate software tool is the practical way to sanitize. This process is used by many government agencies and Fortune 500 companies around the world, including health care providers, financial institutions, hi-tech businesses, and government contractors. This process securely removes sensitive data so it cannot be recovered by unauthorized access and the process is physically verifiable. In addition, sanitization by overwrite preserves the value of the asset or device for future use, resale, getting credit on a warranty claim, etc. Also, overwrite provides a serialized log which allows for cross referencing which assets were erased, to what security level, and at what date.

Even if physical destruction is called for in top secret information applications and economic considerations are not important, a layered protection approach is advisable. Overwriting, using an appropriate tool, in addition to other required processes offers additional protection and traceability. This reduces the risk of device mishandling and security breaches when a device has to be moved to a specialized area for degaussing or physical destruction , thus serving to provide the most secure process for data sanitizing. This most secure process is followed by many of the leading defense contractors in the US and UK.

8. Glossary

Binary: A scheme to represent complex data as a combination of only two states, 1a and 0s.

Bit: A bit is a binary digit, taking a value of either 0 or 1. For example, the number 10010111 is 8 bits long

Byte: A byte is a unit of measurement of information storage, most often consisting of eight bits.

Coercivity: Amount of magnetic field necessary to reduce the magnetic induction to zero. (measured in Oersteds)

Cryptography: The discipline that embodies the principles, means, and methods
for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

Data: Pieces of information from which “understandable information” is derived.
Degauss: To impose a magnetic field on magnetic storage device to neutralize the stored fields representing data

Destruction: The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive.
Digital: A scheme to represent information in one of two states, high or low, 1 or 0. All data can be represented by a combination of these two states.

Information: Meaningful interpretation or expression of data.

Information Security: The term 'information security' means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

Information System: The term 'information system' means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Purge: Rendering sanitized data unrecoverable by laboratory attack methods.

Pulverize: A physically destructive method of sanitizing media; the act of grinding to a powder or dust.

Remanence: Residual information remaining on storage media after clearing.

Sanitize: A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

9. References

[1] “Remembrance of Data Passed: A Study of Disk Sanitization Practices”,
Simson Garfinkel and Abhi Shelat IEEE Security and Privacy, January/February 2003.

[2] “Full Disk Encryption & IT Asset Disposition”, GaurdianEdge White Paper, April 2003.

[3] “Microsoft Extensible Firmware Initiative FAT32 File System Specification,” Microsoft Corp. 6 Dec. 2000.

[4] “Disposition of Unclassified DoD Computer Hard Drives”, Memorandum for the Secretaries of the Military Departments, May 29, 2001.

[5] "Magnetic force microscopy: General principles and application to longitudinal recording media", D.Rugar, H.Mamin, P.Guenther, S.Lambert, J.Stern, I.McFadyen, and T.Yogi, Journal of Applied Physics, Vol.68, No.3 (August 1990), p.1169.

[6] “Magnetic Force Scanning Tunnelling Microscope Imaging of Overwritten Data”, Romel Gomez, Amr Adly, Isaak Mayergoyz, Edward Burke, IEEE Trans.on Magnetics, Vol.28, No.5 (September 1992), p.3141

[7] “Can Intelligence Agencies Read Overwritten Data?” Daniel Feenberg, National Bureau of Economic Research, Cambridge, Massachusettes, May 2004

[8] “Tape & Hard Disk Degaussing, Protect Your Information At Every Step”, John Brandon, Processor, July 14, 2006 • Vol.28 Issue 28

[9] “Unrecoverable Data. The Need for Drive Independent Data Recovery”. Charles H. Sobey, Channel Science – ActionFront Data Recovery Labs, Inc. April 14, 2004

[10] “Cleaning and Sanitization Matrix,” DOS 5220.22-M, US Department of Defense, Washington, D.C., 1995.

[11] “A Guide to Understanding Data Remanence in Automated Information Systems”, National Computer Security Center, Patrick Ghallagher, September 1991.

[12] “Secure Deletion of Data from Magnetic and Solid-State Memory”. Gutmann, Peter, ed San Jose: Sixth USENIX Security Symposium Proceedings, 1996.

[13] “Data Remanence in Semiconductor Devices.” Gutmann, Peter, ed. Washington, D.C: 10th USENIX SECURITY SYMPOSIUM, 2001.

[14] “All About Degausser and Erasure of Magnetic Media” Athana International. 20 June 2005

[15] “NSA/CSS POLICY MANUAL 9-12. Davis”, Harvey A. U.S. National Security Agency – Central Security Service, Fort Meade, Maryland.

[16] “Guidelines For Media Sanitization – Recommendation of the National Institute of Standards and Technology”. Richard kissel et al., NIST Computer Security Division, Information Technology Laboratory Special Publications. Gaithersburg, Maryland, USA, September 2006.

[17] “Security Considerations in the Information System Development Life Cycle”. Tim Grance et al., NIST Computer Security Division, Information Security Laboratory Special Publications Gaithersburg, Maryland, USA, June 2004

[18] “Procurement Strategies: Good Stuff Cheap”, Scott Berinato, CIO Magazine, October 2002

[19] National Industrial Security Program Operating Manual (DoD 5220.22-M)

[20] Remanance Security Guidebook. NAVSO-P-5239-26, US Navy Naval Information Systems.

[21] "Hard Drive Secure Information Removal and Destruction Guidelines", Royal Canadian Mounted Police, October 2003.

Appendix A

US Department of Defense (DOD) 5220.22-M Standard

There has been a standard in place for some time that addresses the problem of permanent removal of data from a hard drive. The standard was developed by the Defense Security Service (DSS) and is used by many federal and commercial organizations. Under the National Industrial Security Program (NISP), DSS Industrial Security Representatives oversee cleared contractor facilities and assist the organizations' management staff and Facility Security Officers in formulating their security programs. As part of the NISP initiative, DSS has developed the DOD standard 5220.22-M NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL. Among other items, the standard outlines the method to be used for removing data from unclassified hard drives – sanitizing. NISP defines an overwriting technique that will remove any existing data yet leave the hard drive in a state where it can be reused. The process involves the following two steps:

1. Before any sanitization product is acquired, careful analysis to the overall costs associated with overwrite/sanitization should be made. Depending on the contractor's environment, the size of the drive and the differences in the individual products time to perform the sanitization, destruction of the media might be the preferred (i.e., economical) sanitization method.

2. Overwrite all addressable locations with a character, then its complement. Verify "complement" character was written successfully to all addressable locations, then overwrite all addressable locations with random characters; or verify third overwrite of random characters. Overwrite utility must write/read to "growth" defect list/sectors or disk must be mapped before initial classified use and remapped before sanitization. Difference in the comparison lists must be discussed with the DSS Industrial Security Representative (IS Rep) and/or Information System Security Professional (ISSP) before declassification. ***Note:*** *Overwrite utilities must be authorized by DSS before use.*

Recommended data sanitizing processes are listed in the DOD table below.

Department of Defense
Clearing and Sanitization Matrix
(DOD 5220.22-M)

from the January 1995 National Industrial Security Program Operating Manual

Media	Clear	Sanitize
Magnetic Tape1		
Type I	a or b	a, b, or m
Type II	a or b	b or m
Type III	a or b	m
Magnetic Disk		
Bernoullis	a or c	m

Floppies	a or c	m
Non-Removable Rigid Disk	c	a, d, or m
Removable Rigid Disk	a or c	a, d, or m
Optical Disk		
Read Many, Write Many	c	m
Read Only		m, n
Write Once, Read Many (Worm)		m, n
Memory		
Dynamic Random Access memory (DRAM)	c or g	c, g, or m
Electronically Alterable PROM (EAPROM)	i	j or m
Electronically Erasabel PROM (EEPROM)	i	h or m
Erasable Programmable (ROM (EPROM)	k	l, then c, or m
Flash EPROM (FEPROM)	i	c then i, or m
Programmable ROM (PROM)	c	m
Magnetic Bubble Memory	c	a, b, c, or m
Magnetic Core Memory	c	a, b, e, or m
Magnetic Plated Wire	c	c and f, or m
Magnetic Resistive Memory	c	m
Nonvolatile RAM (NOVRAM)	c or g	c, g, or m
Read Only Memory ROM		m
Static Random Access Memory (SRAM)	c or g	c and f, g, or m
Equipment		
Cathode Ray Tube (CRT)	g	q
Printers		
Impact	g	p then g
Laser	g	o then g

Clearing and Sanitization Matrix

a. Degauss with Type I, II, or III degausser.

b. Degauss with same Type (I, II, or III) degausser.

c. Overwrite all addressable locations with a single character.

d. Overwrite all addressable locations with a character, its complement, then a random character and verify. THIS METHOD IS NOT APPROVED FOR SANITIZING MEDIA THAT CONTAINS TOP SECRET INFORMATION.

e. Overwrite all addressable locations with a character, its complement, then a random character.

f. Each overwrite must reside in memory for a period longer than the classified data resided.

g. Remove all power to include battery power.

h. Overwrite all locations with a random pattern, then with binary zeros, and finally with binary ones.

i. Perform a full chip erase as per manufacturer's data sheets.

j. Perform i above, then c above, a total of three times.

k. Perform an ultraviolet erase according to manufacturer's recommendation.

l. Perform k above, but increase time by a factor of three.

m. Destroy - Disintegrate, incinerate, pulverize, shred, or melt.

n. Destruction required only if classified information is contained.

o. Run one page (font test acceptable) when print cycle not completed (e.g. paper jam or power failure). Dispose of output as unclassified if visual examination does not reveal any classified information.

p. Ribbons must be destroyed. Platens must be cleaned.

q. Inspect and/or test screen surface for evidence of burned-in information. If present, the screen must be destroyed.

NOTE: As of 22 April, 2002 shredding of IA products is not authorized.

Appendix B

Summary of Minimum Sanitization Techniques for Different Media (Adopted from NIST standards)

Media Type	Clear	Purge	Physical Destruction
Hard Copy Storages			
Paper and microforms	See Physical Destruction.	See Physical Destruction.	Destroy paper using cross cut shredders which produce particles that are 1 x 5 millimeters in size (reference devices on the NSA paper Shredder EPL), or to pulverize/disintegrate paper materials using disintegrator devices equipped with 3/32 inch security screen (reference NSA Disintegrator EPL.). Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning. When material is burned, residue must be reduced to white ash.
Cell Phones	Manually delete all information, such as calls made, phone numbers, then perform a full manufacturer's reset to reset the cell phone back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	Shred. Disintegrate. Pulverize. Incinerate by burning cell phones in a licensed incinerator.
Personal Digital Assistant (PDA) (Palm, PocketPC, other)	Manually delete all information, then perform a manufacturer's hard reset to reset the PDA to factory state. ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	Incinerate PDAs by burning the PDAs in a licensed incinerator. Shred. Pulverize.
Networking Devices			
Routers (home, home office, enterprise)	Perform a full manufacturer's reset to reset the router back to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	Shred. Disintegrate. Pulverize. Incinerate. Incinerate routers by burning the routers in a licensed incinerator.
Equipment			

Copy Machines	Perform a full manufacturer's reset to reset the copy machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedure.		Shred. Disintegrate. Pulverize. Incinerate. Incinerate copy machines by burning the copy machines in a licensed incinerator.
Fax Machines	Perform a full manufacturer's reset to reset the fax machine to its factory default settings. ** Please contact the manufacturer for proper sanitization procedures.		Shred. Disintegrate. Pulverize. Incinerate. Incinerate fax machines by burning the fax machines in a licensed incinerator.
Magnetic Disks			
Floppies	Overwrite media by using agency-approved software and validate the overwritten data.	Degauss in a NSA/CSS-approved degausser.	Incinerate floppy disks and diskettes by burning the floppy disks and diskettes in a licensed incinerator. Shred.
ATA Hard Drives	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	1. Purge using Secure Erase. The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site. 2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.** 3. Purge media by using agency-approved and validated purge technologies/tools. **Degaussing any current generation hard disk will render the drive permanently unusable.	Disintegrate. Shred. Pulverize. Incinerate. Incinerate hard disk drives by burn
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	Purge using Secure Erase The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site. 2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the	Disintegrate. Shred. Pulverize. Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.

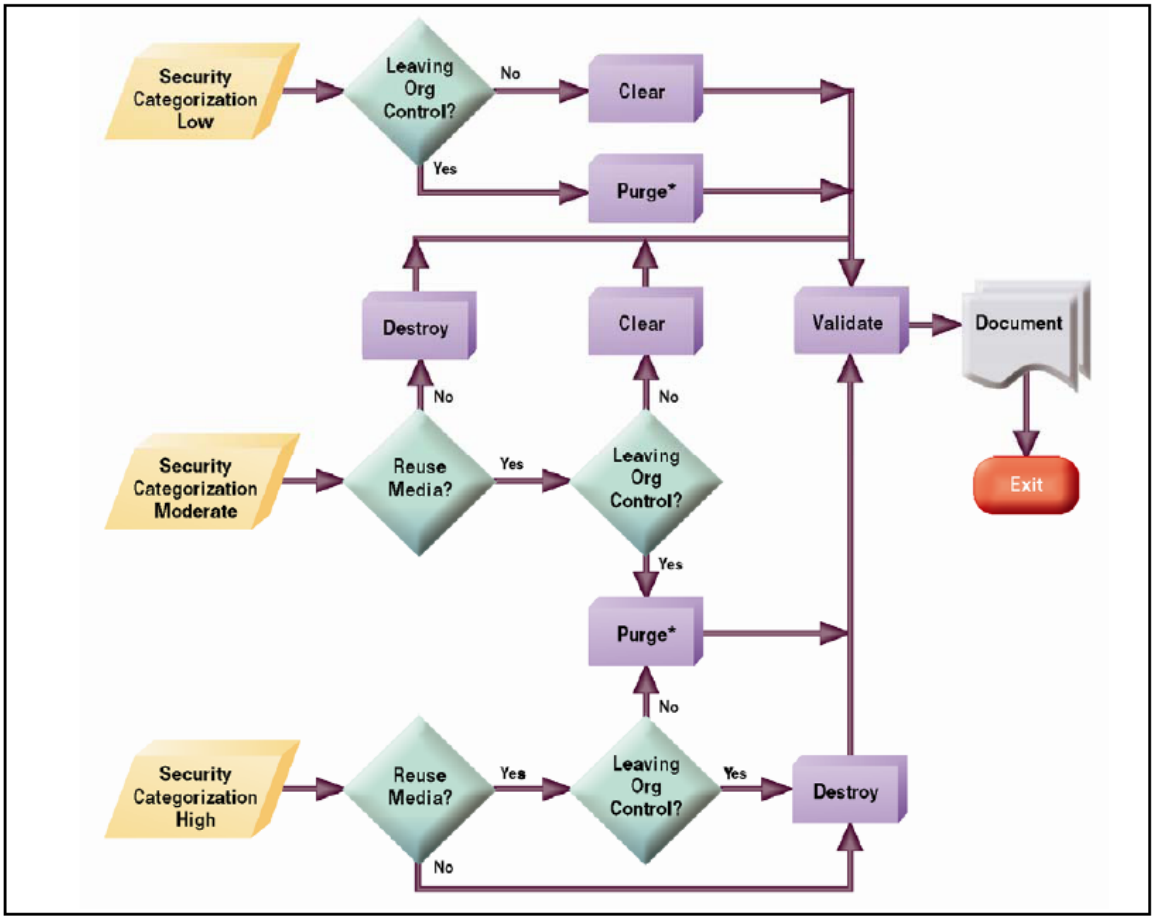
		enclosed platters with an NSA/CSS-approved degaussing wand.** 3. Purge media by using agency-approved and validated purge technologies/tools. **Degaussing any current generation hard disk will render the drive permanently unusable.	
Zip Disks	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	Degauss using a NSA/CSS-approved degausser. **Degaussing any current generation zip disks will render the disk permanently unusable.	Incinerate disks and diskettes by burning the zip disks in a licensed incinerator. Shred.
SCSI Drives	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand. ***Degaussing any current generation hard disk will render the drive permanently unusable.	Disintegrate. Shred. Pulverize. Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
Magnetic Tapes			
Reel and Cassette Format Magnetic Tapes	either re-recording (overwriting) or degaussing. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods. Clearing by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded classified or sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known non-sensitive signals.	Degauss using an NSA/CSS-approved degausser. Purging by Degaussing: Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal. Purging by degaussing can be accomplished easier by using an NSA/CSS-approved degausser for the magnetic tape.	Incinerate by burning the tapes in a licensed incinerator. Shred. Preparatory steps, such as removing the tape from the reel or cassette prior to destruction, are unnecessary. However, segregation of components (tape and reels or cassettes) may be necessary to comply with the requirements of a destruction facility or for recycling measures.
Optical Disks			
CDs / DVDs	See Physical Destruction.	See Physical Destruction.	Destroy in order of

			recommendations: Removing the Information bearing layers of CD media using a commercial optical disk grinding device. Incinerate optical disk media (reduce to ash) using a licensed facility. Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm_2). ** ** This is a current acceptable particle size. Any future disk media shredders obtained should reduce CD to surface area of .25mm^2.
Memory			
Compact Flash Drives, SD	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	See Physical Destruction.	Destroy media in order of recommendations. Shred. Disintegrate. Pulverize. Incinerate by burning in a licensed incinerator.
Dynamic Random Access Memory (DRAM)	Purge DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	Shred. Disintegrate. Pulverize.
Electronically Alterable PROM (EAPROM)	Perform a full chip purge as per manufacturer's data sheets.	Same as Clear.	Shred Disintegrate Pulverize
Electronically Erasable PROM (EEPROM)	Overwrite media by using agency approved and validated overwriting technologies/methods/tools. Remove all labels or markings that indicate previous use or confidentiality.	Same as Clear.	Shred. Disintegrate. Pulverize. Incinerate by burning in a licensed incinerator.
Erasable Programmable ROM (EPROM)	Clear media in order of recommendations. 1. Clear functioning EPROM by performing an ultraviolet purge according to the manufacturer's recommendations, but increase the time requirement by a factor of 3. 2. Overwrite media by using agency-approved and validated overwriting	Same as Clear.	Shred. Disintegrate. Pulverize. Incinerate by burning in a licensed incinerator.

	technologies/methods/tools.		
Field Programmable Gate Array (FPGA) Devices (Non-Volatile)	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	Same as Clear.	Shred. Disintegrate. Pulverize.
Field Programmable Gate Array (FPGA) Devices (Volatile)	Clear functioning FPGA by powering off and removing the battery (if battery backed).	Same as Clear.	Shred. Disintegrate. Pulverize.
Flash Cards	Overwrite media by using agency approved and validated overwriting technologies/methods/tools	Same as Clear.	Shred. Disintegrate. Pulverize.
Flash EPROM (FEPROM)	Perform a full chip purge as per manufacturer's data sheets.	Purge media in order of recommendations. 1. Overwrite media by using agency approved and validated overwriting technologies/methods/tools. 2. Perform a full chip purge as per manufacturer's data sheets.	Shred. Disintegrate. Pulverize. When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance of the destruction device.
Magnetic Bubble Memory	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	Purge by Collapsing the Magnetic Bubbles: 1. Degaussing: Degauss in an NSA/CSS-approved degausser. However, care must be taken to insure that the full field (at least 1500 gauss) of the degausser is applied to the actual bubble array. All shielding materials must be removed from the circuit card and/or bubble memory device before degaussing. 2. Raising the Magnetic Bias Field: Magnetic bubble memory with built-in magnetic bias field controls may be purged by raising the bias voltage to levels sufficient to collapse the magnetic bubbles. Recommend that specific technical guidance be obtained from the bubble memory manufacturer before attempting this procedure.	Shred. Disintegrate. Pulverize. When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance of the destruction device.
Magnetic Core Memory	recommendations. 1. Overwrite media by using agency-approved and validated	Purge core memory devices either by overwriting or degaussing.	Shred. Disintegrate. Pulverize.

	overwriting technologies/methods/tools. 2. Degauss in an NSA/CSS-approved degausser.	Overwrite media by using agency approved and validated overwriting technologies/methods/ tools Degauss in an NSA/CSS-approved degausser. Remove all labels or markings that indicate previous use or confidentiality. NOTE - Attenuation of the magnetic field due to chassis shielding and separation distance are factors that affect erasure performance and should be considered. All steel shielding materials (e.g., chassis, case, or mounting brackets) should be removed before degaussing.	When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance.
Non Volatile RAM (NOVRAM)	1. Overwrite media by using agency approved and validated overwriting technologies/methods/tools. 2. Each overwrite must reside in memory for a period longer than the data resided. 3. Remove all power to include battery power.	Same as Clear.	Shred. Disintegrate. Pulverize.
PC Cards or Personal Computer Memory Card International Association (PCMCIA) Cards	See Physical Destruction.	See Physical Destruction.	Destroy by incinerating in a licensed incinerator or use (an NSA evaluated) a disintegrator to reduce the card's internal circuit board and components to particles that are nominally two (2) millimeters in size.
Programmable ROM (PROM)	See Physical Destruction.	See Physical Destruction.	Destroy by incinerating in a licensed incinerator or use (an NSA evaluated) a disintegrator to reduce the card's internal circuit board and components to particles that are nominally two (2) millimeters in size.
Programmable ROM (PROM)	See Physical Destruction.	See Physical Destruction.	Destroy by incinerating in a licensed incinerator.
RAM	Purge functioning DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	Shred. Disintegrate. Pulverize.
ROM	See Physical Destruction.	See Physical Destruction.	Shred. Disintegrate. Pulverize.

USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) without Hard Drives	Overwrite media by using agency approved and validated overwriting technologies/methods/tools	Same as Clear.	Shred. Disintegrate. Pulverize.
Smart Cards	See Physical Destruction.	See Physical Destruction.	For smart card devices& data storage tokens that are in credit card form, cut or crush the smart card's internal memory chip using metals snips, a pair of scissors, or a strip cut shredder (nominal 2 mm wide cuts). Smart cards packaged into tokens (i.e. SIM chips, thumb drives and other physically robust plastic packages) that are not capable of being shredded should instead be destroyed via incineration licensed incinerator or disintegration to 2 mm size particles.
Magnetic Cards			
Magnetic Cards	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	Degauss in an NSA/CSS-approved degausser.	Shred. Incinerate. Incineration of magnetic cards shall be accomplished by burning the magnetic cards in a licensed incinerator.



Decision Flow Diagram for Sanitizing Data as Recommended by NIST

Appendix C

The Intrinsic Economic Value of Retired or Recycled Equipment

As the number of new storage devices shipped from manufacturers increase year over year, the rate of devices recycling also increases. In 2002 retirement rate of hard drives was over 70%; that is, 212 Million hard drives were shipped and nearly 140 Million hard drives were retired. Because of the high retirement rate as well as backward compatibility of hard drives, a huge secondary (used equipment market) has evolved.

According to a recent CIO survey of 187 information executives, 77 percent are purchasing secondary market equipment, and 46 percent expect to increase their spending in that area next year by an average of 15 percent. Forty-one percent cited lower capital costs as their primary reason for going used, which isn't surprising. The economics of used gear is hard to ignore, where refurbished equipment can be purchased at over a 50% discount to new equipment. Even more significant, 30 percent of survey respondents said that they're there because the performance of new equipment simply doesn't justify its expense. Last year's hardware, it seems, will run this year's applications perfectly well

Major OEM manufacturers like Hewlett Packard and IBM are realizing the potential of the secondary market and have set up recycling / refurbishing facilities for used and leased equipment. These facilities did not exist 5 to 6 years ago. [18]