NIST Special Publication 800-88

Guidelines for Media Sanitization

Recommendations of the National Institute of Standards and Technology

Richard Kissel
Matthew Scholl
Steven Skolochenko
Xing Li

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

August, 2006

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include developing technical, physical, administrative, and management standards and guidelines for cost effective security and privacy of sensitive unclassified information in Federal computer systems. This Special Publication 800-series reports on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-88
Natl. Inst. Stand. Technol. Spec. Publ. 800-88, 41 pages (May, 2006)

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2004

Acknowledgements

The authors, Richard Kissel, Matthew Scholl, Steven Skolochenko and Xing Li wish to express their thanks to colleagues who reviewed the drafts of this document and everyone who provided comments. In particular, their appreciation goes Rick Ayers, Murugiah Souppaya, Mark Wilson, Tanya Brewer and Elizabeth Lennon who assisted with our internal review process. Thanks also goes to William Gill, Dr. Chun Tse, and Dr. Simson Garfinkel for their research, technical support, and written contributions to this document. Thanks also to Kevin Stine of the FDA for his keen insights and assistance with the final review.

This work was sponsored by the Department of Homeland Security (DHS), whose support and guidance in this effort are greatly appreciated.

Table of Contents

List of Figures

List of Tables

Executive Summary

Information systems capture, process, and store information using a wide variety of media. This information is not only located on the intended storage media but also on devices used to create, process, or transmit this information. These media may require special disposition in order to mitigate the risk of unauthorized disclosure of information and to ensure its confidentiality. Efficient and effective management of information that is created, processed, and stored by an information technology (IT) system throughout its life, from inception through disposition, is a primary concern of an information system owner and the custodian of the data.

With the use of increasingly sophisticated encryption, an attacker wishing to gain access to an organization's sensitive information is forced to look outside the system itself for that information. One avenue of attack is the recovery of supposedly deleted data from media. These residual data may allow unauthorized individuals to reconstruct data and thereby gain access to sensitive information. Sanitization can be used to thwart this attack by ensuring that deleted data cannot be easily recovered.

When storage media are transferred, become obsolete, or are no longer usable or required by an information system, it is important to ensure that residual magnetic, optical, electrical, or other representation of data that has been deleted is not easily recoverable. Sanitization refers to the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed.

This guide will assist organizations and system owners in making practical sanitization decisions based on the level of confidentiality of their information. It does not, and cannot, specifically address all known types of media; however, the described sanitization decision process can be applied universally. It should also be noted that Title 40 USC advises system owners and custodians that excess equipment is "Educationally useful" and "Federal equipment is a vital national resource." Wherever possible, excess equipment and media should be made available to schools and non-profit organizations to the extent permitted by law.

1 Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this guide in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all federal agency operations and assets, but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of Office of Management and Budget (OMB) Circular A-130, Section 8b (3), (*Securing Agency Information Systems*) as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

Nothing in this guide should be taken to contradict standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official.

1.2 Purpose and Scope

The information security concern regarding information disposal and media sanitization resides not in the media but in the recorded information. The issue of media disposal and sanitization is driven by the information placed intentionally or unintentionally on the media. With the advanced features of today's operating systems, electronic media used on a system should be assumed to contain information commensurate with the security categorization of the system's confidentiality. If not handled properly, release of these media could lead to an occurrence of unauthorized disclosure of information. Categorization of an information technology (IT) system in accordance with Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, is the critical first step in understanding and managing system information and media.

Based on the results of categorization, the system owner should refer to NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems,* which specifies that, "the organization sanitizes information system digital media using approved equipment, techniques, and procedures. The organization tracks, documents, and verifies media sanitization and destruction actions and periodically tests sanitization equipment/procedures to ensure correct performance. The organization sanitizes or destroys information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media."

This document will assist organizations in implementing a media sanitization program with proper and applicable techniques and controls for sanitization and disposal decisions, considering the security categorization of the associated system's confidentiality.

The objective of this special publication is to assist with decision making when media require disposal, reuse, or will be leaving the effective control of an organization. Organizations should develop and use local policies and procedures in conjunction with this guide to make effective, risk-based decisions on the ultimate sanitization and/or disposition of media and information.

The information in this guide is best applied in the context of current technology and applications. It also provides guidance for information disposition sanitization and control decisions to be made throughout the system life cycle. Forms of media exist that are not addressed by this guide, and media are yet to be developed and deployed that are not covered by this guide. In those cases, the intent of this guide outlined in the procedures section applies to all forms of media based on the evaluated security categorization of the system's confidentiality according to FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.

Before any media are sanitized, system owners are strongly advised to consult with designated officials with privacy responsibilities (e.g., Privacy Officers), Freedom of Information Act (FOIA) officers, and the local records retention office. This consultation is to ensure compliance with record retention regulations and requirements in the Federal Records Act. In addition, organizational management should also be consulted to ensure that historical information is captured and maintained where required by business needs. This should be ongoing, as controls may have to be adjusted as the system and its environment changes.

1.3 Audience

Protecting the confidentiality of information should be a concern for everyone, from federal agencies and businesses to home users. Recognizing that interconnections and information exchange are critical in the delivery of government services, this guide can be used to assist in deciding what processes to use for sanitization or disposal.

1.4 Assumptions

The premise of this guide is that organizations are able to correctly identify the appropriate information categories, confidentiality impact levels, and location of the information. Ideally, this activity is accomplished in the earliest phase of the system life cycle. This critical initial step is outside the scope of this document, but without this identification, the organization will, in all likelihood, lose control of some media containing sensitive information.

This guide does not claim to cover all possible media that an organization could use to store information, nor does it attempt to forecast the future media that may be developed during the effective life of this guide. Users are expected to make sanitization and disposal decisions based on the security categorization of the information contained on the media.

1.5 Relationship to Other NIST Documents

FIPS 199, (Standards for Security Categorization of Federal Information and Information Systems); NIST SP 800-60, (Guide for Mapping Types of Information and Information Systems to Security Categories) provides guidance for establishing the security categorization for a system's confidentiality. This categorization will impact the level of assurance an organization should require in making sanitization decisions.

FIPS 200, (*Minimum Security Requirements for Federal Information and Information Systems*) sets a base of security requirements that requires organizations to have a media sanitization program.

NIST SP 800-53, (*Recommended Security Controls for Federal Information Systems*) provides minimum recommended security controls, including sanitization, for Federal systems based on their overall system security categorization.

NIST SP 800-53A, (*Guide for Assessing the Security Controls in Federal Information Systems)* provides guidance for assessing security controls, including sanitization, for federal systems based on their overall system security categorization.

1.6 Document Structure

The guide is divided into the following five sections and six appendices:

- **Section 1** (this section) explains the authority, purpose and scope, audience, and assumptions of the document, and outlines its structure.
- **Section 2** presents an overview of the need for sanitization and the basic types of information, sanitization, and media.
- **Section 3** provides general information on procedures and principles that influence sanitization decisions.
- **Section 4** provides the user with a process flow to assist with sanitization decision making.
- **Section 5** provides a summary of several general sanitization techniques.
- **Appendix A** contains a matrix of media with minimum recommended sanitization techniques for clearing, purging, or destroying various media. This appendix is to be used with the decision flow chart provided in Section 5.
- **Appendix B** contains a glossary defining terms used in this guide.
- **Appendix C** contains a listing of tools and external resources that can be referenced for assistance with media sanitization.
- **Appendix D** contains information sanitization considerations for a home user or telecommuter who may not have access to organizational resources.

- **Appendix E** contains a listing of sources and correspondence that was essential in developing this guide.
- **Appendix F** contains a sample sanitization form for documenting sanitization activities in an organization.

2 Background

Information disposition and sanitization decisions occur throughout the system life cycle. Critical factors affecting information disposition and media sanitization are decided at the start of a system's development. The initial system requirements should include hardware and software specifications as well as interconnections and data flow documents that will assist the system owner in identifying the types of media used in the system. A determination should be made during the requirements phase about what other types of media will be used to create, capture, or transfer information used by the system. This analysis, balancing business needs and risk to confidentiality, will formalize the media that will be considered for the system to conform to FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*.

Media sanitization and information disposition activity is usually most intense during the disposal phase of the system life cycle. However, throughout the life of an information system, many types of media, containing data, will be transferred outside the positive control of the organization. This activity may be for maintenance reasons, system upgrades, or during a configuration update.

2.1 Need for Proper Media Sanitization and Information Disposition

Media sanitization is one key element in assuring confidentiality. Confidentiality is "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542]

"A loss of confidentiality is the unauthorized disclosure of information." [FIPS-199, Standards for Security Categorization of Federal Information and Information Systems]

In order for organizations to have appropriate controls on the information they are responsible for safeguarding, they must properly safeguard used media. An often rich source of illicit information collection is either through dumpster diving for improperly disposed hard copy media, acquisition of improperly sanitized electronic media, or through keyboard and laboratory reconstruction of media sanitized in a manner not commensurate with the confidentiality of its information. Media flows in and out of organizational control through recycle bins in paper form, out to vendors for equipment repairs, and hot swapped into other systems in response to emergencies. This potential vulnerability can be mitigated through proper understanding of where information is location, what that information is and how to protect it.

2.2 Types of Media

There are two primary types of media in common use:

- Hard Copy. Hard copy media is physical representations of information. Paper printouts, printer, and facsimile ribbons, drums, and platens are all examples of hard copy media. These types of media are often the most

uncontrolled. Information tossed into the recycle bins and trash containers exposes a significant vulnerability to "dumpster divers", and overcurious employees, risking accidental disclosures.

- Electronic (or soft copy). Electronic media are the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment, and many other types listed in Appendix A.

In the future, organizations will be using media types not specifically addressed by this guide. The processes described in this document should guide media sanitization decision making regardless of the type of media in use. To effectively use this guide for all media types, organizations and individuals should focus on the information recorded on the media.

2.3 Trends in Data Storage Media

Computing technologies change rapidly. Users want more powerful but compact devices. New technologies constantly increase processing speed and storage capacity, while decreasing the device size in order to satisfy this demand. These technologies may require new clearing and purging techniques.

Advancing technology has created a situation that has altered previously held best practices regarding magnetic disk type storage media. Basically the change in track density and the related changes in the storage medium have created a situation where the acts of clearing and purging the media have converged. That is, for ATA disk drives manufactured after 2001 (over 15 GB) clearing by overwriting the media once is adequate to protect the media from both keyboard and laboratory attack.

Some emerging data storage technologies are:

- Holographic Storage. Stores data on a holographic (3-dimensional) image by passing light through light-sensitive crystals that retain the light patterns. It will have multiple thousands of times more memory capacity and no mechanical movements. Large blocks of data can be written or read with a single read or write command as opposed to today's 2-dimensional storages devices that read and write data one bit at a time. Researchers believe that a holographic data storage system in which thousands of pages (blocks of data), each containing a million bits, can be stored within the volume of a sugar cube. Ten Gigabytes (GB) of data will fit in one cubic centimeter. Because holographic system can have no moving parts and its pages are accessed in parallel, it is estimated that data throughput on a holographic system can reach one gigabit per second.

- Molecular Memory. Stores data using a protein called bacteriorhodopsin. A laser can change the protein for bR (0 state) to Q (1 state), which makes it an ideal AND data storage gate, or flip-flop. Molecular memory is inexpensive

to produce and can operate over a wider range of temperatures than semiconductor memory. A molecule changes states within microseconds; the combined steps to read or write operation take about 10 milliseconds. That might seem slow. However, like the holographic storage, this device obtains data pages in parallel, so a 10 Mbps throughput speed is possible.

2.4 Types of Sanitization

The key in deciding how to manage media in an organization is to first consider the information, then the media type. The security categorization of the information, along with internal environmental factors, should drive the decisions on how to deal with the media. Again, the key is to first think in terms of information confidentiality, then by media type.

In organizations, information exists that is not associated with any categorized system. This information is often hard copy internal communications such as memoranda, white papers, and presentations. Sometimes this information may be considered sensitive. Examples may include internal disciplinary letters, financial or salary negotiations, or strategy meeting minutes. Organizations should label these media with their internal operating classifications and associate a type of sanitization described in this publication.

There are different types of sanitization for each type of media. We have divided media sanitization into four categories: disposal, clearing, purging and destroying. Disposal exists where media are just tossed out with no special disposition given to them. Some media can be simply disposed if information disclosure would have no impact on organizational mission, would not result in damage to organizational assets, would not result in financial loss or would not result in harm to any individuals. Disposal is mentioned to assure organizations that all media does not require sanitization and that disposal is still a valid method for handling media containing non-confidential information. Since disposal is not technically a type of sanitization, it will not be mentioned or addressed outside of this section.

Encryption is not a generally accepted means of sanitization. The increasing power of computers decreases the time needed to crack cipher text and therefore the inability to recover the encrypted data can not be assured.

It is suggested that the user of this guide categorize the information, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then decide on the appropriate type of sanitization. The selected type should be assessed as to cost, environmental impact, etc., and a decision made that best mitigates the risk to confidentiality and best satisfies other constraints imposed on the process.

Table 2-1. Sanitization Types

Type	Description
Disposal	Disposal is the act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also

Type	Description
	include other media.
Clearing	Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for clearing media. There are overwriting software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not writeable. The media type and size may also influence whether overwriting is a suitable sanitization method. [SP 800-36]. Studies have shown that most of today's media can be effectively cleared by one overwrite. Specific recommendations for clearing different media types are included in Appendix A.
Purging	Purging information is a media sanitization process that protects the confidentiality of information against a laboratory attack. For some media, clearing media would not suffice for purging. However, for ATA disk drives manufactured after 2001 (over 15 GB) the terms clearing and purging have converged. A laboratory attack would involve a threat with the resources and knowledge to use nonstandard systems to conduct data recovery attempts on media outside their normal operating environment. This type of attack involves using signal processing equipment and specially trained personnel. Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. Degaussing is not effective for purging nonmagnetic media, such as optical media [compact discs (CD), digital versatile discs (DVD), etc.). [SP 800-36, Guide to Selecting Information Security Products] Specific recommendations for purging different media types are included in Appendix A. If purging media is not a reasonable sanitization method for organizations, this guide recommends that the media be destroyed.
Destroying	Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting. If destruction is decided upon due to the high security categorization of the information or due to environmental factors, any residual medium should be able to withstand a laboratory attack. ▪ *Disintegration, Incineration, Pulverization, and Melting.* These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. ▪ *Shredding.* Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The

Type	Description
	shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality level that the information cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and magneto-optic (MO) disks must be destroyed by pulverizing, crosscut shredding or burning. Destruction of media should be conducted only by trained and authorized personnel. Safety, hazmat, and special disposition needs should be identified and addressed prior to conducting any media destruction.

2.5 Other Factors Influencing Sanitization and Disposal Decisions

Several factors should be considered along with the security categorization of the system confidentiality when making sanitization decisions. The cost versus benefit of a media sanitization process should be understood prior to a final decision. For instance, it may not be cost-effective to degauss inexpensive media such as diskettes. Even though clear or purge may be the recommended solution, it may be more cost-effective (considering training, tracking, and validation, etc) to destroy media rather than use one of the other options. Organizations can always increase the level of sanitization applied if that is reasonable, and indicated by an assessment of the existing risk.

Organizations should consider the following environmental factors. Note that the list is not all-inclusive:

- What types (e.g., optical non-rewritable, magnetic) and size (e.g., megabyte, gigabyte, and terabyte) of media storage does the organization require to be sanitized?
- What is the confidentiality of the data stored on the media?
- Will the media be processed in a controlled area?
- Should the sanitization process be conducted within the organization or outsourced?
- What is the anticipated volume of media to be sanitized by type of media? [1]
- What is the availability of sanitization equipment and tools?
- What is the level of training of personnel with sanitization equipment/tools?
- How long will sanitization take?
- What type of sanitization will cost more considering tools, training, validation, and reentering media into the supply stream?

[1] SP 800-36 *Guide to Selecting Information Technology Security Products*

3 Roles and Responsibilities:

3.1 Program Managers/Agency Heads

"Ultimately, responsibility for the success of an organization lies with its senior managers."[2] By establishing an effective information security governance structure, they establish the organization's computer security program and its overall program goals, objectives, and priorities in order to support the mission of the organization. Ultimately, the head of the organization is responsible for ensuring that adequate resources are applied to the program and for ensuring program success. Senior management is responsible for ensuring that the resources are allocated to correctly identify types and locations of information and to ensure that resources are allocated to properly sanitize the information.

3.2 Chief Information Officer (CIO)

The CIO[3] is charged with promulgating information security policy. A component of this policy is information disposition and media sanitization. The CIO, as the information custodian, is responsible for ensuring that organizational or local sanitization requirements follow the guidelines of this document.

3.3 Information System Owner

The information system owner[4] should ensure that maintenance or contractual agreements are in place and are sufficient in protecting the confidentiality of the system media and information commensurate with the impact of disclosure of such information on the organization.

3.4 Information Owner

The information owner should ensure that appropriate supervision of onsite media maintenance by service providers occurs, when necessary. The information owner is also responsible for ensuring that users of the information are aware of its sensitivity and the basic requirements for media sanitization.

---

[2]NIST SP 800-18 *Guide for Developing Security Plans for Information Technology Systems*, pg 16.

[3]Information Technology Management Reform Act (Clinger/Cohen) When an agency has not designated a formal CIO position, FISMA requires the associated responsibilities to be handled by a comparable agency official.

[4]The role of the information system owner can be interpreted in a variety of ways depending on the particular agency and the system development life-cycle phase of the information system. Some agencies may refer to the information system owners as program managers or business/asset/mission owners.

3.5 Senior Agency Information Security Officer (SAISO)

The SAISO is responsible for ensuring that the requirements of the information security policy with regard to information disposition and media sanitization are implemented and exercised in a timely and appropriate manner throughout the organization.

3.6 System Security Manager/Officer

Often assisting system management officials in this effort is a *system security manager/officer* responsible for day-today security implementation/administration duties. Although not normally part of the computer security program management office, this person is responsible for coordinating the security efforts of a particular system(s). This role is sometimes referred to as the Computer System Security Officer or the Information System Security Officer.

3.7 Property Management Officer

The property management officer is responsible for ensuring that sanitized media and devices that are redistributed within the organization, donated to external entities or destroyed are properly accounted for.

3.8 Records Management Officer

The records management officer is responsible for advising the system and/or data owner or custodian of retention requirements that must be met so the sanitization of media will not destroy records that should be preserved.

3.9 Privacy Officer

The privacy officer is responsible for providing advice regarding the privacy issues surrounding the disposition of privacy information and the media upon which it is recorded.

3.10 Users

Users have the responsibility for knowing and understanding the confidentiality of the information they are using to accomplish their assigned work and ensure proper handling of information.

4 Information Sanitization and Disposition Decision Making

Organizations can use Figure 4-1 with the descriptions in this section to assist them in making sanitization decisions that are commensurate with the security categorization of the confidentiality of information contained on their media. The decision process is based on the confidentiality of the information, not the type of media. Once organizations decide what type of sanitization is best for their individual case, then the media type will influence the technique used to achieve this sanitization goal.

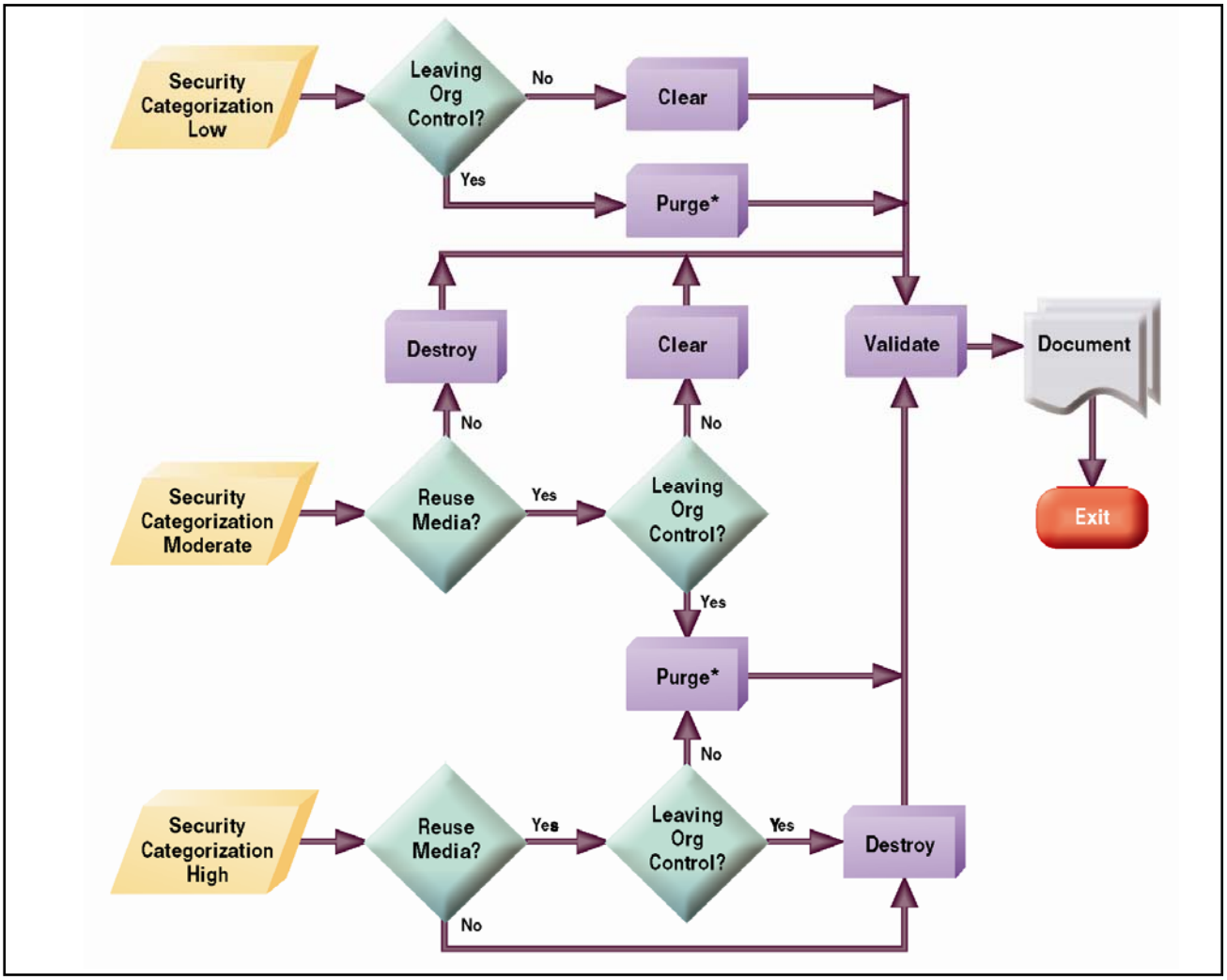


Figure 4-1. Sanitization and Disposition Decision Flow

* For some media, clearing media would not suffice for purging. However, for ATA disk drives manufactured after 2001 (over 15 GB) the terms clearing and purging have converged. Studies have shown that most of today's media can be effectively cleared and purged by one overwrite using current available sanitization technologies.

4.1 Information Decisions In the System Life cycle

The need for, and methods to conduct, media sanitization should be identified and developed before arriving at the system disposal phase in the system life cycle. At the start of system development, when the initial system security plan is developed (see NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Information Technology Systems*), media sanitization controls are developed, documented, and deployed. One of the key decisions that will affect the ability to conduct sanitization is choosing what media are going to be used with the system. Although this is mostly a business decision, system owners must understand early on that this decision affects the types of resources needed for sanitization throughout the rest of the system life cycle.

Organizations should take care in identifying media for sanitization. Many items used will contain multiple forms of media that may require different methods of sanitization. For example, a PC may contain a hard drive, RAM, and ROM, and mobile devices contain on-board volatile memory as well as nonvolatile removable memory in the form of a Subscriber Identity Module (SIM).

4.2 Identification of the Need for Sanitization

One of the first steps in making a sanitization decision is deciding if and when a need exists to sanitize media.

At all points in the system life cycle, media are generated that contain representations of the information held in the system. These media can take different forms, such as simple printouts of data, screenshot captures, or cached memory of user's activities. Organizations must know which media are capturing data and when in order to maintain proper control of the information. This understanding will allow organizations to identify when there is a need to conduct proper sanitization for media disposal. These decisions on proper disposal can be as simple as ensuring placement of paper shredders in work areas during system steady-state activities or address destroying electronic equipment at the end of its life cycle.

4.3 Determination of Security Categorization

Early in the system life cycle, a system is categorized using the guidance found in FIPS 199 and NIST SP 800-60, including the security categorization for the system's confidentiality. This security categorization is often revisited and revalidated throughout the system's life, and any necessary changes to the confidentiality category can be made. Once the security categorization is completed, the system owner can then design a sanitization process that will ensure adequate protection of the system's information.

Much information is not associated with a specific system but is associated with internal business communications, usually on paper. Organizations should label these media with their internal operating classifications and associate a type of sanitization described in this publication.

4.4 Reuse of Media

A key decision on sanitization is whether the media are planned for reuse or recycle. Often, some forms of media are reused to conserve an organization's resources.

If media are not intended for reuse either within or outside an organization due to damage or other reason, the simplest and most cost-effective method of control may be destruction.

4.5 Control of Media

A factor influencing an organizational sanitization decision is who has control and access to the media. This aspect must be considered when media leaves organizational control. Media control may be transferred when media are returned from a leasing agreement or are being donated or resold to be reused outside the organization. The following are examples of media control:

Under Organization Control:

- Media being turned over for maintenance are still considered under organization control if contractual agreements are in place with the organization and the maintenance provider specifically provides for the confidentiality of the information.
- Maintenance being performed on an organization's site, under the organization's supervision, by a maintenance provider is also considered under the control of the organization.

Not Under Organization Control:

- Media that are being exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the organization are considered to be out of organizational control.

4.6 Sanitization and Disposal Decision

Once an organization completes an assessment of its system confidentiality, has determined the need for information sanitization, and has determined the types of media used and the media disposition, an effective, risk-based decision can be made on the appropriate and needed level of sanitization. Again, environmental factors and media type might cause the level of sanitization to change. For example, purging paper copies generally does not make sense, so destroying them would be an acceptable alternative.

Upon completion of sanitization decision making, the organization should document the decision and ensure that a process and proper resources are in place to support these decisions. This process is often the most difficult piece of the media sanitization process because it includes not only the act of sanitization but also the validation: documenting decisions and actions, identifying resources, and having critical interfaces with key officials.

4.7 Verify Methods

Verifying the selected information sanitization and disposal process is an essential step in maintaining confidentiality. A representative sampling of media should be tested for proper sanitization to assure the organization that proper protection is maintained. Verification of the process should be conducted by personnel without a stake in any part of the process.

4.7.1 Verification of Equipment

Verification of the sanitization process is not the only assurance required by the organization. If the organization is using sanitization tools (e.g., a degausser), then equipment calibration, as well as equipment testing, and scheduled maintenance, is also required.

4.7.2 Verification of Personnel Competencies

Another key element is the potential training needs and current expertise of personnel conducting the sanitization. Organizations should ensure that equipment operators are competent to perform sanitization functions.

4.8 Documentation

It is critical that an organization maintain a record of its sanitization to document what media were sanitized, when, how they were sanitized, and the final disposition of the media. Often when an organization is suspected of losing control of its information, it is because of inadequate record keeping of media sanitization.

Organizations should ensure that property management officials are included in documenting the media sanitization process in order to establish proper accountability of equipment and inventory control.

Organizations should conduct sensible documentation activities for media containing low security category information. These are generally considered a consumable or perishable item by property management.

A sample form for organizations to use in documenting sanitization activities is provided in Appendix F.

5 Summary of Sanitization Techniques

Several different methods can be used to sanitize media. Three of the most common are presented in this section. Users of this guide should categorize the information to be disposed of, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then, using information in Table 5-1, decide on the appropriate method for sanitization. The selected method should be assessed as to cost, environmental impact, etc., and a decision should be made that best mitigates the risks to an unauthorized disclosure of information.

Table 5-1. Sanitization Methods

Method	Description
Clear	One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].
Purge	Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging. Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36]
Destroy	There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack. ▪ *Disintegration, Pulverization, Melting, and Incineration.* These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely. ▪ *Shredding.* Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed. Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm^2).

Appendix A. Minimum Sanitization Recommendation for Media Containing Data

Once a decision is made (see section 4) and after applying relevant organizational environmental factors, then Table A-1 can be used to determine recommended sanitization of specific media. This recommendation should reflect the Federal Information Processing Standard (FIPS) 199 security categorization of the system confidentiality to reduce the impact of harm of unauthorized disclosure of information from the media.

Although use of Table A-1 is recommended here, other methods exist to satisfy the intent of clear, purge (still relevant in some cases), and destroy, and methods not specified in this table may be suitable as long as they are vetted and found satisfactory by the organization. Not all types of available media are specified in this table. If your media are not included in this guide, organizations are urged to identify and use processes that will fulfill the intent to clear, purge, or destroy their media.

When an organization or agency has a sanitization technology, method and/or tool that they trust and have validated, they are strongly encouraged to share this information through public forums, such as the Federal Agency Security Practices (FASP) website. The FASP effort was initiated as a result of the success of the Federal Chief Information Officer (CIO) Council's Federal Best Security Practices (BSP) pilot effort to identify, evaluate, and disseminate best practices for critical infrastructure protection (CIP) and security. FASP can be found at http://csrc.nist.gov/fasp/.

Table A-1. Media Sanitization Decision Matrix

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.
Hand-Held Devices			

Media Type	Clear	Purge	Physical Destruction
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.	Same as Clear.	▪ 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.	Same as Clear.	▪ 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.

Media Type	Clear	Purge	Physical Destruction
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 burning the hard disk drives in a licensed incinerator.
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.	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 burning the hard disk drives in a licensed incinerator.

Media Type	Clear	Purge	Physical Destruction
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.

Media Type	Clear	Purge	Physical Destruction
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	Clear magnetic tapes by 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	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 CD into particles that have a surface area of 5 mm.** ** This is a current acceptable particle size. Any future disk media shredders obtained should reduce CD to surface area of .25mm.

Media Type	Clear	Purge	Physical Destruction
DVDs	See Physical Destruction.	See Physical Destruction.	Destroy in order of recommendations: ▪ Removing the Information bearing layers of DVD 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 DVD into particles that have a surface area of 5 mm. ** This is a current acceptable particle size. Any future disk media shredders obtained should reduce DVD to surface area of .25mm.
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.

Media Type	Clear	Purge	Destroy
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 technologies/methods/tools.	Same as Clear.	▪ Shred. ▪ Disintegrate. ▪ Pulverize. ▪ Incinerate by burning in a licensed incinerator.
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. ▪ Incinerate by burning in a licensed incinerator.
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	▪ 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.

Media Type	Clear	Purge	Destroy
		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.	
Magnetic Core Memory	Clear media in order of recommendations. 1. Overwrite media by using agency-approved and validated overwriting technologies/methods/tools. 2. Degauss in an NSA/CSS-approved degausser.	Purge core memory devices either by overwriting or degaussing. ▪ 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.	▪ Shred. ▪ Disintegrate. ▪ Pulverize. 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.

Media Type	Clear	Purge	Destroy
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.
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.

Appendix B. Glossary

Glossary Term	Definition
Clear	To use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. See comments on clear/purge convergence.
CD	Compact Disc: a class of media on which data are recorded by optical means.
CD-RW	Compact Disc Read/Write: A CD that can be purged and rewritten multiple times.
CD-R	Compact Disc Recordable: A CD that can be written on only once but read many times. Also known as WORM.
CMRR	The Center for Magnetic Recording Research (CMRR) advances the state-of-the-art in magnetic storage, and trains graduate students and postdoctoral professionals. The Center is located at the University of California, San Diego.
Data	Pieces of information from which "understandable information" is derived.
Degauss	To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI and Jaz) will render the drive permanently unusable since these drives store track location information on the hard drive in dedicated regions of the drive in between the data sectors.
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	The binary coding scheme generally used in computer technology to represent data as binary bits (1s and 0s).
Disintegration	A physically destructive method of sanitizing media; the act of separating into component parts.
Disposal	Disposal is the act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media.
DVD	Digital Video Disc – a disc the same shape and size as a CD; but the DVD has a higher density and gives the option for data to be double-sided or double-layered.
DVD-RW	A rewritable (re-recordable) DVD disk for both movies and data from the DVD Forum.
DVD+RW	A rewritable (re-recordable) DVD disk for both movies and data from the DVD+RW Alliance.
DVD+R	A write-once (read only) version of the DVD+RW optical disk from the DVD+RW Alliance.
DVD-R	A write-once (read only) DVD disk for both movies and data endorsed by the DVD Forum.
Electronic Media	General term that refers to media on which data are recorded via an electrically based process.
Erasure	Process intended to render magnetically stored information irretrievable by normal means.
FIPS	Federal Information Processing Standard.
Format	Pre-established layout for data.
Hard Disk	A rigid magnetic disk fixed permanently within a drive unit and used for storing data.
Incineration	A physically destructive method of sanitizing media; the act of burning completely to ashes.
Information	Meaningful interpretation or expression of data.
Media	Plural of medium.

Glossary Term	Definition
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Medium	Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs.
Melting	A physically destructive method of sanitizing media; to be changed from a solid to a liquid state generally by the application of heat.
Optical Disks	A plastic disk that is "written" (encoded) and "read" using an optical laser device. The disc contains a highly reflective metal and uses bits to represent data by containing areas that reduce the effect of reflection when illuminated with a narrow-beam source, such as a laser diode.
Overwrite	Writing patterns of data on top of the data stored on a magnetic medium. NSA has researched that one overwrite is good enough to sanitize most drives. See comments on clear/purge convergence.
Physical Destruction	A sanitization method for optical media, such as CDs.
Pulverization	A physically destructive method of sanitizing media; the act of grinding to a powder or dust.
Purge	Rendering sanitized data unrecoverable by laboratory attack methods. See comments on clear/purge convergence.
Read	Fundamental process in an information system that results only in the flow of information from an object to a subject.
Record	To write data on a medium, such as a magnetic tape, magnetic disk, or optical disc.
Recovery Procedures (recoverable)	Action necessary to store data files of an information system and computational capability after a system failure.
Remanence	Residual information remaining on storage media after clearing.
Residue	Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place.
ROM	Read Only Memory. Generally a commercially available disc or solid state device on which the content was recorded during the manufacturing process.
Sanitize	Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
Secure Erase	An overwrite technology using firmware based process to overwrite a hard drive. Is a drive command defined in the ANSI ATA and SCSI disk drive interface specifications, which runs inside drive hardware. It completes in about 1/8 the time of 5220 block erasure. It Was added to the ATA specification in part at CMRR request. For ATA drives manufactured after 2001 (Over 15 GB) have the Secure Erase command and successfully pass secure erase validation testing at CMRR. A standardized internal secure erase command also exists for SCSI drives, but it is optional and not currently implemented in SCSI drives tested by CMRR. SCSI drives are a small percentage of the world's hard disk drives, and the command will be implemented when users demand it.
Shred	A method of sanitizing media; the act of cutting or tearing into small particles.
Storage	Retrievable retention of data. Electronic, electrostatic, or electrical hardware or other elements (media) into which data may be entered, and from which data may be retrieved.
WORM	Write-Once Read Many.
Write	Fundamental operations of an information system that results only in the flow of information from a subject to an object.

This Page Intentionally Left Blank

Appendix C. Tools and Resources

Many different government, U.S. military, and academic institutions have conducted extensive research in sanitization tools, techniques, and procedures in order to validate them to a certain level of assurance. The National Institute of Standards and Technology (NIST) does not conduct an evaluation of any tool set to validate its ability to clear, purge, or destroy information contained on any specific medium.

Organizations are encouraged to seek products that they can evaluate on their own. They can use a trusted service or other federal organizations' evaluation of tools and products and they are expected to continually monitor and validate the effectiveness of their selected sanitization tools as they are used.

If an organization has a product that they trust and have validated, then they are strongly encouraged to share this information through public forums, such as the Federal Agency Security Practices (FASP) website. The FASP effort was initiated as a result of the success of the Federal Chief Information Officer (CIO) Council's Federal Best Security Practices (BSP) pilot effort to identify, evaluate, and disseminate best practices for critical infrastructure protection (CIP) and security. FASP can be found at http://csrc.nist.gov/fasp/.

This guide also recommends that the user consider the NSA devices posted on the public NSA website. NSA states "The products on these lists have met NSA specific performance requirements; however, inclusion on the list does not constitute an endorsement by NSA or the U.S. government.

NSA/CSS-EPL-02-01-M - NSA/CSS Evaluated Products List (EPL) for High Security Crosscut Paper Shredders, Annex A to NSA/CSS 02-01, version M, dated: April 2005

NSA/CSS-EPL-02-02-F - NSA Evaluated High-Security Disintegrators, Annex A to NSA/CSS 02-02, version F, dated: April 2005

NSA/CSS EPL 04-02-B - Optical Media Destruction Devices, Annex A to NSA/CSS 04-02, version B, Date: 30 September 2005

NSA/CSS-EPL-9-12A-B - Degausser Approved Products List - Annex A to NSA/CSS Manual 130-2, version B, dated: May 2005"

In addition to the NSA device listing, the Defense Security Service (DSS) publishes an Assessed Product List (APL), which is a listing of products assessed against the vendors claims of sanitation. The DSS APL states, "The APL does not endorse any company's product, nor does it constitute certification or accreditation for the product's use in a classified environment. The intent is to give security personnel

information on the capability of the product, whereby, they can determine the possible application of the product to meet their security requirement."[5]

This listing can be found at http://www.dss.mil/infoas/assessed_products_list.doc.

For hard drive devices or devices where firmware purge commands can be accessed and utilized, this may be the best option for an organization. Firmware purge commands can provide strong assurance of data protection while allowing the device to be reused. More information on firmware secure erasure for ATA hard drives can be found at http://cmrr.ucsd.edu/hughes/subpgset.htm.

Organizations and individuals wishing to donate used electronic equipment or seeking guidance on disposal of residual materials after sanitization should consult the Environmental Protection Agencies (EPA) electronic recycling and electronic waste information website at http://www.epa.gov/e-Cycling/. This site offers advice, regulations, and standard publications related to sanitization, disposal, and donations. It also provides external links to other sanitization tool resources.

Organizations can outsource media sanitization and destruction if business and security management decide that this would be the most reasonable option for them to maintain confidentiality while optimizing available resources. When exercising this option, this guide recommends that organizations exercise "due diligence" when entering into a contract with another party engaged in media sanitization. Due diligence for this case is accepted as outlined in 16 CFR 682 which states "due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule [guide], obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.'[6]

[5] http://www.dss.mil/infoas/assessed_products_list.doc.

[6] Federal Trade Commission 16 CFR Part 682, *Disposal of Consumer Report Information and Records* Section 682.3 (b) (3).

Appendix D. Considerations for the Home User and Telecommuter

For home users and telecommuters needing to sanitize media, media sanitization methods developed for organizations might be impractical or unsafe. Telecommuters should check their organizational policies before attempting any type of sanitization. Here are a few guidelines that home users and telecommuters could follow:

- If you are a telecommuter, ensure that you follow your organizations sanitization policies and instructions first. Organization policies and procedures take precedent over these instructions.
- Check your provided instruction manual. If guidance for information sanitization for the system is provided, follow those instructions. Instruction manual sanitization guidance takes precedent over these instructions.
- If you are unsure, unclear or cannot conduct sanitization in a safe manner with suitable assurance that your information has been sanitized, take the system to a professional either through your organization or with an outside vendor.
- Be sure you are ready to dispose of your media. ***Have backup copies made of all your information to keep in a secure place in case you ever need to refer to your data.***
- When you are ready to dispose of the system, ensure you follow all disposal instructions. Many media contain hazardous material.

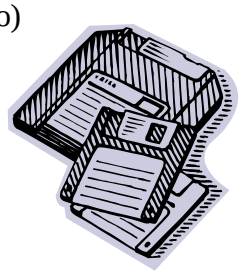
Decide: If you require sanitization for the media under consideration. Is this just a cell phone with public numbers stored in the phone book or is it your home PC with tax preparations, bank account information, and investment records?

First: Ensure that all power sources are disconnected, unplugged, or removed.

If: You have a cell phone, PDA, or other form of mobile computing device,

Then: Manually delete all information. Then see your instruction manual for how to conduct a factory hard reset. Ensure that any removable storage media are removed from the device.

If: You have removable mass storage media, including (but not limited to) compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), Compact Flash, Memory Sticks, Secure Digital, Jump Drives and magneto-optic disks (MO),



Then: These media should be destroyed by shredding, physically breaking, or rendering the media physically unable to be reinserted into the device to read the media.

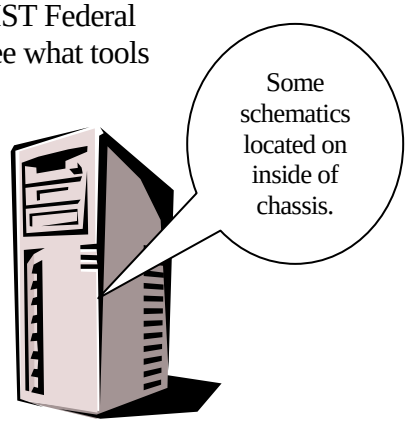
IF: You have a PC,

Then: You can conduct sanitization through the following two methods.

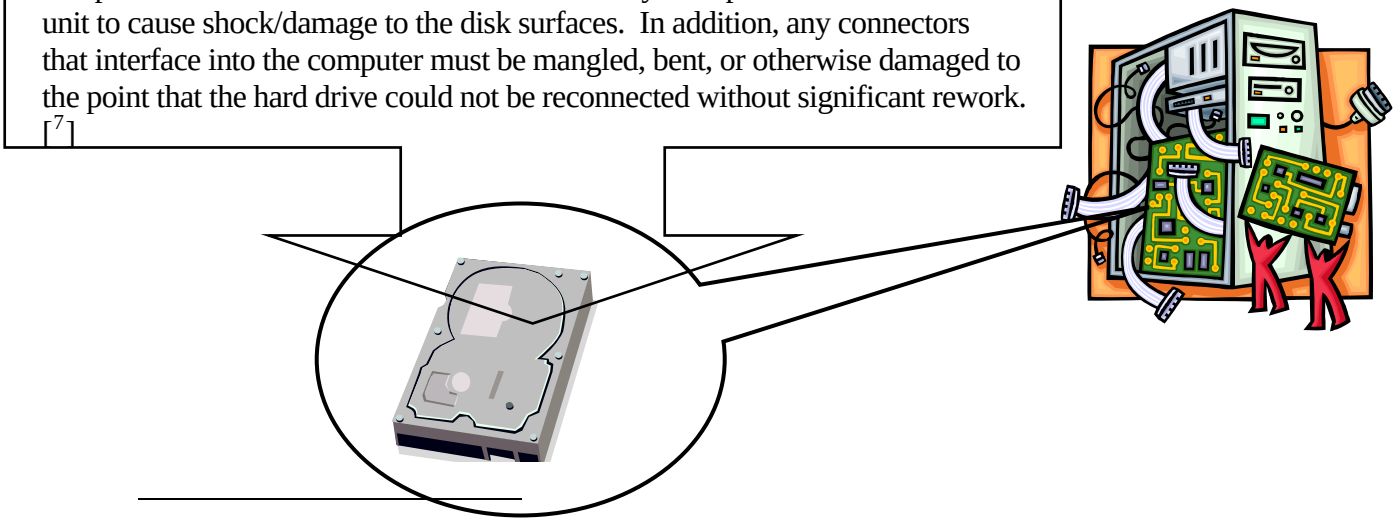
1. Use software to conduct sanitization. Check with your PC maker for a recommended tool and check testimonies of sanitization tools in industry and computing magazines. These resources can be found in hard copy in your local library and online. Conducting online searches for 'Sanitization Tools' and 'Disk Drive Sanitization' will yield multiple sources for research into tools for sanitization. Users can also check the NIST Federal Agency Security Practices (FASP) website at http://csrc.nist.gov/fasp/ to see what tools and procedures some federal agencies are using for sanitization.

2. Physically impair your disk drive to prevent information recovery from a keyboard attack. In order to conduct this, ensure all power sources are disconnected. Locate computer hard drive. Use your provided instruction manual and/or provided schematic to locate. Remove hard drive from PC.

   Remove any steel shielding materials, mounting brackets, and cut any electrical connection to the hard drive unit.



The hard drive should then be subjected, in a suitable facility with individuals wearing appropriate safety equipment, to physical force… (e.g., pounding with a hammer…) that will disfigure, bend, mangle, or otherwise mutilate the hard drive so that it cannot be reinserted into a functioning computer. Sufficient force should be used directly on top of the hard drive unit to cause shock/damage to the disk surfaces. In addition, any connectors that interface into the computer must be mangled, bent, or otherwise damaged to the point that the hard drive could not be reconnected without significant rework. [7]



[7] DOD Memorandum, 8 July, 2001. Subject: Destruction of DoD Computer Hard Drives Prior to Disposal.

Appendix E: Sources

- All About Degausser and Erasure of Magnetic Media. Athana International. 20 June 2005
- Anastasi, Joe. The New Forensics: Investigating Corporate Fraud and the Theft of Intellectual Property . N.p.: John Wiley and Sons, 2003. 1-288.
- Army Regulation 25–2. U.S Army. ELECTRONIC PUBLISHING SYSTEM, 17 Nov 2003.
- D.Millar, "Clean Out Old Computers Before Selling/Donating," June 1997;
- Davis, Harvey A. National Security Agency. NSA/CSS POLICY MANUAL 9-12. N.p.: n.p., 2000.
- "Degaussing Described." Weircliffe International Ltd in the interests of magnetic media users and others who are affected by the phenomena of Ferro-magnetism (2005).
- Dictionary definition of **EPROM**
  The American Heritage® Dictionary of the English Language, Fourth Edition Copyright © 2004, 2000 by Houghton Mifflin Company. Published by Houghton Mifflin Company.
- "Future of Computing (Optical & Biological Possibilities)." Future of Computing. 04 June 1997. Dept. of Engineering, Imperial College London. 10 Nov. 2005
- Garfinkel, Simson L., and Abhi Shelat. "Remembrance of Data Passed: A Study of Disk Sanitization Practices." IEEE Security & Privacy 1st ser. 1 (2003). 09 June 2005
- Gutmann, Peter, ed. Secure Deletion of Data from Magnetic and Solid-State Memory. San Jose: Sixth USENIX Security Symposium Proceedings, 1996.
- Gutmann, Peter, ed. Data Remanence in Semiconductor Devices. Washington, D.C: 10th USENIX SECURITY SYMPOSIUM, 2001.
- J.Hasson, "V.A. Toughens Security after PC Disposal Blunders," *Federal Computer Week,* 26 Aug. 2002;
- LeaseForum. "Understanding Data Storage, Data Liability and Current Data Removal Methodologies." Addressing Data at Asset Retirement. N.p.: n.p. 2002. 1-8.

- Magnetoresistive Random Access Memory (MRAM). Comp. James Daughton. 4 Feb. 2000. NVE. 17 June 2005

- Microsoft, "Microsoft Extensible Firmware Initiative FAT32 File System Specification," 6 Dec. 2000;
- National Computer Security Center, "A Guide to Understanding Data Remanence in Automated Information Systems,"
- Understand Degaussing. Peripheral Manufacturing Inc. 18 June 2005.
- US Department of Defense, "Cleaning and Sanitization Matrix," DOS 5220.22-M, Washington, D.C., 1995.

Appendix F: Sample Sanitization Validation Form

Organization: _____

Item Description: _____

Make/Model: _____

Serial Number(s)/Property Number(s):_____
_____
_____

Backup Made of Information: ☐ Yes
☐ No

If Yes, Backup Location: _____

Item Disposition: ☐ Clear
☐ Purge
☐ Destroy

Date Conducted: _____
Conducted By: _____
Phone #: _____
Validated By: _____
Phone #: _____

Sanitization Method Used: _____

Final Disposition of Media: ☐ Disposed
☐ Reused Internally
☐ Reused Externally
☐ Returned to Manufacturer
☐ Other: _____