NIST Special Publication 800-88
Revision 1

Guidelines for Media Sanitization

Richard Kissel
Andrew Regenscheid
Matthew Scholl
Kevin Stine

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

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

National Institute of
Standards and Technology
U.S. Department of Commerce

NIST Special Publication 800-88
Revision 1

Guidelines for Media Sanitization

Richard Kissel
Andrew Regenscheid
Matthew Scholl
Kevin Stine
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

December 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Willie May, Acting Under Secretary of Commerce for Standards and Technology and Acting Director

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 *et seq.*, Public Law 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), *Securing Agency Information Systems*, as analyzed in Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the 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. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-88 Revision 1
Natl. Inst. Stand. Technol. Spec. Publ. 800-88 Revision 1, 64 pages (December 2014)
CODEN: NSPUE2

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: 800-88r1comments@nist.gov

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 analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization of confidentiality of their information.

Keywords

media sanitization; ensuring confidentiality; sanitization tools and methods; media types; mobile devices with storage; crypto erase; secure erase

Acknowledgements

The authors would like to thank Steven Skolochenko and Xing Li for their contributions to the original version of this publication. The authors would also like to thank Jim Foti for his exceptional editing skills and thorough review of this document – his work made this a much better document. Kudos to each of the individuals and organizations who provided comments on this revision. It is a more accurate and usable document due to their contributions.

Executive Summary

The modern storage environment is rapidly evolving. Data may pass through multiple organizations, systems, and storage media in its lifetime. The pervasive nature of data propagation is only increasing as the Internet and data storage systems move towards a distributed cloud-based architecture. As a result, more parties than ever are responsible for effectively sanitizing media and the potential is substantial for sensitive data to be collected and retained on the media. This responsibility is not limited to those organizations that are the originators or final resting places of sensitive data, but also intermediaries who transiently store or process the information along the way. The efficient and effective management of information from inception through disposition is the responsibility of all those who have handled the data.

The application of sophisticated access controls and encryption help reduce the likelihood that an attacker can gain direct access to sensitive information. As a result, parties attempting to obtain sensitive information may seek to focus their efforts on alternative access means such as retrieving residual data on media that has left an organization without sufficient sanitization effort having been applied. Consequently, the application of effective sanitization techniques and tracking of storage media are critical aspects of ensuring that sensitive data is effectively protected by an organization against unauthorized disclosure. Protection of information is paramount. That information may be on paper, optical, electronic or magnetic media.

An organization may choose to dispose of media by charitable donation, internal or external transfer, or by recycling it in accordance with applicable laws and regulations if the media is obsolete or no longer usable. Even internal transfers require increased scrutiny, as legal and ethical obligations make it more important than ever to protect data such as Personally Identifiable Information (PII). No matter what the final intended destination of the media is, it is important that the organization ensure that no easily re-constructible residual representation of the data is stored on the media after it has left the control of the organization or is no longer going to be protected at the confidentiality categorization of the data stored on the media.

Sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This guide will assist organizations and system owners in making practical sanitization decisions based on the categorization 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.

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

1.1 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. 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*[1], 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 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*[2], 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.

---

[1] Federal Information Processing Standards (FIPS) Publication 199 *Standards for Security Categorization of Federal Information and Information Systems*, February 2004, 13 pp. http://csrc.nist.gov/publications/PubsFIPS.html#199.

[2] NIST Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (includes updates as of January 15, 2014), 460 pp. http://dx.doi.org/10.6028/NIST.SP.800-53r4.

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.

1.2 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.

1.3 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.[3] 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.

1.4 Relationship to Other NIST Documents

The following NIST documents, including FIPS and Special Publications, are directly related to this document:

- FIPS 199 and NIST SP 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*[4], provide 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.

[3] NIST SP 800-64 Revision 2, *Security Considerations in the Systems Development Life Cycle*, October 2008, 67 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-64.

[4] NIST SP 800-60 Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008, 2 vols. http://csrc.nist.gov/publications/PubsSPs.html#800-60.

- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*[5], sets a base of security requirements that requires organizations to have a media sanitization program.

- FIPS 140-2, *Security Requirements for Cryptographic Modules*[6], establishes a standard for cryptographic modules used by the U.S. Government.

- NIST SP 800-53 Revision 4 provides minimum recommended security controls, including sanitization, for Federal systems based on their overall system security categorization.

- NIST SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*[7], provides guidance for assessing security controls, including sanitization, for federal systems based on their overall system security categorization.

- NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*[8], provides guidance for selecting and using storage encryption technologies.

- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*[9], provides guidance for protecting the confidentiality of personally identifiable information in information systems.

1.5 Document Structure

The guide is divided into the following sections and appendices:

- **Section 1** (this section) explains the authority, purpose and scope, audience, assumptions of the document, relationships to other documents, and outlines its structure.

- **Section 2** presents an overview of the need for sanitization and the basic types of information, sanitization, and media.

---

[5] FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems,* March 2006, 17 pp. http://csrc.nist.gov/publications/PubsFIPS.html#200.

[6] FIPS 140-2, *Security Requirements for Cryptographic Modules*, May 25, 2001 (includes change notices through December 3, 2002), 69 pp. http://csrc.nist.gov/publications/PubsFIPS.html#140-2.

[7] NIST SP 800-53A Revision 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans*, June 2010, 399 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-53A.

[8] NIST SP 800-111, *Guide to Storage Encryption Technologies for End User Devices,* November 2007, 40 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-111.

[9] NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* April 2010, 59 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-122.

- **Section 3** provides an overview of relevant roles and responsibilities for the management of data throughout its lifecycle.
- **Section 4** provides the user with a process flow to assist with sanitization decision making.
- **Section 5** summarizes some general sanitization techniques.
- **Appendix A** specifies the minimum recommended sanitization techniques to Clear, Purge, or Destroy various media. This appendix is used with the decision flow chart provided in Section 4.
- **Appendix B** defines terms used in this guide.
- **Appendix C** lists tools and external resources that can assist with media sanitization.
- **Appendix D** contains considerations for selecting a storage device implementing Cryptographic Erase.
- **Appendix E** identifies a set of device-specific characteristics of interest that users should request from storage device vendors.
- **Appendix F** contains a bibliography of sources and correspondence that was essential in developing this guide.
- **Appendix G** provides a sample certificate of sanitization form for documenting an organization's sanitization activities.

2 Background

Information disposition and sanitization decisions occur throughout the information 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. Some storage devices support enhanced commands for sanitization, which may make sanitization easier, faster, and/or more effective. The decision may be even more fundamental, because effective sanitization procedures may not yet have been determined for emerging media types. Without an effective command or interface-based sanitization technique, the only option left may be to destroy the media. In that event, the media cannot be reused by other organizations that might otherwise have been able to benefit from receiving the repurposed storage device.

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.

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 defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…"[10] Additionally, "a loss of confidentiality is the unauthorized disclosure of information."[11]

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 hardware or software failures. This potential vulnerability can be mitigated through proper understanding of where information is located, what that information is, and how to protect it.

[10] "Definitions," Title 44 *U.S.Code*, Sec. 3542. 2006 ed. Supp. 5. Available: http://www.gpo.gov/; accessed 7/21/2014.

[11] FIPS 199, p.2.

2.2 Types of Media

There are two primary types of media in common use:

- **Hard Copy.** Hard copy media are physical representations of information, most often associated with paper printouts. However, printer and facsimile ribbons, drums, and platens are all examples of hard copy media. The supplies associated with producing paper printouts are often the most uncontrolled. Hard copy materials containing sensitive data that leave an organization without effective sanitization expose a significant vulnerability to "dumpster divers" and overcurious employees, risking unwanted information disclosures.

- **Electronic (i.e., "soft copy").** Electronic media are devices containing bits and bytes such as hard drives, random access memory (RAM), read-only memory (ROM), disks, flash memory, memory devices, phones, mobile computing devices, networking devices, office 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 that could possibly have been recorded on the media, rather than on the media itself.

2.3 Trends in Data Storage Media

Historical efforts to sanitize magnetic media have benefitted from the wide use of a single common type of storage medium implemented relatively similarly across vendors and models. The storage capacity of magnetic media has increased at a relatively constant rate and vendors have modified the technology as necessary to achieve higher capacities. As the technology approaches the superparamagnetic limit, or the limit at which magnetic state can be changed with existing media and recording approaches, additional new approaches and technologies will be necessary in order for storage vendors to produce higher capacity devices.

Alternative technologies such as flash memory-based storage devices, or Solid State Drives (SSDs), have also become prevalent due to falling costs, higher performance, and shock resistance. SSDs have already begun changing the norm in storage technology, and—at least from a sanitization perspective—the change is revolutionary (as opposed to evolutionary). Degaussing, a fundamental way to sanitize magnetic media, no longer applies in most cases for flash memory-based devices. Evolutionary changes in magnetic media will also have potential impacts on sanitization. New storage technologies, and even variations of magnetic storage, that are dramatically different from legacy magnetic media will clearly require sanitization research and require a reinvestigation of sanitization procedures to ensure efficacy.

Both revolutionary and evolutionary changes make sanitization decisions more difficult, as the storage device may not clearly indicate what type of media is used for data storage. The burden falls on the user to accurately determine the media type and apply the associated sanitization procedure.

2.4 Trends in Sanitization

For storage devices containing *magnetic* media, a single overwrite pass with a fixed pattern such as binary zeros typically hinders recovery of data even if state of the art laboratory techniques are applied to attempt to retrieve the data. One major drawback of relying solely upon the native Read and Write interface for performing the overwrite procedure is that areas not currently mapped to active Logical Block Addressing (LBA) addresses (e.g., defect areas and currently unallocated space) are not addressed. Dedicated sanitize commands support addressing these areas more effectively. The use of such commands results in a tradeoff because although they should more thoroughly address all areas of the media, using these commands also requires trust and assurance from the vendor that the commands have been implemented as expected.

Users who have become accustomed to relying upon overwrite techniques on magnetic media and who have continued to apply these techniques as media types evolved (such as to flash memory-based devices) may be exposing their data to increased risk of unintentional disclosure. Although the host interface (e.g. Advanced Technology Attachment (ATA) or Small Computer System Interface (SCSI)) may be the same (or very similar) across devices with varying underlying media types, it is critical that the sanitization techniques are carefully matched to the media.

Destructive techniques for some media types may become more difficult or impossible to apply in the future. Traditional techniques such as degaussing (for magnetic media) become more complicated as magnetic media evolves, because some emerging variations of magnetic recording technologies incorporate media with higher coercivity (magnetic force). As a result, existing degaussers may not have sufficient force to effectively degauss such media.

Applying destructive techniques to electronic storage media (e.g., flash memory) is also becoming more challenging, as the necessary particle size for commonly applied grinding techniques goes down proportionally to any increases in flash memory storage density. Flash memory chips already present challenges with occasional damage to grinders due to the hardness of the component materials, and this problem will get worse as grinders attempt to grind the chips into even smaller pieces.

Cryptographic Erase (CE), as described in Section 2.6, is an emerging sanitization technique that can be used in some situations when data is encrypted as it is stored on media. With CE, media sanitization is performed by sanitizing the cryptographic keys used to encrypt the data, as opposed to sanitizing the storage locations on media containing the encrypted data itself. CE techniques are typically capable of sanitizing media very quickly and could support partial sanitization, a technique where a subset of storage media is sanitization. Partial sanitization, sometimes referred to as selective sanitization, has potential applications in cloud computing and mobile devices. However, operational use of CE today presents some challenges. In some cases, it may be difficult to verify that CE has effectively sanitized media. This challenge, and possible approaches, is described in Section 4.7.3. If verification cannot be performed, organizations should use alternative sanitization methods that can be verified, or use CE in combination with a sanitization technique that can be verified.

A list of device-specific characteristics of interest for the application of sanitization techniques is

included in Appendix E. These characteristics can be used to drive the types of questions that media users should ask vendors, but ideally this information would be made readily available by vendors so that it can be easily retrieved by users to facilitate informed risk based sanitization decisions. For example, knowing the coercivity of the media can help a user decide whether or not the available degausser(s) can effectively degauss the media.

2.5 Types of Sanitization

Regarding sanitization, the principal concern is ensuring that data is not unintentionally released. Data is stored on media, which is connected to a system. This guidance focuses on the media sanitization component, which is simply data sanitization applied to a representation of the data as stored on a specific media type. Other potential concern areas exist as part of the system, such as for monitors, which may have sensitive data burned into the screen. Sensitive data stored in areas of the system other than storage media (such as on monitor screens) are not addressed by this document.

When media is repurposed or reaches end of life, the organization executes the system life cycle sanitization decision for the information on the media. For example, a mass-produced commercial software program contained on a DVD in an unopened package is unlikely to contain confidential data. Therefore, the decision may be made to simply dispose of the media without applying any sanitization technique. Alternatively, an organization is substantially more likely to decide that a hard drive from a system that processed PII needs sanitization prior to Disposal.

Disposal without sanitization should be considered only if information disclosure would have no impact on organizational mission, would not result in damage to organizational assets, and would not result in financial loss or harm to any individuals.

The security categorization of the information, along with internal environmental factors, should drive the decisions on how to deal with the media. The key is to first think in terms of information confidentiality, then apply considerations based on 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 confidentiality levels and associate a type of sanitization described in this publication.

Sanitization is a process to render access to target data (the data subject to the sanitization technique) on the media infeasible for a given level of recovery effort. The level of effort applied when attempting to retrieve data may range widely. For example, a party may attempt simple keyboard attacks without the use of specialized tools, skills, or knowledge of the media characteristics. On the other end of the spectrum, a party may have extensive capabilities and be able to apply state of the art laboratory techniques.

Clear, Purge, and Destroy are actions that can be taken to sanitize media. The categories of sanitization are defined as follows:

- **Clear** applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).

- **Purge** applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.

- **Destroy** renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.

A more detailed summary of sanitization techniques is provided in Section 5. Sanitization requirements for specific media/device types are provided in Appendix A.

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, the organization can choose the appropriate type(s) of sanitization. The selected type(s) should be assessed as to cost, environmental impact, etc., and a decision should be made that best mitigates the risk to confidentiality and best satisfies other constraints imposed on the process.

2.6 Use of Cryptography and Cryptographic Erase

Many storage manufacturers have released storage devices with integrated encryption and access control capabilities, also known as Self-Encrypting Drives (SEDs). SEDs feature always-on encryption that substantially reduces the likelihood that unencrypted data is inadvertently retained on the device. The end user cannot turn off the encryption capabilitieswhich ensures that all data in the designated areas are encrypted. A significant additional benefit of SEDs is the opportunity to tightly couple the controller and storage media so that the device can directly address the location where any cryptographic keys are stored, whereas solutions that depend only on the abstracted user access interface through software may not be able to directly address those areas.

SEDs typically encrypt all of the user-addressable area, with the potential exception of certain clearly identified areas, such as those dedicated to the storage of pre-boot applications and associated data.

Cryptographic Erase (CE) leverages the encryption of target data by enabling sanitization of the target data’s encryption key. This leaves only the ciphertext remaining on the media, effectively sanitizing the data by preventing read-access.

Without the encryption key used to encrypt the target data, the data is unrecoverable. The level of effort needed to decrypt this information without the encryption key then is the lesser of the

strength of the cryptographic key or the strength of the cryptographic algorithm and mode of operation used to encrypt the data.

If strong cryptography is used, sanitization of the target data is reduced to sanitization of the encryption key(s) used to encrypt the target data. Thus, with CE, sanitization may be performed with high assurance much faster than with other sanitization techniques. The encryption itself acts to sanitize the data, subject to constraints identified in this guidelines document. Federal agencies must use FIPS 140 validated encryption modules[12] in order to have assurance that the conditions stated above have been verified for the SED.

Typically, CE can be executed in a fraction of a second. This is especially important as storage devices get larger resulting in other sanitization methods take more time. CE can also be used as a supplement or addition to other sanitization approaches.

2.6.1 When Not To Use CE To Purge Media

- Do not use CE to purge media if the encryption was enabled after sensitive data was stored on the device without having been sanitized first.
- Do not use CE if it is unknown whether sensitive data was stored on the device without being sanitized prior to encryption.

2.6.2 When to Consider Using CE

- Consider using CE when all data intended for CE is encrypted prior to storage on the media (including the data, as well as virtualized copies).
- Consider using CE when we know the location(s) on the media where the encryption key is stored (be it the target data's encryption key or an associated wrapping key) and can sanitize those areas using the appropriate media-specific sanitization technique, ensuring the actual location on media where the key is stored is addressed.
- Consider using CE when we can know that all copies of the encryption keys used to encrypt the target data are sanitized
- Consider using CE when the target data's encryption keys are, themselves, encrypted with one or more wrapping keys and we are confident that we can sanitize the corresponding wrapping keys.
- Consider using CE when we are confident of the ability of the user to clearly identifyand use the commands provided by the device to perform the CE operation.

[12] NIST maintains lists of validated cryptographic modules (http://csrc.nist.gov/groups/STM/cmvp/validation.html) and cryptographic algorithms (http://csrc.nist.gov/groups/STM/cavp/validation.html).

2.6.3 Additional CE Considerations

If the encryption key exists outside of the storage device (typically due to backup or escrow), there is a possibility that the key could be used in the future to recover data stored on the encrypted media.

CE should only be used as a sanitization method when the organization has confidence that the encryption keys used to encrypt the Target Data have been appropriately protected. Such assurances can be difficult to obtain with software cryptographic modules, such as those used with software-based full disk encryption solutions, as these products typically store cryptographic keys in the file system or other locations on media which are accessible to software. While there may be situations where use of CE with software cryptographic modules is both appropriate and advantageous, such as performing a quick remote wipe on a lost mobile device, unless the organization has confidence in both the protection of the encryption keys, and the destruction of all copies of those keys in the sanitization process, CE should be used in combination with another appropriate sanitization method.

Sanitization using CE should not be trusted on devices that have been backed-up or escrowed the key(s) unless the organization has a high level of confidence about how and where the keys were stored and managed outside the device. Such back-up or escrowed copies of data, credentials, or keys should be the subject of a separate device sanitization policy. That policy should address backups or escrowed copies within the scope of the devices on which they are actually stored.

A list of applicable considerations, and a sample for how vendors could report the mechanisms implemented, is included in Appendix E. Users seeking to implement CE should seek reasonable assurance from the vendor (such as the vendor's report as described in Appendix E) that the considerations identified here have been addressed and only use FIPS 140 validated cryptographic modules.

2.7 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 tradeoff of a 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 verification, etc.) to destroy media rather than use one of the other options. Organizations retain the ability increase the level of sanitization applied if that is reasonable and indicated by an assessment of the existing risk.

Organizations should consider environmental factors including (but not limited to):

- 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 requirement for 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? [13]
- 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 is the cost of sanitization when considering tools, training, verification, and re-entering media into the supply stream?

2.8 Sanitization Scope

For most sanitization operations, the target of the operation is all data stored on the media by the user. However, in some cases, there may be a desire or need to sanitize a subset of the media. Partial sanitization comes with some risk, as it may be difficult to verify that sensitive data stored on a portion of the media did not spill over into other areas of the media (e.g., remapped bad blocks). In addition, the dedicated interfaces provided by storage device vendors for sanitization typically operate at the device level, and are not able to be applied to a subset of the media. As a result, partial sanitization usually depends on the typical read and write commands available to the user, which may not be able to bypass any interface abstraction that may be present in order to directly address the media area of concern.

On some storage devices featuring integrated encryption capabilities, CE provides a unique mechanism for supporting some forms of partial sanitization. Some of these devices support the ability to encrypt portions of the data with different encryption keys (e.g., encrypting different partitions with different encryption keys). When the interface supports sanitizing only a subset of the encryption keys, partial sanitization via CE is possible. As with any other sanitization technique applied to media, the level of assurance depends both upon vendor implementation and on the level of assurance that data was stored only in the areas that are able to be reliably sanitized. Data may be stored outside these regions either because the user or software on the system moved data outside of the designated area on the media, or because the storage device stored data to the media in a manner not fully understood by the user.

Due to the difficulty in reliably ensuring that partial sanitization effectively addresses all sensitive data, sanitization of the whole device is preferred to partial sanitization whenever possible. Organizations should understand the potential risks to this approach and make appropriate decisions on this technique balancing the factors described earlier in this sectionas

[13] NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, October 2003, 67 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-36.

well as their business missions and specific use cases. For example, a drive in a datacenter may contain customer data from multiple customers. When one customer discontinues service and another begins storing data on the same media, the organization may choose to apply partial sanitization in order to retain the data of other customers that is also stored on the same storage device on other areas of the media. The organization may choose to apply partial sanitization because the drive remains in the physical possession of the organization, access by the customer is limited to the interface commands, and the organization has trust in the partial sanitization mechanism available for that specific piece of media. In cases where the alternative to partial sanitization is not performing sanitization at all, partial sanitization provides benefits that should be considered.

3 Roles and Responsibilities

3.1 Program Managers/Agency Heads

"Ultimately, responsibility for the success of an organization lies with its senior managers."[14] 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.

The other responsibilities in the remainder of this section are for illustrative purposes and the intent is to ensure that organizations think through the different responsibilities for sanitizing media and assign those responsibilities appropriately.

3.2 Chief Information Officer (CIO)

The CIO[15] 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[16] 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/Steward

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 they fully understand the sensitivity of the information under their control and that the users of the information are aware of its confidentiality and the basic requirements for media sanitization.

---

[14]NIST SP 800-18 Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006, 16. http://csrc.nist.gov/publications/PubsSPs.html#800-18.

[15]Per the Information Technology Management Reform Act of 1996 ("Clinger-Cohen Act"; P.L. 104-106 (Division E) 10 Feb. 1996), when an agency has not designated a formal CIO position, FISMA requires the associated responsibilities to be handled by a comparable agency official.

[16]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. The SAISO also requires access to the technical basis/personnel to understand and properly implement the sanitization procedures.

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

An organization may maintain storage devices with differing levels of confidentiality, and it is important to understand what types of data may be stored on the device in order to apply the techniques that best balance efficiency and efficacy to maintain the confidentiality of the data. Data confidentiality level should be identified using procedures described in FIPS 199. Additional information is available on mapping information types to security categories in SP 800-60 Revision 1.

While most devices support some form of Clear, not all devices have a reliable Purge mechanism. For moderate confidentiality data, the media owner may choose to accept the risk of applying Clear techniques to the media, acknowledging that some data may be able to be retrieved by someone with the time, knowledge, and skills to do so.

Purge (and Clear, where applicable) may be more appropriate than Destroy when factoring in environmental concerns, the desire to reuse the media (either within the organization or by selling or donating the media), the cost of a media or media device, or difficulties in physically Destroying some types of media.

The risk decision should include the potential consequence of disclosure of information retrievable from the media, the cost of information retrieval and its efficacy, and the cost of sanitization and its efficacy. Additionally, the length of time the data will remain sensitive should also be considered. These values may vary between different environments.

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.

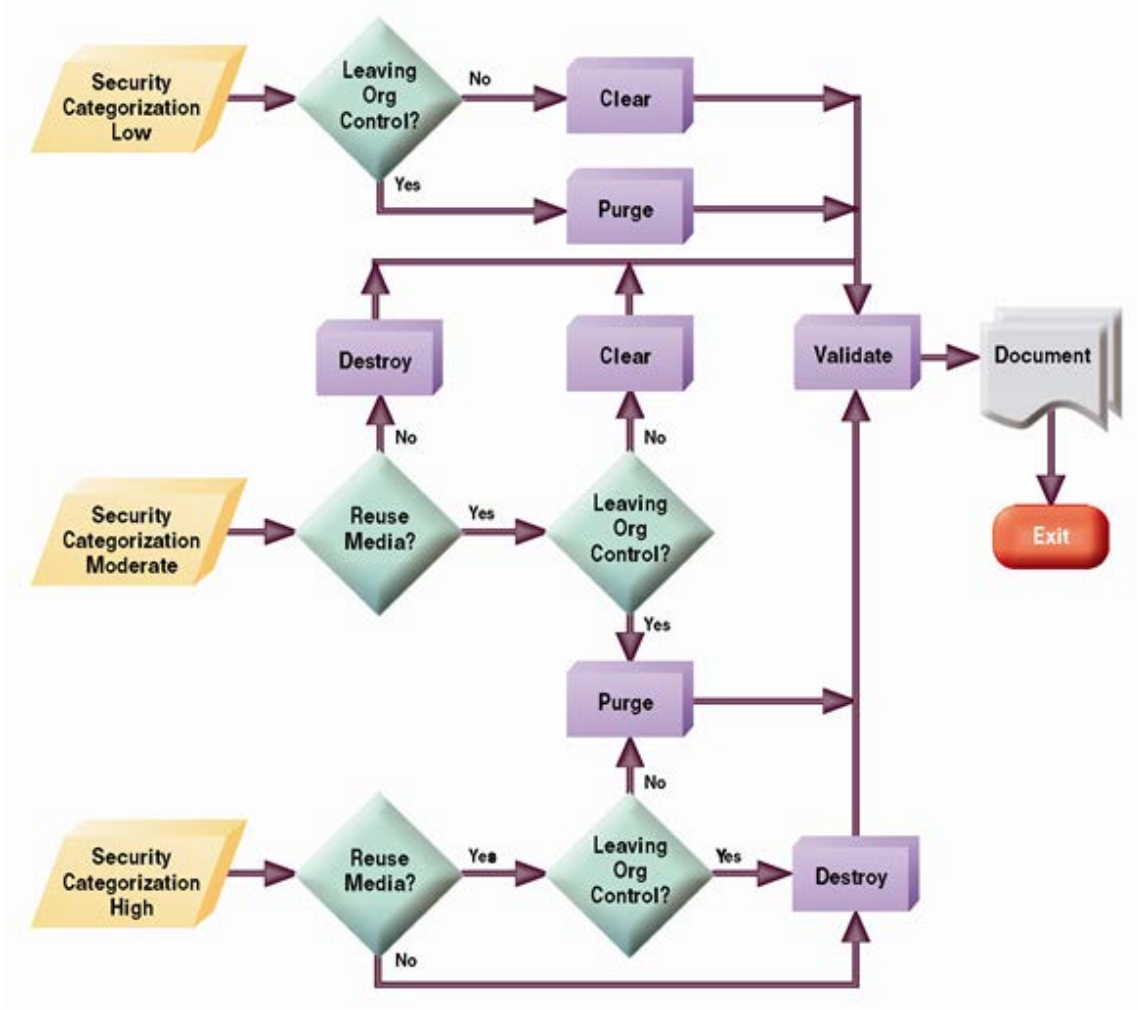

Figure 4-1: Sanitization and Disposition Decision Flow

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 Disposal phase in the system life cycle. At the start of system development, when the initial system security plan is developed[17], 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 within the system. Although this is

[17] NIST SP 800-18 Revision 1, p.19.

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.

An organization may ask a product vendor for assistance in identifying storage media that may contain sensitive data. This information is typically documented in a 'statement of volatility'. The statement may be used to support decisions about which equipment to purchase, based on the ease or difficulty of sanitization. While volatility statements are useful, caution should be applied in comparing statements across vendors because vendors may state volatility details differently.

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 desktop computer may contain a hard drive, motherboard, RAM, and ROM, and mobile devices contain on-board volatile memory as well as nonvolatile removable memory.

The increasing availability of rapidly applicable techniques, such as Cryptographic Erase, provides opportunities for organizations to reduce the risk of inadvertent disclosure by combining sanitization technologies and techniques. For example, an organization could choose to apply Cryptographic Erase at a user's desktop before removing the media to send it to be 'formally' sanitized at the sanitization facility, in order to reduce risk and exposure.

4.2 Determination of Security Categorization

Early in the system life cycle, a system is categorized using the guidance found in FIPS 199, NIST SP 800-60 Rev. 1, or CNSSI 1253[18], including the security categorization for the system's confidentiality. This security categorization is revisited at least every three years (or when significant change occurs within the system) 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 confidentiality levels and associate a type of sanitization described in this publication.

4.3 Reuse of Media

A key decision on sanitization is whether the media are planned for reuse or recycle. Some forms of media are often 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 Destroy.

[18] Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, March 27, 2014. https://www.cnss.gov/CNSS/issuances/Instructions.cfm.

4.4 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 (External 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.

4.5 Data Protection Level

Even within an organization, varying data protection policies may be established. For instance, a company may have an engineering department and a sales department. The sales personnel may not have a need for access to the detailed proprietary technical data such as source code and schematics, and the engineers may not have a need to access the PII of the company's customers. Both might be within the same confidentiality categorization, but contextually different and with different internal and external rules regarding necessary controls. As such, data protection level is a complementary consideration to organizational control. When identifying whether sanitization is necessary, both the organizational control and data protection level should be considered.

4.6 Sanitization and Disposal Decision

Once an organization completes an assessment of its system confidentiality, determines the need for information sanitization, determines appropriate time frames for sanitization, and determines 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 record 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 verification: capturing 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. Two types of verification should be considered. The first is verification every time sanitization is applied (where applicable, as most Destroy techniques do not support practical verification for each sanitized piece of media). The second is a representative sampling verification, applied to a selected subset of the media. If possible, the sampling should be executed by personnel who were not part of the original sanitization action. If sampling is done after full verification in cases of low risk tolerance then a different verification tool than the one used in the original verification should be used.

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 or a dedicated workstation), then equipment calibration, as well as equipment testing, and scheduled maintenance, is also needed.

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.

4.7.3 Verification of Sanitization Results

The goal of sanitization verification is to ensure that the target data was effectively sanitized. When supported by the device interface (such as an ATA or SCSI storage device or solid state drive), the highest level of assurance of effective sanitization (outside of a laboratory) is typically achieved by a full reading of all accessible areas to verify that the expected sanitized value is in all addressable locations. A full verification should be performed if time and external factors permit. This manner of verification typically only applies where the device is in an operational state following sanitization so that data can be read and written through the native interface.

If an organization chooses representative sampling then there are three main goals applied to electronic media sanitization verification:

1. Select pseudorandom locations on the media each time the analysis tool is applied. This reduces the likelihood that a sanitization tool that only sanitizes a subset of the media will result in verification success in a situation where sensitive data still remains.

2. Select locations across the addressable space (user addressable and reserved areas). For instance, conceptually break the media up into equally sized subsections. Select a large enough number of subsections so that the media is well-covered. The number of practical subsections depends on the device and addressing scheme. The suggested minimum number of subsections for a storage device leveraging LBA

addressing is one thousand. Select at least two non-overlapping pseudorandom locations from within each subsection. For example, if one thousand conceptual subsections are chosen, at least two pseudorandom locations in the first thousandth of the media addressing space would be read and verified, at least two pseudorandom locations in the second thousandth of the media addressing space would be read and verified, and so on.

   a. In addition to the locations already identified, include the first and last addressable location on the storage device.

3. Each consecutive sample location (except the ones for the first and last addressable location) should cover at least 5 % of the subsection and not overlap the other sample in the subsection. Given two non-overlapping samples, the resulting verification should cover at least 10 % of the media once all subsections have had two samples taken.

Cryptographic Erase has different verification considerations than procedures such as rewriting or block erasing, because the contents of the physical media following Cryptographic Erase may not be known and therefore cannot be compared to a given value. When Cryptographic Erase is leveraged, there are multiple options for verification, and each uses a quick review of a subset of the media. Each involves a selection of pseudorandom locations to be sampled from across the media.

The first option is to read the pseudorandom locations prior to Cryptographic Erase, and then again following Cryptographic Erase to compare the results. This is likely the most effective verification technique. Another option is to search for strings across the media or looking for files that are in known locations, such as operating system files likely to be stored in a specific area.

The number of locations and size of each sample should take into consideration the risks in transferring the Target Data to the storage media of the machine hosting the sanitization application. As a result, the proportion of the media covered by verification for the Cryptographic Erase technique may be relatively small (or at least lower than the above guidance of 10 % for verification of non-cryptographic sanitization techniques), but should still be applied across a wide range of the addressable area.

However, these techniques may not always be available because the individual performing the sanitization may not have the authentication token needed to access and read the data stored on the drive. If an organization cannot verify that CE effectively sanitized storage media, organizations should employ an alternative sanitization method that can be verified, either in combination with CE or in place of CE.

As part of the sanitization process, in addition to the verification performed on each piece of media following the sanitization operation, a subset of media items should be selected at random for secondary verification using a different verification tool. The secondary verification tool should be from a separate developer. For the secondary verification, a full verification should be performed. At least 20 % of sanitized media (by number of media

items sanitized) should be verified. The secondary verification provides assurance that the primary operation is working as expected.

4.8 Documentation

Following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized. A certification of media disposition may be a piece of paper or an electronic record of the action taken. For example, most modern hard drives include bar codes on the label for values such as model and serial numbers. The person performing the sanitization might simply enter the details into a tracking application and scan each bar code as the media is sanitized. Automatic documentation can be important as some systems make physical access to the media very difficult.

The decision regarding whether to complete a certificate of media disposition and how much data to record depends on the confidentiality level of the data on the media. For a large number of devices with data of very low confidentiality, an organization may choose not to complete the certificate.

When fully completed, the certificate should record at least the following details:

- Manufacturer
- Model
- Serial Number
- Organizationally Assigned Media or Property Number (if applicable)
- Media Type (i.e., magnetic, flash memory, hybrid, etc.)
- Media Source (i.e., user or computer the media came from)
- Pre-Sanitization Confidentiality Categorization (optional)
- Sanitization Description (i.e., Clear, Purge, Destroy)
- Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.)
- Tool Used (including version)
- Verification Method (i.e., full, quick sampling, etc.)
- Post-Sanitization Confidentiality Categorization (optional)
- Post-Sanitization Destination (if known)
- For Both Sanitization and Verification:
    - Name of Person

- Position/Title of Person
- Date
- Location
- Phone or Other Contact Information
- Signature

Optionally, an organization may choose to record the following (if known):

- Data Backup (i.e., if data was backed up, and if so, where)

A sample certificate is included in Appendix G.

If the storage device has been successfully verified and the sanitization results in a lower confidentiality level of the storage device, all markings on the device indicating the previous confidentiality level should be removed. A new marking indicating the updated confidentiality level should be applied, unless the device is leaving the organization and is stored in a location where access is carefully controlled until the device leaves the organization to prevent reintroduction of sensitive data.

The value of a certification of media disposition depends on the organization's handling of storage media over the media's lifecycle. If records are maintained when the media is introduced to the environment, when the media leaves the place it was last used, and when it reaches the sanitization destination, the organization can most effectively identify how well media sanitization is being applied across the enterprise. If there is a breakdown in tracking at locations other than the sanitization destination, the sanitization records only show that specific media was sanitized and not whether the organization is effectively sanitizing all media that has been introduced into the operating environment.

5 Summary of Sanitization Methods

Several different methods can be used to sanitize media. Four 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 user-addressable storage space on the media with non-sensitive data, using the standard read and write commands for the device. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also should include all user-addressable locations. The security goal of the overwriting process is to replace Target Data with non-sensitive data. Overwriting cannot be used for media that are damaged or not rewriteable, and may not address all areas of the device where sensitive data may be retained. The media type and size may also influence whether overwriting is a suitable sanitization method. For example, flash memory-based storage devices may contain spare cells and perform wear levelling, making it infeasible for a user to sanitize all previous data using this approach because the device may not support directly addressing all areas where sensitive data has been stored using the native read and write interface. The Clear operation may vary contextually for media other than dedicated storage devices, where the device (such as a basic cell phone or a piece of office equipment) only provides the ability to return the device to factory state (typically by simply deleting the file pointers) and does not directly support the ability to rewrite or apply media-specific techniques to the non-volatile storage contents. Where rewriting is not supported, manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device and associated media. These still meet the definition for Clear as long as the device interface available to the user does not facilitate retrieval of the Cleared data.
Purge	Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwrite, block erase, and Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands. Destructive techniques also render the device Purged when effectively applied to the appropriate media type, including incineration, shredding, disintegrating, degaussing, and pulverizing. The common benefit across all these approaches is assurance that the data is infeasible to recover using state of the art laboratory techniques. However, Bending, Cutting, and the use of some emergency procedures (such as using a firearm to shoot a hole through a storage device) may only damage the media as portions of the media may remain undamaged and therefore accessible using advanced laboratory techniques. Degaussing renders a Legacy Magnetic Device Purged when the strength of the degausser is carefully matched to the media coercivity. Coercivity may be difficult to determine based only on information provided on the label. Therefore, refer to the device manufacturer for coercivity details. Degaussing should never be solely relied upon for flash memory-based storage devices or for magnetic storage devices that also contain non-volatile non-magnetic storage. Degaussing

Method	Description
	renders many types of devices unusable (and in those cases, Degaussing is also a Destruction technique).
Destroy	There are many different types, techniques, and procedures for media Destruction. While some techniques may render the Target Data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the device is not considered Destroyed unless Target Data retrieval is infeasible using state of the art laboratory techniques. • *Disintegrate, Pulverize, Melt, and Incinerate*. 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. • *Shred*. 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. To make reconstructing the data even more difficult, the shredded material can be mixed with non-sensitive material of the same type (e.g., shredded paper or shredded flexible media). The application of Destructive techniques may be the only option when the media fails and other Clear or Purge techniques cannot be effectively applied to the media, or when the verification of Clear or Purge methods fails (for known or unknown reasons).

Appendix A—Minimum Sanitization Recommendations

Once a decision is made based on factors such as those described in Section 4, and after applying relevant organizational environmental factors, then the tables in this Appendix can be used to determine recommended sanitization of specific media. That recommendation should reflect the 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 the tables in this Appendix is recommended here, other methods exist to satisfy the intent of Clear, Purge, and Destroy. Methods not specified in this table may be suitable as long as they are verified 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 tested, they are strongly encouraged to share this information through public forums, such as the Federal Agency Security Practices (FASP) website[19]. 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.

The proper initial configuration of each type of device helps ensure that the sanitization operation is as effective as possible. While called out for some specific items below, users are encouraged to check manufacturer recommendations and guides such as the DISA Security Technical Implementation Guides (STIGs)[20] for additional information about recommended settings for any other items in this list as well.

If a mobile device has nonvolatile removable memory, it may contain additional information that may or may not be addressed by the sanitization process identified in Table A-3. Contact the manufacturer and/or cellular provider to determine what types of data are stored on the removable memory and identify whether any additional sanitization is required for the removable memory. Additional details about such removable memory and associated data recovery capabilities are available in NIST SP 800-101 Revision 1[21]. If a mobile device does not have sufficient built-in sanitization appropriate for the sensitivity or impact level of the data it contains, then rather than destroy the device (to protect the information) consider contacting businesses providing sanitization services to determine if their services meet your needs.

Many internal storage devices (as opposed to removable media, such as an SD card) as well as storage subsystems that incorporate installed media, support dedicated sanitize commands. The

[19] http://csrc.nist.gov/groups/SMA/fasp/

[20] http://iase.disa.mil/stigs/

[21] NIST SP 800-101 Revision 1, *Guidelines on Mobile Device Forensics*, May 2014, 87 pp. http://dx.doi.org/10.6028/NIST.SP.800-101r1.

availability of these commands is impacted in some cases by system (i.e., BIOS/UEFI—Basic Input-Output System/Unified Extensible Firmware Interface) characteristics, such as how and when freeze lock commands are issued to a device. The use of a dedicated computer or equipment to perform sanitization that facilitates leveraging these commands (such as a PC or workstation, with an external drive bay that facilitates safely connecting a drive after the system has been powered on) can help address this issue. The behavior and methods to bypass freeze lock or other limitations on command availability vary between computers, so refer to the computer manufacturer for details about the behavior of specific models. Alternative approaches exist for addressing the issue, and will vary depending on the hardware, software, and firmware of the computer. University of California San Diego (UCSD)'s Center for Magnetic Recording Research (CMRR) has also developed some tools and documentation about work-arounds for this issue (see Appendix C for details).

Some sanitization procedures feature additional optional methods. The choice regarding whether to apply the optional components depends on the level of confidentiality of the data and assurance of correct implementation of the non-optional portion of the sanitization procedure. For example, an organization might decide that for PII, for example, that any method applied with an available optional component should execute that optional component. The choice may also be based on the time factor, as some procedures, including the optional method, can be executed in a total of a matter of minutes. In that case, the organization might decide to include the optional component even if the data is not in a higher confidentiality category.

Table A-1: Hard Copy Storage Sanitization

Hard Copy Storage	
Paper and microforms	
Clear:	N/A, see Destroy.
Purge:	N/A, see Destroy
Destroy:	Destroy paper using cross cut shredders which produce particles that are 1 mm x 5 mm (0.04 in. x 0.2 in.) in size (or smaller), or pulverize/disintegrate paper materials using disintegrator devices equipped with a 3/32 in. (2.4 mm) security screen. Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning.
Notes:	When material is burned, residue must be reduced to white ash.

Table A-2: Networking Device Sanitization

Networking Devices	
Routers and Switches (home, home office, enterprise)	
Clear:	Perform a full manufacturer's reset to reset the router or switch back to its factory default settings.

Purge:	See Destroy. Most routers and switches only offer capabilities to Clear (and not Purge) the data contents. A router or switch may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	For both Clear and (if applicable) Purge, refer to the manufacturer for additional information on the proper Sanitization procedure. Network Devices may contain removable storage. The removable media must be removed and sanitized using media-specific techniques.

Table A-3: Mobile Device Sanitization

Mobile Devices **(If a device has removable storage – first check for encryption and unencrypt if so – then remove the removable storage prior to sanitization)**	
Apple iPhone and iPad (current generation and future iPhones and iPads)	
Clear:	Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu). (The sanitization operation should take only minutes as Cryptographic Erase is supported. This assumes that encryption is on and that all data has been encrypted.) Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu). (The sanitization operation should take only minutes with Cryptographic Erase being supported. This assumes that encryption is on and that all data has been encrypted.)
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Before sanitizing the device, ensure that the data is backed up to a safe place. Current iPhones have hardware encryption – turned on by default.
Blackberry	**(back up data on device before sanitization)**
Clear:	BB OS 7.x/6.x - Select Options > Security Options > Security Wipe , making sure to select all subcategories of data types for sanitization. Then type "blackberry" in the text field, then click on "Wipe" ("Wipe Data" in BB OS 6.x) BB OS 10.x (Decrypt media card before continuing) Select Settings, Security and Privacy, Security Wipe . Type "blackberry" in the text field, then click on "Delete Data". The sanitization operation may take as long as several hours depending on the media size. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	BB OS 7.x/6.x - Select Options > Security > Security Wipe, then make sure to select all subcategories of data types for sanitization. Then type "blackberry" in the text field, then click on "Wipe" ("Wipe Data" in BB OS 6.x). For BB OS 10.x Select Settings> Security and Privacy>Security Wipe. Type "blackberry" in the text field, then click on "Delete Data". The

	sanitization operation may take as long as several hours depending on the media size.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Centralized management (BES) allows for device encryption. Refer to the manufacturer for additional information on the proper sanitization procedure, and for details about implementation differences between device versions and OS versions. Proper initial configuration using guides such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible. If the device contains removable storage media, ensure that the media is sanitized using appropriate media-dependent procedures.
Devices running the Google Android OS (connect to power before starting encryption)	
Clear:	Perform a factory reset through the device's settings menu. For example, on Samsung Galaxy S5 running Android 4.4.2, select settings, then, under User and Backup, select Backup and reset, then select Factory data reset. For other versions of Android and other mobile phone devices, refer to the user manual. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	The capabilities of Android devices are determined by device manufacturers and service providers. As such, the level of assurance provided by the factory data reset option may depend on architectural and implementation details of a particular device. Devices seeking to use a factory data reset to purge media should use the eMMC Secure Erase or Secure Trim command, or some other equivalent method (which may depend on the device's storage media). Some versions of Android support encryption, and may support Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a Purge capability that applies media-dependent sanitization techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Proper initial configuration using guides such as the DISA STIGs (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible. Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. When in doubt, check device manual or call tech support. For both Clear and Purge, refer to the manufacturer for additional information on the proper sanitization procedure.
Windows Phone OS 7.1/8/8.x (Centralized management may be needed for encryption)	
Clear:	Select the Settings option (little gear symbol) from the live tile or from the app list. On the "Settings" page, scroll to the bottom of the page and select the "About" button. In the about page, there will be a **reset your phone** button at the bottom of the page. Click on this button to continue. Choose Yes when you see the warning messages. Please note that after the process is completed, all your personal content will disappear. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	The capabilities of Windows Phone devices are determined by device manufacturers and service providers. As such, the level of assurance provided by the factory data reset

	option may depend on architectural and implementation details of a particular device. Devices seeking to use a factory data reset to purge media should use the eMMC Secure Erase or Secure Trim command, or some other equivalent method (which may depend on the device's storage media). In some environments, Windows Phone devices may support encryption, and may support Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a Purge capability that applies media-dependent sanitization techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Before sanitizing your device, ensure that you back up your data to a safe location. Refer to the manufacturer for proper sanitization procedure, and for details about implementation differences between device versions and OS versions. Proper initial configuration using guides such as the DISA STIGs (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible.
All other mobile devices *This includes cell phones, smart phones, PDAs, tablets, and other devices not covered in the preceding mobile categories.*	
Clear:	Manually delete all information, then perform a full manufacturer's reset to reset the mobile device to factory state. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.
Purge:	See Destroy. Many mobile devices only offer capabilities to Clear (and not Purge) the data contents. A mobile device may offer Purge capabilities, but these capabilities are specific to the hardware and software of the device and should be applied with caution. The device manufacturer should be referred to in order to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as call history, browser history, files, photos, etc.) to verify that no personal information has been retained on the device. For both Clear and (if applicable) Purge, refer to the manufacturer for proper sanitization procedure.

Table A-4: Equipment Sanitization

Equipment
Office Equipment *This includes copy, print, fax, and multifunction machines*

Clear:	Perform a full manufacturer's reset to reset the office equipment to its factory default settings.
Purge:	See Destroy. Most office equipment only offers capabilities to Clear (and not Purge) the data contents. Office equipment may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. Office equipment may have removable storage media, and if so, media-dependent sanitization techniques may be applied to the associated storage device.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	For both Clear and (if applicable) Purge, manually navigate to multiple areas of the device (such as stored fax numbers, network configuration information, etc.) to verify that no personal information has been retained on the device. For both Clearing and (if applicable) Purge, the ink, toner, and associated supplies (drum, fuser, etc.) should be removed and destroyed or disposed of in accordance with applicable law, environmental, and health considerations. Some of these supplies may retain impressions of data printed by the machine and therefore could pose a risk of data exposure, and should be handled accordingly. If the device is functional, one way to reduce the associated risk is to print a blank page, then an all-black page, then another blank page. For devices with dedicated color components (such as cyan, magenta, and yellow toners and related supplies), one page of each color should also be printed between blank pages. The resulting sheets should be handled at the confidentiality of the Office Equipment (prior to sanitization). Note that these procedures do not apply to supplies such as ink/toner on a one-time use roll, as they are typically not used again and therefore will not be addressed by sending additional pages through the equipment. They will, however, still need to be removed and destroyed. Office Equipment supplies may also pose health risks, and should be handled using appropriate procedures to minimize exposure to the print components and toner. For both Clear and (if applicable) Purge, refer to the manufacturer for additional information on the proper sanitization procedure.

Table A-5: Magnetic Media Sanitization

Magnetic Media	
Floppies	
Clear:	Overwrite media by using organizationally approved software and perform verification on the overwritten data. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.
Purge:	Degauss in an organizationally approved degausser rated at a minimum for the media.
Destroy:	Incinerate floppy disks and diskettes by burning in a licensed incinerator or Shred.
Magnetic Disks (flexible or fixed)	
Clear:	Overwrite media by using organizationally approved software and perform verification on the overwritten data. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.

Purge:	Degauss in an organizationally approved degausser rated at a minimum for the media.
Destroy:	Incinerate disks and diskettes by burning in a licensed incinerator or Shred.
Notes:	Degaussing magnetic disks typically renders the disk permanently unusable.
Reel and Cassette Format Magnetic Tapes	
Clear:	Re-record (overwrite) all data on the tape using an organizationally approved pattern, using a system with similar characteristics to the one that originally recorded the data. For example, overwrite previously recorded 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. 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.
Purge:	Degauss the magnetic tape in an organizationally approved degausser rated at a minimum for the media.
Destroy:	Incinerate by burning the tapes in a licensed incinerator or Shred.
Notes:	Preparatory steps for Destruction, 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.
ATA Hard Disk Drives *This includes PATA, SATA, eSATA, etc*	
Clear:	Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.
Purge:	Four options are available: 1. Use one of the ATA Sanitize Device feature set commands, if supported, to perform a Sanitize operation. One or both of the following options may be available: a. The overwrite EXT command. Apply one write pass of a fixed pattern across the media surface. Some examples of fixed patterns include all zeros or a pseudorandom pattern. A single write pass should suffice to Purge the media. *Optionally:* Instead of one write pass, use three total write passes of a pseudorandom pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified. b. If the device supports encryption and the technical specifications described in this document have been satisfied, the Cryptographic Erase (also known as CRYPTO SCRAMBLE EXT) command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase. 2. Use the ATA Security feature set's SECURE ERASE UNIT command, if support, in Enhanced Erase mode. The ATA Sanitize Device feature set commands are preferred over the over the ATA Security feature set SECURITY ERASE UNIT command when supported by the ATA device. 3. Cryptographic Erase through the Trusted Computing Group (TCG) Opal Security Subsystem Class (SSC) or Enterprise SSC interface by issuing commands as

	necessary to cause all MEKs to be changed (if the requirements described in this document have been satisfied). Refer to the TCG and device manufacturers for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase. 4. Degauss in an organizationally approved automatic degausser or disassemble the hard disk drive and Purge the enclosed platters with an organizationally approved degaussing wand.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge, except degaussing. The assurance provided by degaussing depends on selecting an effective degausser, applying it appropriately and periodically spot checking the results to ensure it is working as expected. When using the three pass ATA sanitize overwrite procedure with the invert option, the verification process would simply search for the original pattern (which would have been written again during the third pass). The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media as defined in the ATA standard, such as a Host Protected Area (HPA), Device Configuration Overlay (DCO), or Accessible Max Address. Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. Recovery data, such as an OEM-provided restoration image may have been stored in this manner, and sanitization may therefore impact the ability to recover the system unless reinstallation media is also available. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in section 4.7 should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. Given the variability in implementation of the ATA Security feature set SECURITY ERASE UNIT command, use of this command is not recommended without first consulting with the manufacturer to verify that the storage device's model-specific implementation meets the needs of the organization. This guidance applies to Legacy Magnetic media only, and it is critical to verify the media type prior to sanitization. Note that emerging media types, such as HAMR media or hybrid drives may not be easily identifiable by the label. Refer to the manufacturer for details about the media type in a storage device. Degaussing the media in a storage device typically renders the device unusable.
SCSI Hard Disk Drives *This includes Parallel SCSI,Serial Attached SCSI (SAS), Fibre Channel, USB Attached Storage (UAS), and SCSI Express Partial sanitization is not supported in this section.*	
Clear:	Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may optionally be used.
Purge:	Four options are available: 1. Apply the SCSI SANITIZE command, if supported. One or both of the following options

	may be available: a. The OVERWRITE service action. Apply one write pass of a fixed pattern across the media surface. Some examples of fixed patterns include all zeros or a pseudorandom pattern. A single write pass should suffice to Purge the media. *Optionally:* Instead of one write pass, use three total write passes of a pseudorandom pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified. b. If the device supports encryption, the CRYPTOGRAPHIC ERASE service action. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Clear procedure could alternatively be applied. 3. Degauss in an organizationally approved automatic degausser or disassemble the hard disk drive and Purge the enclosed platters with an organizationally approved degaussing wand. The degausser/wand should be rated sufficient for the media.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection, except degaussing. The assurance provided by degaussing depends on selecting an effective degausser, applying it appropriately and periodically spot checking the results to ensure it is working as expected. When using the three pass SCSI sanitize overwrite procedure with the invert (also known as complement) option, the verification process would simply search for the original pattern (which would have been written again during the third pass). While it is widely accepted that one pass of overwriting should be sufficient for Purging the data, the availability of a dedicated command that incorporates the ability to invert the data pattern allows an efficient and effective approach that mitigates any residual risk associated with variations in implementations of magnetic recording features across device manufacturers. The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media, such as "SCSI mode parameter block descriptor's NUMBER OF LOGICAL BLOCKS field (accessible with the SCSI MODE SENSE and MODE SELECT commands". Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. This guidance applies to Legacy Magnetic media only, and it is critical to verify the media type prior to sanitization. Note that emerging media types, such as HAMR media or hybrid drives may not be easily identifiable by the label. Refer to the manufacturer for details about the media type in a storage device.

	Degaussing the media in a storage device typically renders the device unusable.

Table A-6: Peripherally Attached Storage Sanitization

Peripherally Attached Storage	
External Locally Attached Hard Drives *This includes, USB, Firewire, etc. (Treat eSATA as ATA Hard drive.)*	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.
Purge:	The implementation of External Locally Attached Hard Drives varies sufficiently across models and vendors that the issuance of any specific command to the device may not reasonably and consistently assure the desired sanitization result. When the external drive bay contains an ATA or SCSI hard drive, if the commands can be delivered natively to the device, the device may be sanitized based on the associated media-specific guidance. However, the drive could be configured in a vendor-specific manner that precludes sanitization when removed from the enclosure. Additionally, if sanitization techniques are applied, the hard drive may not work as expected when reinstalled in the enclosure. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting, block erasing, Cryptographic Erase, etc.) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification as described in the Verify Methods subsection must be performed for each technique within Clear and Purge. Some external locally attached hard drives, especially those featuring security or encryption features, may also have hidden storage areas that might not be addressed even when the drive is removed from the enclosure. The device vendor may leverage proprietary commands to interact with the security subsystem. Please refer to the manufacturer to identify whether any reserved areas exist on the media and whether any tools are available to remove or sanitize them, if present.

Table A-7: Optical Media Sanitization

Optical Media	
CD, DVD, BD	
Clear/ Purge:	N/A

Destroy:	Destroy in order of recommendations: 1. Removing the information-bearing layers of CD media using a commercial optical disk grinding device. Note that this applies only to CD and not to DVD or BD media 2. Incinerate optical disk media (reduce to ash) using a licensed facility. 3. Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of 0.5 mm and surface area of 0.25 mm^2 or smaller.

Table A-8: Flash Memory-Based Storage Device Sanitization

Flash Memory-Based Storage Devices	
ATA Solid State Drives (SSDs) *This includes PATA, SATA, eSATA, etc.*	
Clear:	1. Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used. Note: It is important to note that overwrite on flash-based media may significantly reduce the effective lifetime of the media and it may not sanitize the data in unmapped physical media (i.e., the old data may still remain on the media). 2. Use the ATA Security feature set's SECURITY ERASE UNIT command, if supported.
Purge:	Three options are available: 1. Apply the ATA sanitize command, if supported. One or both of the following options may be available: a. The block erase command. *Optionally:* After the block erase command is successfully applied to a device, write binary 1s across the user addressable area of the storage media and then perform a second block erase. b. If the device supports encryption, the Cryptographic Erase (also known as sanitize crypto scramble) command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, Secure Erase or the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, Secure Erase or the Clear procedure could alternatively be applied.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase.

	The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media as defined in the ATA standard, such as a Host Protected Area (HPA), Device Configuration Overlay (DCO), or Accessible Max Address. Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. Recovery data, such as an OEM-provided restoration image may have been stored in this manner, and sanitization may therefore impact the ability to recover the system unless reinstallation media is also available. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. Given the variability in implementation of the Enhanced Secure Erase feature, use of this command is not recommended without first referring the manufacturer to identify that the storage device's model-specific implementation meets the needs of the organization. Whereas ATA Secure Erase was a Purge mechanism for magnetic media, it is only a Clear mechanism for flash memory due to variability in implementation and the possibility that sensitive data may remain in areas such as spare cells that have been rotated out of use. Degaussing must not be solely relied upon as a sanitization technique on flash memory-based storage devices or on hybrid devices that contain non-volatile flash memory storage media. Degaussing may be used when non-volatile flash memory media is present if the flash memory components are sanitized using media-dependent techniques.
SCSI Solid State Drives (SSSDs) *This includes Parallel SCSI, Serial Attached SCSI (SAS), Fibre Channel, USB Attached Storage (UAS), and SCSI Express.*	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used. Note: It is important to note that overwrite on flash-based media may significantly reduce the effective lifetime of the media and it may not sanitize the data in unmapped physical media (i.e., the old data may still remain on the media).
Purge:	Two options are available: 1. Apply the SCSI SANITIZE command, if supported. One or both of the following options may be available: a. The BLOCK ERASE service action. b. If the device supports encryption, the CRYPTOGRAPHIC ERASE service action. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure is an acceptable alternative.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection. The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media, such as SCSI mode select. Even when a dedicated sanitization

	command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D. Degaussing must not be performed as a sanitization technique on flash memory-based storage devices.
NVM Express SSDs	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.
Purge:	Two options are available: 1. Apply the NVM Express Format command, if supported. One or both of the following options may be available: a. The User Data Erase command. b. If the device supports encryption, the Cryptographic Erase command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the User Data Erase command (if supported) to erase the media. If the User Data Erase command is not supported, the Clear procedure could alternatively be applied. 2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the User Data Erase command (if supported) to erase the media. If the User Data Erase command is not supported, the Clear procedure is an acceptable alternative.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification must be performed for each technique within Clear and Purge. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase. Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance. Degaussing must not be performed as a sanitization technique on flash memory-based storage devices.
USB Removable Media *This includes Pen Drives, Thumb Drives, Flash Memory Drives, Memory Sticks, etc.*	
Clear:	Overwrite media by using organizationally approved and tested overwriting

	technologies/methods/tools. The Clear pattern should be at least two passes, to include a pattern in the first pass and its complement in the second pass. Additional passes may be used.
Purge:	Most USB removable media does not support sanitize commands, or if supported, the interfaces are not supported in a standardized way across these devices. Refer to the manufacturer for details about the availability and functionality of any available sanitization features and commands.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	For most cases where Purging is desired, USB removable media should be Destroyed.
Memory Cards *This includes SD, SDHC, MMC, Compact Flash Memory, Microdrive, MemoryStick, etc.*	
Clear:	Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear pattern should be at least two passes, to include a pattern in the first pass and its complement in the second pass. Additional passes may be used.
Purge:	N/A
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	None.
Embedded Flash Memory on Boards and Devices *This includes motherboards and peripheral cards such as network adapters or any other adapter containing non-volatile flash memory.*	
Clear:	If supported by the device, reset the state to original factory settings.
Purge:	N/A If the flash memory can be easily identified and removed from the board, the flash memory may be Destroyed independently from the disposal of the board that contained the flash memory. Otherwise, the whole board should be Destroyed.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	While Embedded flash memory has traditionally not been specifically addressed in media sanitization guidelines, the increasing complexity of systems and associated use of flash memory has complementarily increased the likelihood that sensitive data may be present. For example, remote management capabilities integrated into a modern motherboard may necessitate storing IP addresses, hostnames, usernames and passwords, certificates, or other data that may be considered sensitive. As a result, for Clearing, it may be necessary to interact with multiple interfaces to fully reset the device state. When this concept is applied to the example, this might include the BIOS/UEFI interface as well as the remote management interface. As with other types of media, the choice of sanitization technique is based on environment-specific considerations. While the choice might be made to neither Clear nor Purge embedded flash memory, it is important to recognize and accept the potential risk and continue to reevaluate the risk as the environment changes.

Table A-9: RAM- and ROM-Based Storage Device Sanitization

RAM and ROM-Based Storage Devices	
Dynamic Random Access Memory (DRAM)	
Clear/ Purge:	Power off device containing DRAM, remove from the power source, and remove the battery (if battery backed). Alternatively, remove the DRAM from the device.
Destroy:	Shred, Disintegrate, or Pulverize.
Notes:	In either case, the DRAM must remain without power for a period of at least five minutes.
Electronically Alterable PROM (EAPROM)	
Clear/ Purge:	Perform a full chip Purge as per manufacturer's data sheets.
Destroy:	Shred, Disintegrate, or Pulverize.
Notes:	None.
Electronically Erasable PROM (EEPROM)	
Clear/ Purge:	Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	None.

Appendix B—Glossary

ATA	Magnetic media interface specification. Also known as "IDE" – Integrated Drive Electronics.
BD	A Blu-ray Disc (BD) has the same shape and size as a CD or DVD, but has a higher density and gives the option for data to be multi-layered.
Bend	The use of a mechanical process to physically transform the storage media to alter its shape and make reading the media difficult or infeasible using state of the art laboratory techniques.
Clear	A method of Sanitization by applying logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user; typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).
CD	A Compact Disc (CD) is a class of media from which data are read by optical means.
CD-RW	A Compact Disc Read/Write (CD-RW) is a CD that can be Purged and rewritten multiple times.
CD-R	A Compact Disc Recordable (CD-R) is a CD that can be written on only once but read many times. Also known as WORM.
CE	See *Cryptographic Erase*.
CMRR	The Center for Magnetic Recording Research, located at the University of California, San Diego, advances the state-of-the-art in magnetic storage and trains graduate students and postdoctoral professionals (CMRR homepage: http://cmrr.ucsd.edu/).
Cut	The use of a tool or physical technique to cause a break in the surface of the electronic storage media, potentially breaking the media into two or more pieces and making it difficult or infeasible to recover the data using state of the art laboratory techniques.
Cryptographic Erase	A method of Sanitization in which the Media Encryption Key (MEK) for the encrypted Target Data (or the Key Encryption Key – KEK) is sanitized, making recovery of the decrypted Target Data infeasible.

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. 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. Also called "demagnetizing."
Destroy	A method of Sanitization that renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.
Digital	The coding scheme generally used in computer technology to represent data.
Disintegration	A physically Destructive method of sanitizing media; the act of separating into component parts.
Disposal	Disposal is a release outcome following the decision that media does not contain sensitive data. This occurs either because the media never contained sensitive data or because Sanitization techniques were applied and the media no longer contains sensitive data.
DVD	A Digital Video Disc (DVD) has the same shape and size as a CD, but with a higher density that gives the option for data to be double-sided and/or double-layered.
DVD-RW	A rewritable (re-recordable) DVD for both movies and data from the DVD Forum.
DVD+RW	A rewritable (re-recordable) DVD for both movies and data from the DVD+RW Alliance.
DVD+R	A write-once (read only) version of the DVD+RW from the DVD+RW Alliance.
DVD-R	A write-once (read only) DVD 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. It could also be a removable cartridge containing one or more magnetic disks.
Incineration	A physically Destructive method of sanitizing media; the act of burning completely to ashes.
Information	Meaningful interpretation or expression of data.
Magnetic Media	A class of storage device that uses only magnetic storage media for persistent storage, without the assistance of heat (ie. heat assisted magnetic recording (HAMR)) or the additional use of other persistent storage media such as flash memory-based media.
Media	Plural of medium.
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 Disk	A plastic disk that is read using an optical laser device.
Overwrite	Writing data on top of the physical location of data stored on the media.
Physical Destruction	A Sanitization method for media.
Pulverization	A physically Destructive method of sanitizing media; the act of grinding to a powder or dust.
Purge	A method of Sanitization by applying physical or logical techniques that renders Target Data recovery infeasible using state of the art laboratory techniques.
Read	Fundamental process in an information system that results only in the flow of information from storage media to a requester.
Read-Only Memory	ROM is a pre-recorded storage medium that can only be read from

	and not written to.
Record	To write data on a medium, such as a magnetic tape, magnetic disk, or optical disk.
Remanence	Residual information remaining on storage media.
ROM	See *Read-Only Memory*.
Sanitize	A process to render access to Target Data on the media infeasible for a given level of effort. Clear, Purge, and Destroy are actions that can be taken to sanitize media.
SANITIZE Command	A command in the ATA and SCSI standards that leverages a firmware-based process to perform a Sanitization action. If a device supports the *sanitize* command, the device must support at least one of three options: *overwrite*, *block erase* (usually for flash memory-based media), or *crypto scramble* (Cryptographic Erase). These commands typically execute substantially faster than attempting to rewrite through the native read and write interface. The ATA standard clearly identifies that the Sanitization operations must address user data areas, user data areas not currently allocated (including "previously allocated areas and physical sectors that have become inaccessible"), and user data caches. The resulting media contents vary based on the command used. The *overwrite* command allows the user to specify the data pattern applied to the media, so that pattern (or the inverse of that pattern, if chosen) will be written to the media (although the actual contents of the media may vary due to encoding). The result of the *block erase* command is vendor unique, but will likely be 0s or 1s. The result of the *crypto scramble* command is vendor unique, but will likely be cryptographically scrambled data (except for areas that were not encrypted, which are set to the value the vendor defines).
SCSI	A magnetic media interface specification. Small Computer System Interface.
Secure Erase Command	An *overwrite* command in the ATA standard (as 'Security Erase Unit') that leverages a firmware-based process to overwrite the media. This command typically executes substantially faster than attempting to rewrite through the native read and write interface. There are up to two options, 'normal erase' and 'enhanced erase'. The normal erase, as defined in the standard, is only required to address data in the contents of LBA 0 through the greater of READ NATIVE MAX or READ NATIVE MAX EXT, and replaces the contents with 0s or 1s. The *enhanced erase* command specifies that, "…all previously written user data shall be overwritten, including

	sectors that are no longer in use due to reallocation" and the contents of the media following Sanitization are vendor unique. The actual action performed by an *enhanced erase* varies by vendor and model, and could include a variety of actions that have varying levels of effectiveness. The *secure erase* command is not defined in the SCSI standard, so it does not apply to media with a SCSI interface.
Shred	A method of sanitizing media; the act of cutting or tearing into small particles.
SSD	A Solid State Drive (SSD) is a storage device that uses solid state memory to store persistent data.
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.
Target Data	The information subject to a given process, typically including most or all information on a piece of storage media.
Validate	The step in the media sanitization process flowchart which involves testing the media to ensure the information cannot be read.
Verification	The process of testing the media to ensure the information cannot be read.
WORM	Write-Once Read Many. Also see *CD-R*.
Write	Fundamental operations of an information system that results only in the flow of information from an actor to storage media.

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 verify them to a certain level of assurance. NIST does not conduct an evaluation of any tool set to verify 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 should continually monitor and verify the effectiveness of their selected sanitization tools as they are used.

If an organization has a product that they trust and have tested, then they are strongly encouraged to share this information through public forums, such as the Federal Computer Security Managers' Forum[22].

C.1 NSA Media Destruction Guidance

This guide also recommends that the user consider the National Security Agency (NSA) devices posted in the Media Destruction Guidance area of the public NSA website[23]. NSA states that "the products on these lists meet specific NSA performance requirements for sanitizing, destroying, or disposing of media containing sensitive or classified information. Inclusion on a list does not constitute an endorsement by NSA or the U.S. Government." The evaluated products lists provided on NSA's website cover:

- Crosscut paper shredders,
- Optical media,
- Degaussers,
- Storage devices, and
- Disintegrators.

C.2 Open Source Tools

There are a variety of open source tools available that support leveraging the sanitize commands based on standardized interfaces. As with any sanitization tool, independent validation should be performed to ensure the desired functionality is provided. However, the availability of open source tools helps organizations understand how the commands work and allows testing of sanitize commands on a drive, as well as supporting the ability of home users to apply sanitization to their personal media.

---

[22] http://csrc.nist.gov/groups/SMA/forum/

[23] http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

For example, one open source project is **hdparm**, which is available on SourceForge[24].

C.3 EPA Information on Electronic Recycling (e-Cycling)

Organizations and individuals wishing to donate used electronic equipment or seeking guidance on disposal of residual materials after sanitization should consult the Environmental Protection Agency's (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.

C.4 Outsourcing Media Sanitization and Destruction

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.'[25]

C.5 Trusted Computing Group Storage Specifications

Information on the TCG storage specifications (Opal SSC or Enterprise SSC interface specs) is available on the TCG's website:
http://www.trustedcomputinggroup.org/

C.6 Standards for ATA and SCSI

Information on the ATA and SCSI standards is available at:

http://www.t13.org/

http://www.t10.org/

Note: The ATA and SCSI standards are published by:

---

[24] http://hdparm.sourceforge.net/

[25] "Disposal of Consumer Report Information and Records Section," Title 16 *Code of Federal Regulations*, Pt. 682.3 (b) (3).

a) INCITS and ANSI as an American National Standard (see http://www.incits.org and http://www.ansi.org)

b) ISO/IEC as an International standard (see http://www.iso.org and http://www.iec.ch)

C.7 NVM Express Specification

Information on NVM Express is available at:

http://www.nvmexpress.org/

Appendix D—Cryptographic Erase Device Guidelines

The determination of whether to use Cryptographic Erase on a given device depends on an organization's sanitization requirements. It also depends on the end user's ability to determine whether the implementation offers sufficient assurance against future recovery of the data. The level of assurance depends in large part on the factors described in Table D-1.

Table D-1: Cryptographic Erase Considerations

Area	Consideration(s)	Relevant Doc(s)
Key Generation	The level of entropy of the random number sources and quality of whitening procedures applied to the random data. This applies to the cryptographic keys, and potentially to wrapping keys affected by the CE operation.	SP 800-90[26] SP 800-90A SP 800-90B SP 800-90C, SP 800-133
Media Encryption	The security strength and validity of implementation of the encryption algorithm/mode used for protection of the Target Data.	FIPS 140-2[27] FIPS 197 SP 800-38A (not including ECB) SP 800-38E
Key Level and Wrapping	The key being sanitized might not be the Media Encryption Key (MEK), but instead a key used to wrap (that is, encrypt) the MEK or another key. In this case, the security strength and level of assurance of the wrapping techniques used should be commensurate with the level of strength of the CE operation.	FIPS 197 SP 800-38A SP 800-38F SP 800-131A

Before relying on Cryptographic Erase for media sanitization, users should identify the mechanisms implemented by the storage device to address these areas:

1. **Make/Model/Version/Media Type:** The product and versions the statement applies to, and the type of media the device uses (ie. magnetic, SSD, hybrid, other).

   Many devices store the Target Data in several different media - e.g. a DRAM (Dynamic Random Access Memory) cache in addition to rotating platters. It is important to identify the storage locations and how each is sanitized.

[26] A list of validated Deterministic Random Bit Generators (DRBGs) is available at: http://csrc.nist.gov/groups/STM/cavp/documents/drbg/drbgval.html.

[27] Conformance testing for FIPS 140-2 is conducted within the framework of the Cryptographic Module Validation Program (CMVP), http://csrc.nist.gov/groups/STM/cmvp/, and the Cryptographic Algorithm Validation Program (CAVP), http://csrc.nist.gov/groups/STM/cavp/.

2. **Key Generation:** Identify whether a Deterministic Random Bit Generator (DRBG), such as one of those listed in SP 800-90,[28] was used, and whether it was validated.

3. **Media Encryption:** Identify the algorithm, key strength, mode of operation, and any applicable validation(s).

4. **Key Level and Wrapping:** Identify if the MEK (either wrapped with another value or not wrapped) is directly sanitized, or if a key that wraps the MEK (a key encryption key, or KEK) is sanitized. A description of the wrapping techniques only applies where a KEK (and not the MEK) is sanitized. Wrapping details, when provided, should include the algorithm used, strength, and (if applicable) mode of operation.

5. **Data Areas Addressed:** Describe which areas are encrypted and which areas are not encrypted. For any unencrypted areas, describe how sanitization is performed.

6. **Key Life Cycle Management:** The key(s) on a device may have multiple wrapping activities (wrapping, unwrapping, and rewrapping) throughout the device's lifecycle. Identify how the key(s) being sanitized are handled during wrapping activities that are not directly part of the Cryptographic Erase operation. For example, a user may have received an SED that was always encrypting, and simply turned on the authentication interface. Identify how the previous instance of the MEK was sanitized when it was wrapped with the user's authentication credentials.

7. **Key Sanitization Technique:** Describe the media-dependent sanitization method for the key being sanitized. Some examples might include one or more inverted overwrite passes if the media is magnetic, a block erase for an SSD, or other media-specific techniques for other types of media.

8. **Key Escrow or Backup:** Identify whether the device supports key escrow or backup. Identify whether the device supports discovery of whether any key(s) at or below the level of the key escrowed has/have ever been escrowed from or injected into the device.If the MEK is directly sanitized and only a KEK can be escrowed, clearly identify that fact.

9. **Error Condition Handling:** Identify how the device handles error conditions that prevent the Cryptographic Erase operation from fully completing. For example, if the location where the key was stored cannot be sanitized, does the Cryptographic Erase operation report success or failure to the user?

10. **Interface Clarity:** Identify which interface commands support the features described in the statement. If the device supports the use of multiple MEKs, identify whether all MEKs are changed using the interface commands available and any additional commands or actions necessary to ensure all MEKs are changed. Note that under certain conditions, not all MEKs have to be cleared (e.g., partial sanitization of target data).

[28] NIST SP 800-90A (as amended), *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*, January 2012, 136 pp. http://csrc.nist.gov/publications/PubsSPs.html#800-90A.

D.1 Example Statement of Cryptographic Erase Features

The following statements should be placed by the storage device vendor in an area accessible to potential users of a device, such as on the vendor's website or in product literature that is widely available. Information of a proprietary nature may not be available in published product information.

1. **Make/Model/Version/Media Type:** Acme hard drive model abc12345 version 1+. Media type is Legacy Magnetic media.

2. **Key Generation:** A DRBG is used as specified in SP 800-90, with validation [number].

3. **Media Encryption:** Media is encrypted with AES-256 media encryption in Cipher Block Chaining (CBC) mode as described in SP 800-38A. This device is FIPS 140 validated with certificate [number].

4. **Key Level and Wrapping:** The media encryption key is sanitized directly during Cryptographic Erase.

5. **Data Areas Addressed:** The device encrypts all data stored in the LBA-addressable space except for a preboot authentication and variable area and the device logs. Device log data is retained by the device following Cryptographic Erase.

6. **Key Lifecycle Management:** As the MEK moves between wrapped, unwrapped, and re-wrapped states, the previous instance is sanitized using three inverted overwrite passes.

7. **Key Sanitization Technique:** Three passes with a pattern that is inverted between passes.

8. **Key Escrow or Injection:** The device does not support escrow or injection of the keys at or below the level of the sanitization operation.

9. **Error Condition Handling:** If the storage device encounters a defect in a location where a key is stored, the device attempts to rewrite the location and the Cryptographic Erase operations continues, reporting success to the user if the operation is otherwise successful.

10. **Interface Clarity:** The device has an ATA interface and supports the ATA Sanitize Device feature set CRYPTO SCRAMBLE EXT command and a TCG Opal interface with the ability to sanitize the device by cryptographically erasing the contents. Both of these commands apply the functionality described in this statement.

Appendix E—Device-Specific Characteristics of Interest

Storage vendors implement a range of devices and media types that leverage the same standardized command sets. Some examples of command sets include ATA, SCSI, and NVM Express. There are likely to be differences in implementation between, for example, the enhanced Security Erase command for ATA devices from different vendors. Some vendors may have implementations 'under the hood' that apply techniques such as Cryptographic Erase, block erase (for flash memory devices), or other techniques. It may be difficult or impossible for users to know for sure how the sanitization action is being implemented.

In order to support informed decision making by users, vendors may choose to provide information about how a specific device implements any dedicated sanitize commands supported by the device. When reported by vendors, this information also helps purchasing authorities make informed decisions about which storage devices to acquire based on the availability of suitable sanitization functions and approaches. This vendor-reported information should address the following:

- The media type (i.e., Legacy Magnetic, HAMR, magnetic shingle, SLC/MLC/TLC Flash Memory, Hybrid, etc.)
    - If the device contains magnetic media, the coercivity of the magnetic media (to support an informed decision about whether to attempt to degauss the media)
- Which sanitize commands are supported (if any)
- For each sanitize command supported:
    - A list of any areas not addressed by the sanitization command
    - The estimated time necessary for the command to successfully complete
    - The results of any validation testing, if applicable

Appendix F—Selected Bibliography

Additional sources of useful information pertinent to SP 800-88 Rev 1

- *All About Degaussers and Erasure of Magnetic Media*, Athana International [Web page], http://www.athana.com/ddequip/allaboutdegaussers.htm [accessed 7/18/14].
- J. Anastasi, *The New Forensics: Investigating Corporate Fraud and the Theft of Intellectual Property.* Hoboken, N.J.: John Wiley and Sons, 2003.
- J. Daughton, *Magnetoresistive Random Access Memory (MRAM)*, (February 4, 2000), 13pp. http://www.nve.com/Downloads/mram.pdf [accessed 7/21/14].
- H.A. Davis, National Security Agency. NSA/CSS POLICY MANUAL 9-12. (NSA/CSS STORAGE DEVICE DECLASSIFICATION MANUAL) http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf N.p.: n.p., 2006.
- *Degaussing Described.* Weircliffe International Ltd, 9th English edition, 2006. Archived copy available at: https://web.archive.org/web/20070129044258/http://www.weircliffe.co.uk/pdf/Weircliffe_Degaussing.pdf [accessed 7/18/14]..
- Y. Deng, "What is the future of disk drives, death or rebirth?" *ACM Computing Surveys*, 43(3), Article no. 23, (April 2011). http://dx.doi.org/10.1145/1922649.1922660.
- S.L. Garfinkel, and A. Shelat, "Remembrance of Data Passed: A Study of Disk Sanitization Practices," *IEEE Security & Privacy* 1(1), 17-27, (Jan.-Feb. 2003). http://dx.doi.org/10.1109/MSECP.2003.1176992.
- G. Gibson, and M. Polte, *Directions for Shingled-Write and Two- Dimensional Magnetic Recording System Architectures: Synergies with Solid-State Disks*, CMU-PDL-09-104, Carnegie Mellon University Parallel Data Laboratory, Pittsburgh, Pennsylvania, May 2009, 2pp. http://repository.cmu.edu/cgi/viewcontent.cgi?article=1004&context=pdl [accessed 7/21/14].
- *A Guide to Understanding Data Remanence in Automated Information Systems*, National Computer Security Center, NCSC-TG-025, Version 2. https://www.marcorsyscom.usmc.mil/Sites/PMIA%20Documents/Resources/national/NCSC-TG-025%20Data%20Remanence.html [accessed 7/21/14].
- P. Gutmann, "Data Remanence in Semiconductor Devices," *Proceedings of the 10th USENIX Security Symposium*, Washington, D.C. (August 13-17, 2001), 16pp. http://static.usenix.org/publications/library/proceedings/sec01/full_papers/gutmann/gutmann.pdf [accessed 7/21/14].
- P. Gutmann, , "Secure Deletion of Data from Magnetic and Solid-State Memory," *Proceedings of the Sixth USENIX Security Symposium*, San Jose, California, (July 22-25,

1996) 77-90. http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html [accessed 7/21/14].

- G.F. Hughes, T. Coughlin, T., and D.M. Commins, "Disposal of Disk and Tape Data by Secure Sanitization," *IEEE Security & Privacy* 7(4), 29-34 (July-Aug. 2009). http://dx.doi.org/10.1109/MSP.2009.89.

- InterNational Committee for Information Technology Standards. *Information technology – AT Attachment 8 - ATA/ATAPI Command Set - 2 (ATA8-ACS-2)*, INCITS 482-2012, American National Standards Institute, New York, May 30, 2012.

- InterNational Committee for Information Technology Standards., *Information technology - SCSI Primary Commands - 4 (SPC-4)*, INCITS 513, May 17, 2014. http://www.t10.org/cgi-bin/ac.pl?t=f&f=spc4r37.pdf [accessed 7/18/14].

- J. Hasson, "V.A. Toughens Security after PC Disposal Blunders," *Federal Computer Week*, August 26, 2002. http://fcw.com/Articles/2002/08/26/VA-toughens-security-after-PC-disposal-blunders.aspx [accessed 7/21/14].

- C. King, and T. Vidas, "Empirical analysis of solid state disk data retention when used with contemporary operating systems," *Digital Investigation* 8 (2011), S111-S117. http://dx.doi.org/10.1016/j.diin.2011.05.013.

- *Microsoft EFI FAT32 File System Specification*, Microsoft Corporation, December 6, 2000. http://msdn.microsoft.com/en-us/library/windows/hardware/gg463080.aspx [accessed 7/21/14].

- B.J. Phillips, C.D. Schmidt, and D.R. Kelly, "Recovering data from USB flash memory sticks that have been damaged or electronically erased," *e-Forensics '08: Proceedings of the 1st international conference on Forensic applications and techniques in telecommunications, information, and multimedia and workshop*, Adelaide, Australia (January 21-23, 2008), article no. 19. http://dx.doi.org/10.4108/e-forensics.2008.2771.

- A. Suresh, G. Gibson, and G. Ganger. *Shingled Magnetic Recording for Big Data Applications*, CMU-PDL-12-105, Carnegie Mellon University, Parallel Data Lab, Pittsburgh, Pennsylvania, May 2012, 29 pp. http://www.pdl.cmu.edu/PDL-FTP/FS/CMU-PDL-12-105.pdf [accessed 7/18/14].

- U.S. Army. *Information Assurance*, Army Regulation (AR) 25–2, October 24, 2007 (with Rapid Action Release on March 23, 2009). http://armypubs.army.mil/epubs/pdf/r25_2.pdf [accessed 7/18/14].

- U.S. Department of Defense, "Clearing and Sanitization Data Storage," Table C8.T1 in *National Industrial Security Program: Operating Manual*, DoD 5220.22-M-Sup-1, Washington, D.C. (February 1, 2005), pp.82-83. http://www.dtic.mil/whs/directives/corres/pdf/522022MSup1.pdf Page 81[accessed 7/21/14].

- *Understand Degaussing*, Peripheral Manufacturing Inc. [Web page], http://www.periphman.com/understand_degaussing.shtml [accessed 7/21/14].

- M. Wei, L.M. Grupp, F.E. Spada, and S. Swanson, "Reliably Erasing Data From Flash-Based Solid State Drives," *9th USENIX Conference on File and Storage Technologies (FAST '11)*, San Jose, California (February 15-17, 2011), 13pp. http://www.usenix.org/events/fast11/tech/full_papers/Wei.pdf [accessed 7/21/14].

- B. Xu, J. Yang, H. Yuan, J. Zhang, Q. Zhang, and T.C. Chong, "Thermal Effects in Heat Assisted Bit Patterned Media Recording," *IEEE Transactions on Magnetics* 45(5) 2292-2295 (May 2009). http://dx.doi.org/10.1109/TMAG.2009.2016466.

Appendix G—Sample "Certificate of Sanitization" Form

This certificate is simply an example to demonstrate the types of information that should be collected and how a certificate might be formatted. An organization could alternatively choose to electronically record sanitization details, either through a native application or by using a form such as this one with an automated data transfer utility (such as a PDF form with a button to send the data to a database or email address). In the event that the records need to be referenced in the future, electronic records will likely provide the fastest search capabilities and best likelihood that the records are reliably retained.

CERTIFICATE OF SANITIZATION		
PERSON PERFORMING SANITIZATION		
Name:	Title:	
Organization:	Location:	Phone:
MEDIA INFORMATION		
Make/ Vendor:	Model Number:	
Serial Number:		
Media Property Number:		
Media Type:	Source *(ie user name or PC property number)*:	
Classification:	Data Backed Up: ☐ Yes ☐ No ☐ Unknown	
Backup Location:		
SANITIZATION DETAILS		
Method Type: ☐ Clear ☐ Purge ☐ Damage ☐ Destruct		
Method Used: ☐ Degauss ☐ Overwrite ☐ Block Erase ☐ Crypto Erase ☐ Other:		
Method Details:		
Tool Used *(include version):*		
Verification Method: ☐ Full ☐ Quick Sampling ☐ Other:		
Post Sanitization Classification:		
Notes:		
MEDIA DESTINATION		
☐ Internal Reuse ☐ External Reuse ☐ Recycling Facility ☐ Manufacturer ☐ Other *(specify in details area)*		
Details:		
SIGNATURE		
I attest that the information provided on this statement is accurate to the best of my knowledge.		
Signature:		Date:
VALIDATION		
Name:	Title:	
Organization:	Location:	Phone:
Signature:		Date: