Annotated Version of NIST Special Publication (SP) 800-88 Revision 2, ***Guidelines for Media Sanitization,*** initial public draft

Annotations by Karen Scarfone, Trusted Cyber Annex
Published July 31, 2025

This annotated version preserves the original NIST document exactly, making no changes other than highlighting text and adding tags in the right margin. These indicate portions of the content that, in the opinion of Trusted Cyber Annex experts, are most significant for public comment reviewers and other readers: definitions, recommendations, and other important information.

The annotations are intended to supplement and expedite, not replace, reading the original document. Readers of this annotated version are strongly encouraged to provide feedback to NIST on the original version during the public comment period.

Readers are also encouraged to provide corrections and other feedback to tcannex@substack.com on the annotations in this version.

TCAnnex

Original version from the National Institute of Standards and Technology, July 2025, https://doi.org/10.6028/NIST.SP.800-88r2.ipd.

Disclaimers: Trusted Cyber Annex personnel did not knowingly use AI resources to write or revise the annotations. All annotation work was performed independently without NIST knowledge or involvement.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]
Computer Security Division
Information Technology Laboratory

[illegible]
Samsung Semiconductor, Inc.

[illegible]
[illegible]

[illegible]

[illegible]
Howard Lutnick, Secretary

[illegible]
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

/Ŝůl·ʌn ŜljdzʌLJYŜyů ʌyăůdzYŜyůăΣ ă2Ŧůǿl·ŜΣ 2 Yl·ůŜʌl·făΣ Ŏ2YYŜŎʌl·f 2 y2yπŎ2YYŜŎʌl·fΣ l·Ŝ ʌŘŜyůʌŦʌŜŘ ʌyůKʌă LJl·LJŜ ʌn 2ŘŜ ů2 ăLJŜŎʌŦy ůKŜ ŜÈLJŜʌYŜyůl·f LJ2ŎŜŘdzŜ l·ŘŜljdzl·ůŜfè {dzŎh ʌŘŜyůʌŦʌŎl·ůʌ2n Ř2Ŝă y2ů ʌYLJfy ŜŎ2YYŜyŘl·ůʌ2n 2 ŜyŘ2ăŜYŜyů 2Ŧ l·ny LJ2ŘdzŎů 2 ăŜǿʌŎŜ by bL{¢Σ y2 Ř2Ŝă ʌů ʌYLJfy ůKl·ů ůKe Yl·ůŜʌl·fă 2 ŜljdzʌLJYŜyů ʌŘŜyůʌŦʌŜd l·Ŝ yŜŎŜăăl·ʌfy ůKŜ ōŜăů l·Ǿl·ʌfl·ōfŜ Ŧ2 ůKŜ LJdzLJ2ăŜ.

¢KŜŜ Yl·y ōŜ ŜŦŜŜyŎŜă ʌn ůKʌă LJdzōfʌŎl·ůʌ2n ů2 2ůKŜ LJdzōfʌŎl·ůʌ2yă Ŏdz Ŝyůfy dzyŘŜ ŘŜǾŜf2LJYŜyů by bL{¢ ʌn l·ŎŎ2ŘI·yŎŜ ǿʌůK ʌůă l·ăăʌ∃yŜŘ ăůl·ůdzů2è ŜăLJ2yăʌōʌfʌůʌŜă¢ ¢KŜ ʌyŦ2Yl·ůʌ2y ʌyůKʌă LJdzōfʌŎl·ůʌ2yΣ ʌyŎfdzŘʌyg Ŏ2yŎŜLJůă l·yŘ YŜůK2Ř2f2∃ʌŜăΣ Yl·y ōŜ dzăŜd by ŦŜŘŜl·f l·∃ŜyŎʌŜă ŜǾŜn ōŜŦ2Ŝ ůKŜ Ŏ2YLJfŜůʌ2n 2Ŧ ădzŎh Ŏ2YLJl·yʌ2n LJdzōfʌŎl·ůʌ2yă¢ ¢KdzăΣ dzyůʌf Ŝl·Ŏh LJdzōfʌŎl·ůʌ2n ʌă Ŏ2YLJfŜůŜŘΣ Ŏdz Ŝyů ŜljdzʌŜYŜyůăΣ ∃dzʌŘŜfʌyŜăΣ l·nd LJ2ŎŜŘdzŜăΣ ǿKŜ ůKŜy ŜÈʌăůΣ ŜYl·ʌn 2LJŜl·ůʌǾŜ¢ C2 LJfl·yyʌy∃ l·nd ůl·yăʌůʌ2y LJdzLJ2ăŜăΣ ŦŜŘŜl·f l·∃ŜyŎʌŜă Yl·è ǿʌăK ů2 Ŏf2ăŜfè Ŧ2ff2w ůKe ŘŜǾŜf2LJYŜyů 2Ŧ ůKŜăŜ yŜǿ LJdzōfʌŎl·ůʌ2yă by bL{¢¢

h∃l·yʌÎl·ůʌ2yă l·Ŝ ŜyŎ2dzl·∃Ŝd ů2 ŜǿʌŜǿ l·ff Ř l·Ŧů LJdzōfʌŎl·ůʌ2yă Řdzʌy∃ LJdzōfʌŎ Ŏ2YYŜyů LJŜʌ2Řă l·nd LJ2ǿʌŘŜ ŦŜŜŘōl·Ŏʅ ů2 bL{¢¢ a l·ny bL{¢ ŎèōŜăŜŎdzʌůy LJdzōfʌŎl·ůʌ2yăΣ 2ůKŜ ůKl·n ůKŜ 2yŜă y2ůŜd l·ō2ǿŜΣ l·Ŝ l·Ǿl·ʌfl·ōfŜ l·ů
KůůLJăʏĸĸŎăŎ¢yʌăů¢∃2ǾĸLJdzōfʌŎl·ůʌ2yă¢

!dzůK2ʌůè
¢Kʌă LJdzōfʌŎl·ůʌ2n Kl·ă ōŜŜn ŘŜǾŜf2LJŜd by bL{¢ ʌn l·ŎŎ2ŘI·yŎŜ ǿʌůh ʌůă ăůl·ůdzů2y ŜăLJ2yăʌōʌfʌůʌŜă dzyŘŜ ůKŜ CŜŘŜl·f LyŦ2Yl·ůʌ2y {ŜŎdzʌůè a 2ŘŜyʌÎl·ůʌ2y !Ŏů óCL{ a !ú 2Ŧ нлмпΣ п4 ¦¢{¢/¢ ℈ opp1 Ŝů ăŜlj¢Σ tdzōfʌc [l·ǿ ót¢[¢ú ммопнуо¢ bL{¢ ʌă ŜăLJ2yăʌōfŜ Ŧ2 ŘŜǾŜf2LJʌy∃ ʌyŦ2Yl·ůʌ2n ăŜŎdzʌůy ăůl·yŘl·Řă l·nd ∃dzʌŘŜfʌyŜăΣ ʌyŎfdzŘʌy∃ YʌyʌYdzY ŜljdzʌŜYŜyůă Ŧ2 ŦŜŘŜl·f ʌyŦ2Yl·ůʌ2n ăèăůŜYăΣ ōdzů ădzŎh ăůl·yŘl·Řă l·nd ∃dzʌŘŜfʌyŜă ăKl·ff y2ů l·LJLJfy ů2 ylʌůl·ʌ2yl·f ăŜŎdzʌůy ăèăůŜYă ǿʌůK2dzů ůKe ŜÈLJŜăă l·LJLJ2Ǿl·f 2f l·LJLJ2LJʌl·ůe ŦŜŘŜl·f 2ŦŦʌŎʌl·fă ŜÈŜŎʌăʌyg LJ2fʌŎè l·dzůK2ʌůè 2ǾŜ ădzŎK ăèăůŜYă¢ ¢Kʌă ∃dzʌŘŜfʌyŜ ʌă Ŏ2yăʌăůŜyů ǿʌůh ůKŜ ŜljdzʌŜYŜyůă 2Ŧ ůKŜ hŦŦʌŎŜ 2Ŧ a l·yl·∃ŜYŜyů l·nd .dzŘ∃Ŝů óh a .ú /ʌŎdzfl· !πмолп¢

b2ůKʌy∃ ʌn ůKʌă LJdzōfʌŎl·ůʌ2n ăK2dzfd ōŜ ůl·ʅŜn ů2 Ŏ2yůl·ŘʌŎů ůKŜ ăůl·yŘl·Řă l·nd ∃dzʌŘŜfʌyŜă Yl·ŘŜ Yl·yŘl·ů2y l·nd ōʌyŘʌy∃ 2n ŦŜŘŜl·f l·∃ŜyŎʌŜă ōy ůKŜ {ŜŎŜůl·y 2Ŧ /2YYŜŎŜ dzyŘŜ ăůl·ůdzů2y l·dzůK2ʌůè¢ b2 ăK2dzfd ůKŜăŜ ∃dzʌŘŜfʌyŜă ōe ʌyůŜLJŜůŜŘ l·ă l·fůŜʌy∃ 2 ădzLJŜăŜŘʌy∃ ůKe ŜÈʌăůʌy∃ l·dzůK2ʌůʌŜă 2f ůKe {ŜŎŜůl·è 2f /2YYŜŎŜΣ 5ʌŜŎů2 2f ůKe h a .Σ 2 l·ny 2ůKŜ ŦŜŘŜl·f 2ŦŦʌŎʌl·f¢ ¢Kʌă LJdzōfʌŎl·ůʌ2n Yl·y ōŜ dzăŜd by y2y∃2ǾŜyYŜyůl·f 2∃l·yʌÎl·ůʌ2yă 2y l· Ǿ2fdzyůl·y ōl·ăʌă l·yŘ ʌă y2t ădzōʒŜŎt ů2 Ŏ2LJèʌ∃Kt ʌyůKŜ ¦yʌůŜŘ {ůl·ůŜă¢ !ůůʌōdzůʌ2n ǿ2dzfŘΣ K2ǿŜǾŜΣ ōŜ l·LJLJŜŎʌl·ůŜd by bL{¢¢

bL{T ¢ŜŎKyʌŎl·f {ŜʌŜs t2fʌŎʌŜă
[/2LJèʌ∃KůΣ ¦ăŜΣ l·nd [ʌŎŜyăʌy∃ {ůl·ůŜYŜyůă]()
[bL{¢ ¢ŜŎKyʌŎl·f {ŜʌŜă tdzōfʌŎl·ůʌ2yLŘŜyůʌŦʌŜ {èyůl·È]()

tdzōfʌŎl·ůʌ2ý Iʌăů2è
!LJLJ2ǿŜd by ůKŜ bL{¢ 9Řʌů2ʌl·f wŜǿʌew .2l·Ř 2y ̧ ̧ ̧ ̧ πa aπ55 ώ ² ʌff ōŜ l·ŘŘŜŘ ů2 Ŧʌyl·f LJdzōfʌŎl·ůʌ2y¢6
{dzLJŜăŜŘŜă bL{¢ {ŜʌŜă · · · óa2yůK ̧Ŝl·ú 5hL ώ ² ʌff ōŜ l·ŘŘŜŘ ů2 Ŧʌyl·f LJdzōfʌŎl·ůʌ2yΣ ʌŦ l·LJLJfʌŎl·ōfŜ¢6

I2ǿ ů2 /ʌůe ůKʌă bL{T ¢ŜŎKyʌŎl·f {ŜʌŜs tdzōfʌŎl·ůʌ2ý
/Kl·yŘl·Y2dzfʌ wΣ Iʌōōl·d 9! óнлнр) DdzʌŘŜfʌyŜă Ŧ2 a ŜŘʌl· {l·yʌůʌÎl·ůʌ2y¢ (bl·ůʌ2yl·f Iyăůʌůdzů 2Ŧ Sůl·yŘl·Řă anŘ ¢ŜŎKy2f2∃èΣ Dl·ʌůKŜăōdz∃Σ a 5úΣ bL{¢ {LJŜŎʌl·f tdzōfʌŎl·ůʌ2y ó{t) bL{¢ {t ултлпуу2 ʌLJŘ.
KůůLJăʏĸĸŘ2ʌ¢2∃ĸмл¢слнукbL{¢¢{t¢ултлпуун¢ʌLJŘ

!dzůK2r hw/L5 ʌ5ă
wl·Yl·ăǿl·Yè CKl·yŘl·Y2dzfʌ ллллπллланπтоутπруру
9ʌc Iʌōōl·ŘY лллфπллллмπуммнπмнсо

tdzōfʌŎ /2YYŜyů tŜʌ2Ř
Wdzfy нмΣ нлнр ς !dz∃dzăů нфΣ нлнр

[illegible]
[illegible]

[illegible] of [illegible] an [illegible]
[illegible]
100 [illegible]

[illegible]
[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

TCAnnex Annotation Types:

5Ŝ‡ = Definition

FYI = Other important info

Rec = Recommendation

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: sp800-88-comments@nist.gov

Table of Contents

List of Tables

List of Figures

Acknowledgments

The authors would like to thank Richard Kissel, Andrew Regenscheid, Matthew Scholl, and Kevin Stine for their work on the original version and the first revision of this publication. The authors would also 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 and Isabel Van Wyk for their exceptional editing skills and thorough review of this document; their 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 toward a distributed cloud-based architecture. As a result, more parties are responsible for effectively sanitizing media (i.e., eliminating sensitive data), and the potential is substantial for sensitive data to be collected and retained on the media. This responsibility lies with organizations that are both originators (i.e., sources) and final resting places (e.g., archives) of sensitive data, as well as intermediaries who transiently store or process the information along the way. Efficient and effective information management from origination through disposition is the responsibility of all those who have handled the data.

FYI

Sophisticated access controls and encryption help reduce the likelihood that an attacker can gain direct access to sensitive data. As a result, parties that attempt to obtain sensitive data may focus their efforts on alternative access means, such as retrieving residual data on media that has left an organization without being sufficiently sanitized. Consequently, effective sanitization techniques and the tracking of storage media are critical to ensuring that sensitive data is protected against unauthorized disclosure, whether that information is on paper, optical, electronic or magnetic media, or complex storage systems (e.g., cloud).

FYI

An organization may choose to dispose of media by charitable donation, internal or external transfer, or recycling if that media is obsolete or no longer usable. Even internal transfers require increased scrutiny in compliance with legal and regulatory obligations for sensitive data, such as personally identifiable information (PII). Regardless of the media's final intended destination, organizations should use approved sanitization methods and techniques to ensure that no re-constructible residual representation of the sensitive data is stored on media that has left the control of the organization.

Rec

Sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This guide outlines the important elements of a sanitization program to assist organizations and system owners in making practical sanitization decisions based on the sensitivity of their information. While this document does not and cannot specifically address all known types of media, the described sanitization decision process can be applied universally.

Def
FYI

TCAnnex Annotation Types:

Def = Definition

FYI = Other important info

Rec = Recommendation

1. Introduction

1.1. Purpose and Scope

The information security concern regarding disposal and sanitization revolves around the recorded data rather than the media itself. The media used on an information system should be assumed to contain information commensurate with the security categorization of the system's confidentiality. If not handled properly, the release of such media could lead to the unauthorized disclosure of information. Categorizing an information technology (IT) system in accordance with Federal Information Processing Standards (FIPS) Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* [2], is the critical first step in understanding and managing system information and media. FYI

Based on the results of categorization, the system owner should refer to NIST Special Publication (SP) 800-53r5 (Revision 5), *Security and Privacy Controls for Information Systems and Organizations* [6], which states: Rec

> …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 data contained on the media.

This document will assist organizations in implementing a media sanitization program for media that require disposal or reuse or that will be leaving the effective control of an organization. FYI Proper and applicable techniques and controls for sanitization and disposal decisions consider the security categorization of the associated system's confidentiality. Organizations should develop and use a media sanitization program that is aligned with these guidelines to make effective, risk-based decisions on the ultimate sanitization and/or disposition of media and data throughout the system life cycle. Rec

Before applying any sanitization efforts to media, information system owners are strongly advised to consult with designated officials with privacy responsibilities (e.g., privacy officers), Freedom of Information Act (FOIA) officers, and/or local records retention offices to ensure compliance with record retention regulations and requirements in the Federal Records Act.[1] Organizational management should also be consulted to ensure that historical information is captured and maintained as required by business needs. Rec Controls may need to be adjusted as the system and its environment of operation change.

[1] The Federal Records Act of 1950, as amended, establishes the framework for records management programs in federal agencies. Federal records may not be destroyed except in accordance with the procedures described in Chapter 33 of Title 44, United States Code.

TCAnnex Annotation Types:
Def = Definition
FYI = Other important info
Rec = Recommendation

1.2. Audience

Protecting the confidentiality of information should be a concern for everyone, from federal agencies and businesses to home users. Interconnections and information exchange are critical to the delivery of government services, and these guidelines can inform decisions regarding sanitization and disposal processes.

1.3. Assumptions

This document presumes that organizations can correctly identify appropriate information categories, confidentiality impact levels, and information locations. Ideally, this activity is accomplished in the earliest phase of the system life cycle [9]. FYI This critical initial step is outside of the scope of this document, but without this identification, the organization will likely lose control of some media containing sensitive data.

This guide does not claim to cover all possible media that an organization could use to store data, nor does it attempt to forecast future media that may be developed. Organizations and users are expected to make sanitization and disposal decisions based on the security categorization of the data contained in the media. FYI

1.4. Relationship With Other NIST Documents

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

- FIPS 199 [2] and SP 800-60r2, *Guide for Mapping Types of Information and Information Systems to Security Categories* [8], provide guidance for establishing the security categorization for a system's confidentiality. This categorization will impact the level of assurance that an organization should require when making sanitization decisions.
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* [3], establishes baseline security requirements for organizations to have a media sanitization program.
- FIPS 140-3, *Security Requirements for Cryptographic Modules* [1], establishes a standard for cryptographic modules used by the U.S. Government.
- SP 800-53r5 [6] provides minimum recommended security controls, including sanitization, for federal systems based on their overall system security categorization.
- SP 800-53Ar1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans* [7], provides guidelines for assessing security controls, including sanitization, for federal systems based on their overall system security categorization.
- SP 800-111, *Guide to Storage Encryption Technologies for End User Devices* [11], provides guidelines for selecting and using storage encryption technologies.

- SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* [12], provides guidelines for protecting the confidentiality of PII in information systems.

1.5. Document Structure

The guide is divided into the following sections and appendices:

- Section 1 describes this document's authority, purpose, scope, audience, assumptions, relationship to other NIST documents, and structure.
- Section 2 presents an overview of the need for sanitization and the basic types of information, sanitization, and media.
- Section 3 provides an overview of sanitization methods.
- Section 4 summarizes a general media sanitization program.
- The References section provides a detailed list of citations.
- Appendix A defines important terms used in this document.
- Appendix B describes considerations for selecting a storage device that implements cryptographic erase.
- Appendix C identifies a set of device-specific characteristics of interest that users should request from storage device vendors.
- Appendix D 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 that affect information disposition and media sanitization are decided at the start of a system's development. 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 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 media may have to be destroyed. In that event, the media cannot be reused by other organizations that could have benefited from receiving the repurposed storage device. Rec FYI

During the requirements phase, other types of media that will be used to create, capture, or transfer information used by the system should be identified. This analysis balances business needs and confidentiality risks in compliance with FIPS 200 [3]. While media sanitization and information disposition activities primarily occur during the disposal phase of the system life cycle, many types of media containing data will be transferred outside of the positive control of the organization throughout the life of an information system (e.g., for maintenance, system upgrades, or during a configuration update). Rec

2.1. Need for Proper Media Sanitization and Information Disposition

Media sanitization is key to ensuring confidentiality, which is defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [22]. Additionally, "a loss of confidentiality is the unauthorized disclosure of information" [2]. Def

The unauthorized disclosure of sensitive and/or regulated information often constitutes the basis of a data breach, which can necessitate undesirable data breach notifications and other remedies. In some jurisdictions, simply losing control of sensitive information without disclosure is enough to be considered a data breach. Understanding where this sensitive information is stored and tracking the media on which it is stored can be important guards against data breaches. FYI

In order for organizations to have appropriate controls on the information for which they are responsible, they must properly safeguard used media. Illicit information collection can result from improperly disposed hard copy media, the acquisition of improperly sanitized electronic media, or keyboard and laboratory reconstruction of media sanitized in a manner that is not commensurate with the confidentiality of information stored on that media. Media flows in and out of organizational control through recycle bins in paper form, out to vendors for equipment repairs, and swapped into other systems in response to hardware or software failures. This potential vulnerability can be mitigated by properly understanding where information is located and how to protect it. Rec FYI

2.2. Types of Media

For the purposes document, there are two primary abstract types of media in common use: Def

- **Hard copy.** Hard copy media refers to physical representations of information, typically paper printouts. However, printer and facsimile ribbons, drums, and platens are also 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. Def
- **Information storage media (ISM).** ISM commonly[2] takes the form of: Def
    - Devices that contain 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, and office equipment
    - Systems that provide "virtual" or "logical" storage that abstracts the underlying electronic media (e.g., cloud storage, object storage)

  ISM can be volatile/non-persistent storage (i.e., fails to retain its contents after power is removed) or non-volatile/persistent storage (i.e., retains its contents after power is removed). This latter type of ISM is where most organizations should focus their sanitization efforts. Rec

2.3. Target of Sanitization

In general, sanitization safeguards the confidentiality of sensitive information that is stored on media by eliminating either the information on the media or the underlying media itself. This sensitive information is the target of sanitization activities. When considering hard copy, all sanitizations' activities focus on the proper elimination of the media. For ISM, sensitive information is stored as data on media and can constitute some or all the user data stored on the storage device or media. If the target data cannot be surgically sanitized, sanitization operations may be expanded to cover all user data. FYI

Some forms of ISM may contain more physical storage than the user addressable capacity (e.g., overprovisioning) for endurance and performance purposes. For example, a drive may have 1024 GB of total physical capacity but only 900 GB of available capacity (i.e., user accessible storage). However, user data may be stored on the full 1024 GB because of the overprovisioning mechanisms in the drive. In such a situation, the entire contents of the ISM may need to be sanitized.

[2] There are other forms of storage (e.g., DNA-based, ceramic/glass-based) that may exist for long-term preservation applications, but they are not widely available.

2.4. Factors Influencing Sanitization and Disposal Decisions

When making sanitization decisions for ISM, several factors should be considered along with the security categorization of the system confidentiality. The cost versus benefit trade-off of a sanitization process should be understood prior to a final decision. For instance, it may be more cost-effective to destroy rather than degauss inexpensive media, such as diskettes. Organizations retain the ability to increase the level of sanitization applied if that is reasonable and indicated by an assessment of the existing risk. Rec

Organizations should consider other factors, including: Rec

- The types (e.g., optical non-rewritable, magnetic) and sizes (e.g., megabyte, gigabyte, terabyte) of the media storage to be sanitized
- The confidentiality requirement for the data stored on the media
- Whether the media will be processed in a controlled area
- Whether the sanitization process should be conducted within the organization or outsourced
- The anticipated volume of media to be sanitized by type
- The availability of sanitization equipment and tools
- The training level of personnel with sanitization equipment/tools
- How long sanitization will take
- The cost of sanitization when considering tools, training, verification, and re-entering media into the supply stream

3. Summary of Sanitization Methods

The level of effort applied when attempting to retrieve data may vary widely. A party may attempt simple keyboard attacks without the use of specialized tools, skills, or knowledge, or they may have extensive capabilities that enable them to apply state-of-the-art laboratory techniques.[3]

Users of this guide should categorize the information to be disposed of, assess the nature of the medium on which that information is recorded, assess the risk to confidentiality, and determine future plans for the media. The organization can then choose the appropriate method of sanitization. The selected method should be assessed based on applicable factors (e.g., cost, environmental impact), and a decision should be made that best mitigates the risk to confidentiality and satisfies other constraints imposed on the process. Rec Rec

3.1. Sanitization Methods

Several different methods can be used to sanitize media, including clear (see Sec. 3.1.1), purge (see Sec. 3.1.2), and destroy (see Sec. 3.1.3). One or more sanitization techniques may be available for each method. FYI

ISM sanitization techniques take one of the following forms: FYI

- **Logical techniques.** Software or other tools are used over an interface to replace data in a systematic manner, issue specific commands to cause data to be eliminated, or eliminate access to the data. The confidentiality protection can vary significantly, depending on the specific technique. Logical sanitization leaves the ISM in a usable state. FYI
- **Physical techniques.** External physical measures are applied to eliminate data or the ISM. With few exceptions, physical techniques typically involve some form of destruction. FYI

Technology-specific sanitization techniques are out of scope for this document. FYI

3.1.1. Clear

Clear is a method of sanitization that applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple, non-invasive data recovery techniques using the same interface that is available to the user (e.g., host interface). The clear sanitization method is *not* appropriate for hard copy under any conditions but may be appropriate for ISM. Def

Clear is typically applied through the standard read and write commands to the ISM, such as by rewriting with a new value or using a menu option to reset the device to the factory state if FYI

[3] "State-of-the-art laboratory techniques" refer to the most advanced and innovative methods currently available for performing experiments, analyses, and procedures within a laboratory setting. Such a capability is assumed to be available to a party (e.g., nation-state actor) that desires the ability to recover sensitive data that has been sanitized.

rewriting is not supported. Clear sanitization operations typically have no impact on the usability of the ISM.

One approach to clear is to use software or hardware products to overwrite user-addressable storage space on the ISM with non-sensitive data using the standard read and write commands for the device. This process may include overwriting both the logical storage location of a file (e.g., file allocation table) and all user-addressable locations. The security goal of the overwriting process is to replace target data with non-sensitive data. Overwriting typically hinders the recovery of data even if state-of-the-art laboratory techniques are applied to attempt to retrieve the data. FYI

In the past, hard drives were often erased using multiple overwrite passes (e.g., based on DoD 5220.22-M [21]) with specific binary patterns (e.g., a pattern of all zeros). The number of passes ranged from a single pass to as high as 39. The binary pattern could change for each pass, and there could be verification after some or all of the overwrite passes. Such practices should be avoided as very little confidentiality protection is achieved. Instead, a more secure sanitization method in the form of purge (see Sec. 3.1.2) or destroy (see Sec. 3.1.3) should be used. Rec Rec

Overwriting cannot be used for damaged or non-rewriteable ISM and may not address all areas of the device where sensitive data may be retained. The ISM's 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 in which sensitive data has been stored using the native read and write interface.

Users who have become accustomed to relying on overwrite techniques on magnetic ISM and who have continued to apply these techniques as ISM types evolved (e.g., to flash memory-based devices) may be exposing their data to increased risk of unintentional disclosure. Although the host interface may be the same or very similar across devices with varying underlying ISM types, sanitization techniques must be carefully matched to the ISM.

Alternatively, the ISM may support dedicated sanitize commands that address all storage areas more effectively. The use of such commands results in a trade-off because they require trust and assurance from the vendor that the commands have been implemented as expected.

The clear operation may vary contextually for ISM other than dedicated storage devices, where the device (e.g., a basic cell phone, a piece of office equipment) only provides the ability to return the device to its factory state (e.g., deleting the file pointers) and does not directly support the ability to rewrite or apply ISM-specific techniques to the non-volatile storage contents. If rewriting is not supported, manufacturer resets and procedures that do not include rewriting may be the only option to clear the device and associated ISM. 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.

3.1.2. Purge

Purge applies physical or logical techniques that make the recovery of target data infeasible using state-of-the-art laboratory techniques but preserves the ISM in a potentially reusable state. Def The purge sanitization method is *not* appropriate for hard copy under any conditions but may be appropriate for ISM.

Logical purging techniques can vary by ISM and include overwrite, block erase, and cryptographic erase (see Sec. 3.2) through the use of dedicated, standardized device sanitize commands that apply ISM-specific techniques to bypass the abstraction inherent in typical read and write commands. Careful selection of the purge technique increases the likelihood of preserving the storage device in a usable state. FYI

Physical purging techniques traditionally included degaussing, which has become more complicated as magnetic ISM evolves, and some emerging variations of magnetic recording technologies incorporate ISM with higher coercivity (i.e., magnetic force) [19]. As a result, existing degaussers [20] may not have sufficient force to effectively degauss such ISMs. Additionally, degaussing may only damage some types of ISM, rendering them inoperable, but fail to sanitize the target data. Other physical purging techniques may also exist.

Degaussing renders a legacy magnetic device purged when the strength of the degausser is carefully matched to the ISM 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 magnetic storage devices that also contain non-volatile, non-magnetic storage. Rec Degaussing renders many types of devices unusable, making it a potential destruction technique. FYI

For an ISM that takes the form of logical/virtual storage (e.g., cloud storage), cryptographic erase (see Sec. 3.2) may be the only viable option. FYI Typically, the underlying physical ISM is abstracted such that the data owner has no direct access to the physical ISM, and sanitization on them is impossible and/or practical. As such, organizations should clearly understand their purge options and the effectiveness of the technique prior to storing sensitive data on such ISMs. Rec

3.1.3. Destroy

Destroy renders target data recovery infeasible using state-of-the-art laboratory techniques and results in the subsequent inability to use the ISM for the storage of data. Def The destroy sanitization method is appropriate for all hard copy and most ISM, except for logical/virtual storage.

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 access or recovery is infeasible using state-of-the-art laboratory techniques. FYI The application of destructive techniques may be the only option when the ISM fails and other clear or purge techniques cannot be effectively applied to the ISM.

The following physical destructive techniques are commonly associated with the destroy Def sanitization method:

- *Disintegrate.* Process that completely destroys the media by breaking, separating, or decomposing (e.g., dissolving with acid) media into its constituent elements, parts, or small particles such that there is nothing or very little of it that is recognizable after the process.
- *Incinerate*. Process that completely destroys the media by burning it to ash.
- *Melt*. Process that completely destroys the media by liquefying it (i.e., loses intactness or solidness), generally through the application of extreme heat.
- *Pulverize.* Process that completely destroys the media by reducing it to a fine powder or dust through crushing, grinding, or other mechanical means.
- *Shred*. Process that completely destroys the media by cutting or tearing it into small particles.

Techniques like bending, cutting, or some emergency procedures (e.g., using a firearm to shoot FYI a hole through a storage device) may only partly damage the ISM, leaving portions of it accessible using advanced laboratory techniques.

As the density of data and the hardness of the component materials increase on an ISM, certain destructive techniques may become ineffective. Pulverize and shred techniques for ISM should Rec be avoided for anything but the lowest security categories of data.

3.2. Use of Cryptography and Cryptographic Erase

Many storage manufacturers have released storage devices with integrated encryption and Def 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 capabilities, which 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 Def target data's encryption key. This leaves only the ciphertext remaining on the ISM, effectively sanitizing the data by preventing read-access. Without the encryption key, the target data is unrecoverable. The level of effort needed to decrypt this data without the encryption key then FYI is the lesser of the security strength of the cryptographic key or the security strength of the cryptographic algorithm and mode of operation used to encrypt the data.

FYI

If strong cryptography is used, sanitization of the target data is reduced to sanitization of the encryption keys 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 the constraints identified in these guidelines.

Rec

Federal agencies must use FIPS 140-validated encryption modules[4] in order to have assurance that the conditions stated above have been verified for the SED.

FYI

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 taking more time. CE can also be used as a supplement or addition to other sanitization approaches. Since data is left untouched for CE, sanitization assurance is obtained by observing the due diligence steps outlined in Sec. 3.1.1, Sec. 3.1.2, Sec. 3.1.3, and Appendix B.

3.2.1. When Not To Use CE To Purge Media

Rec

Do not use CE:

- To purge ISM if the encryption was enabled after sensitive data was stored on the device without having been sanitized first
- If it is unknown whether sensitive data was stored on the device without being sanitized prior to encryption

3.2.2. When to Consider Using CE

Rec

Consider using CE when:

- All of the data intended for CE is encrypted prior to storage on the ISM, including the data and virtualized copies.
- The encryption key's storage location on the ISM is known (e.g., target data's encryption key, an associated wrapping key) and those areas can be sanitized using the appropriate ISM-specific sanitization technique.
- All copies of the encryption keys used to encrypt the target data are sanitized.
- The target data's encryption keys are encrypted with one or more wrapping keys, and the corresponding wrapping keys can be sanitized.
- The user can clearly identify and use the commands provided by the device to perform the CE operation.

3.2.3. Additional CE Considerations

If the encryption key exists outside of the storage device (e.g., due to backup or escrow), it could potentially be used in the future to recover data stored on the encrypted ISM.

Rec

CE should only be used as a sanitization method when the organization is confident that the encryption

[4] NIST maintains lists of validated cryptographic modules and cryptographic algorithms.

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

Sanitization using CE should not be trusted on devices that have been backed up or escrowed unless the organization has a high level of confidence regarding how and where the keys were stored and managed outside of the device. Such backed up or escrowed copies of data, credentials, or keys should be subject to a separate device sanitization policy. Rec

Appendix C provides a list of applicable considerations and a sample for how vendors could report the mechanisms implemented. Users who want to implement CE should seek reasonable assurance from the vendor (e.g., the vendor's report described in Appendix C) that the considerations identified here have been addressed and only use FIPS 140-validated cryptographic modules. Rec

4. Media Sanitization Program

A storage sanitization program can help ensure the consistent and appropriate disposal of storage assets and avoid data breaches due to mishandling. ISO/IEC 27040 [16] states that storage sanitization should be an element of the organization's data governance process, which should also include: FYI Rec

- Policies that specify the expectations associated with storage asset disposal (i.e., transfer, reuse, elimination) and minimum acceptable sanitization methods
- Identifying the scope and sanitization decision criteria
- Performing storage sanitization
- Determining the adequacy of the sanitization performed
- Identifying the necessary records or evidence (i.e., documentation) to meet compliance obligations

4.1. Storage Sanitization Policy

The presence or absence of a storage sanitization policy can significantly impact the effectiveness of an organization's storage sanitization activities. Such a policy should address the following: Rec

- Alignment of the organization's data classification scheme (e.g., low, medium, and high security categorizations) with minimum acceptable sanitization methods (i.e., clear, purge, and destroy)
- Requirements for the disposal and/or reuse of storage assets
- Expected outcomes from storage sanitization activities (e.g., identification of specific, acceptable sanitization techniques [14])
- Documentation or evidence associated with sanitization activities (see Sec. 4.6)
- The identification of roles and responsibilities (see Sec. 4.7) and personnel competencies, skills, and training
- The use of sanitization tools, including equipment calibration, testing, and maintenance
- Type of assurances (e.g., guarantees, assessment results, formal certifications) that the ISM vendor should provide for the sanitization capabilities

4.2. Sanitization Scope

Unclassified ISM that is never used in a classified information system and does not contain For Official Use Only (FOUO) information, Privacy Act information, or PII does not require sanitization [18]. FYI

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

On ISMs with integrated encryption capabilities, CE provides a unique mechanism for supporting some forms of partial sanitization. These devices may 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 ISMs, the level of assurance depends on both vendor implementation and confidence that the data was only stored in areas that can be reliably sanitized. Data may be stored outside of these regions if the user or software on the system moved data outside of the designated area on the ISM or if the ISM stored data in a manner that was 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 of this approach and make appropriate decisions that balance missions and specific use cases. Rec For example, a drive in a data center may contain customer data from multiple customers. When one customer discontinues service and another begins storing data on the same ISM, the organization may choose to apply partial sanitization in order to retain the data of other customers. The organization may also 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 that is available for that specific ISM. If the alternative to partial sanitization is not performing sanitization at all, partial sanitization provides benefits that should be considered. Rec

4.3. Storage Sanitization and Disposition Decision Framework

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. The data confidentiality level should be identified using the procedures described in FIPS 199 [2]. Rec Additionally, SP 800-60r2 [8] describes mapping information types to security categories.

While most devices support some form of clear, not all ISMs have a reliable purge mechanism. For moderate confidentiality data, the ISM owner may choose to accept the risk of applying clear techniques to the ISM, acknowledging that some data may be retrievable 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 ISM (either within the organization or by selling or donating the ISM), the cost of an ISM, or the difficulties in physically destroying some types of ISM. The risk decision should include the potential consequences of information disclosure, the cost of information retrieval and its efficacy, the cost of sanitization and its efficacy, and how long the data will remain sensitive. These values may vary between different environments. Rec

Organizations can refer to Fig. 1 and the descriptions in this section to make sanitization decisions that are commensurate with the security categorization of the confidentiality of information contained on their media.

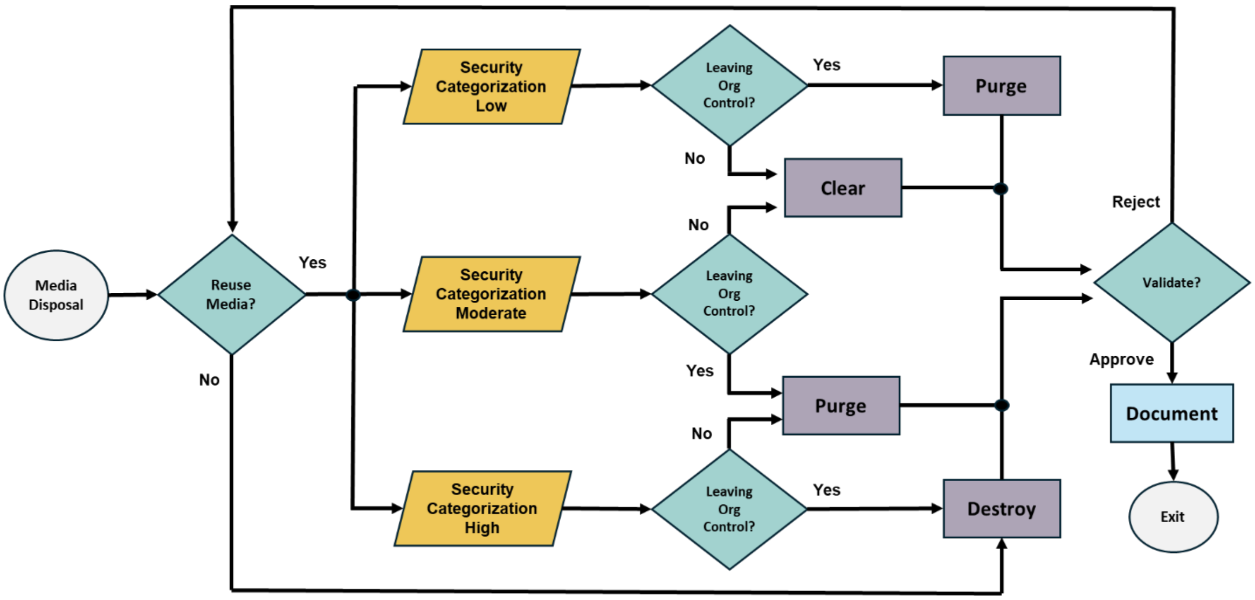

Fig. 1. Sanitization and disposition decision flow

The decision process is based on the confidentiality of the information rather than the type of media. Once the organization decides what type of sanitization is best for their individual case, the media type will influence the technique used to achieve the sanitization goal.

4.3.1. Information Decisions in the System Life Cycle

The need and methods for conducting media sanitization should be identified and developed before arriving at the disposal phase in the system life cycle. ISM sanitization controls should be developed, documented, and deployed when the initial system security plan is developed [13]. One of the key decisions that will affect the ability to conduct sanitization is choosing what ISMs will be used within the system. Although this is mostly a business decision, system owners must understand that this decision will affect the types of resources needed for sanitization throughout the entire system life cycle. Rec Rec

An organization may ask a product vendor for assistance in identifying ISMs that contain sensitive data, which is typically documented in a Statement of Volatility (SoV). An SoV 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 when comparing statements across vendors because vendors may state volatility details differently. Rec

A list of device-specific characteristics of interest for the application of sanitization techniques is included in Appendix C. These characteristics can be used to drive the types of questions that ISM users should ask vendors. 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 an ISM can help a user decide whether or not available degaussers can effectively degauss the ISM. FYI

Organizations should take care when identifying ISM for sanitization. Many items used will contain multiple forms of ISM that may require different methods of sanitization. For example, a desktop computer may contain a hard drive, motherboard, RAM, and ROM, and mobile devices may contain on-board volatile memory and non-volatile removable memory. Rec

The increasing availability of rapidly applicable techniques (e.g., CE) provides opportunities for organizations to reduce the risks of inadvertent disclosure by combining sanitization technologies and techniques. For example, an organization could choose to apply CE at a user's desktop before sending the ISM to a sanitization facility in order to reduce risk and exposure.

When an ISM is repurposed or reaches the end of its life, the organization executes the system life cycle sanitization decision for the information on the ISM. Disposal without sanitization should be considered only if information disclosure would have no impact on the organization's mission, would not result in damage to organizational assets, and would not result in financial loss or harm to any individuals. 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 ISM 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. Rec

4.3.2. Determination of Security Categorization

Early in the system life cycle, a system is categorized using the guidance found in FIPS 199 [2], SP 800-60r2 [8], or CNSSI 1253 [13], 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.

Organizations may have information that is not associated with any categorized system. This information is often hard copy internal communications, such as memoranda, white papers, and presentations. This information may sometimes be considered sensitive, such as internal disciplinary letters, financial or salary negotiations, or strategy meeting minutes. Organizations should label these ISMs with their internal operating confidentiality levels and associate a type of sanitization described in this publication. Rec

4.3.3. Reuse of Media

A key sanitization decision is whether the media is planned for reuse (e.g., internal transfer, donations, refurbishment, recycling). If the media is not intended for reuse within or outside of an organization due to damage or another reason, the simplest and most cost-effective sanitization method may be to destroy the media. FYI

4.3.4. Control of Media

Organizational sanitization decisions are influenced by who has control and access to the media. This aspect must be considered when media leaves organizational control. Rec

Media control may be transferred when ISMs are returned from a leasing agreement, donated, or resold to be reused outside of the organization. For example:

- ISMs under organizational control
    - ISMs that are turned over for maintenance are still considered to be under organizational 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 to be under the control of the organization.
- ISMS not under organizational control (i.e., external control)
    - ISMs that are being exchanged for warranty, cost rebates, or other purposes and will not be returned to the organization are considered to be out of organizational control.

4.3.5. Data Protection Level

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

4.3.6. 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, then an effective, risk-based decision can be made on the appropriate and needed level of sanitization. Again, certain factors and media types might cause the level of sanitization to change. For example, purging paper copies is generally not recommended, so destroying them would be an acceptable alternative.

Once a sanitization decision has been made, the organization should record the decision and ensure that a process and proper resources are in place to support that decision. The process includes the act of sanitization as well as verification, including decisions, actions, resources, and critical interfaces with key officials. Rec

4.4. Performing Sanitization

After the requirement to sanitize media has been established, the sanitization should be performed based on the selected sanitization method (i.e., clear, purge, or destroy) and in a manner that complies with IEEE 2883 [14][5] or a standard that is identified as acceptable by organizational policy (e.g., NSA/CSS Policy 6-22 [18], NSA/CSS Policy Manual 6-12 [17]). Depending on the media type and selected sanitization method, there may be multiple sanitization technique options. The option that provides the most confidentiality protection should be used. When the purge method of CE is used for an ISM, Sec. 3.2 and Appendix B should be consulted for additional considerations or requirements. Rec

As part of performing the sanitization, certain details will need to be captured, including the results/outcomes of the sanitization (see Sec. 4.5), the information necessary to document the sanitization (see Sec. 4.6), and other relevant information. FYI

The proper initial configuration of each ISM helps ensure that the sanitization operation is as effective as possible. The individuals performing the sanitization are encouraged to check manufacturer recommendations and guides, such as the DISA Security Technical Implementation Guides (STIGs) [23], for additional information about recommended settings. FYI Sanitization techniques typically play no role in configuring ISMs. A frequent misconception is that a sanitized ISM will resemble a factor fresh drive (i.e., in a factory default state), but this is often not the case. Additional configuration changes may be necessary before the ISM can be readily reused.

4.5. Sanitization Assurance

Per ISO/IEC 27040 [16], verifying the adequacy or effectiveness of sanitization outcomes is an important aspect of a sanitization program. FYI The results of attempted sanitization techniques are inspected, and a decision on the adequacy of the results is made. If the outcomes are expected and appropriate, the sanitization is accepted. If outcomes are not acceptable, then sanitization is repeated. Repeated sanitization should recheck the reuse of media because a previous sanitization technique may have rendered the media unusable or inoperable. Rec

[5] The IEEE 2883 series provides additional information about selecting appropriate sanitization methods for use, as well as technology-specific sanitization techniques.

4.5.1. Sanitization Verification

The goal of sanitization verification is to determine the outcome of the sanitization technique used during the sanitization operation. The sanitization results should be inspected to verify that the sanitization technique was completed successfully. For both hard copy and ISMs, this verification involves inspecting the remnants of a destruction technique. Rec

For non-destructive sanitization methods for ISM, verification can be more complex and typically depends on the type of ISM. Clear and logical purge techniques that involve tools and systems can be verified by checking the completion status of the tools and identifying errors, anomalies, and the health of the ISM. For physical purge techniques, the equipment performing the sanitization should be checked to confirm that it completed its operation successfully. The ISM may not be in a usable state until certain device software and configurations are reestablished, so there may be limitations on further inspections of the ISM. Rec

Unless explicitly required by the organization, elaborate ISM sampling of contents (e.g., full or representative) after clear or purge sanitization is not necessary. FYI

4.5.2. Sanitization Validation

The goal of sanitization validation is to ensure that the target data was effectively sanitized. Sanitization validation results in a decision to either approve the sanitization as being effective or reject it, which would require repeating the sanitization method using a different sanitization technique or escalating to a more secure sanitization method. FYI

The results of the sanitization verification are considered (see Sec. 4.5.1). Any identified errors, anomalies, or other issues should be analyzed, and risks to data confidentiality should be assessed. Unacceptable data confidentiality risks associated with the sanitization operation should result in the sanitization not being accepted (i.e., rejected) as sufficient to ensure the confidentiality of sensitive data (i.e., an additional sanitization method is needed). Rec

The effectiveness of the sanitization may be called into question by several other considerations, including:

- The ISM may appear fully functional, but some portion of the ISM may no longer be accessible through the ISM's interface due to errors or performance conditions.
- The selected sanitization method and/or technique is not appropriate for the media or the security category of the data. For example, a sanitization operation that degausses an SSD is unlikely to sanitize any sensitive data.
- The sanitization may have been performed by unqualified personnel or used tools or equipment that were not approved or were improperly calibrated.
- The outcome does not meet minimum requirements. For example, a shredder is used on an optical disc and results in pieces that are 50 % larger than what is acceptable to the organization. The sanitization technique completed successfully but is not considered effective.

- The scope of the sanitization (i.e., target data) was too narrowly focused. For example, an ISM that employs overprovisioning is cleared using simple writes to overwrite existing contents and potentially leaves a substantial amount of user data unchanged.

The validation process considers the sanitization outcomes and the sensitivity of the target data and decides (shown as "Validate" in Fig. 1) whether the target data has been sanitized to an acceptable level (i.e., the organization accepts any residual risks). In other words, the level of effort that is necessary to potentially gain access to the data after the sanitization operations is deemed sufficient to ensure the confidentiality of the data. FYI

4.6. Documentation

Following sanitization, a certificate of media disposition should be completed for each piece of ISM that has been sanitized. A certification of media disposition may be a physical (e.g., piece of paper) or electronic record of the action taken. For example, ISMs include bar codes on the label for the 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 ISM is sanitized. Automatic documentation can be important as some systems make physical access to the ISM very difficult. Rec

The decision to complete a certificate of media disposition and determining how much data to record depend on the confidentiality level of the data on the ISM. For a large number of ISM 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: Rec

- Manufacturer
- Model
- Serial number
- Organizationally assigned media or property number (if applicable)
- Media type (e.g., magnetic, flash memory, hybrid)
- Media source (e.g., user, computer)
- Pre-sanitization confidentiality categorization (optional)
- Sanitization method (i.e., clear, purge, destroy)
- Sanitization technique (e.g., degauss, overwrite, block erase, crypto erase)
- Tool used, including version
- Verification method (e.g., full, quick sampling)
- Post-sanitization confidentiality categorization (optional)
- Post-sanitization destination (if known)

- Information of individuals performing verification and validation:
    - Name of person
    - Position/title of person
    - Date
    - Location
    - Contact information (e.g., phone number)
    - Signature

Optionally, an organization may choose to record information on data backups, including where the backs are stored. Appendix D provides an example Certification of Sanitization form. FYI

If the ISM has been successfully validated (see Sec. 4.5) and the sanitization results in a lower confidentiality level for the storage device, all markings on the device that indicate the previous confidentiality level should be removed. A new marking that indicates 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 to prevent the reintroduction of sensitive data. Rec

The value of a certification of media disposition depends on the organization's handling of ISM over the media's life cycle. The organization can most effectively identify how well media sanitization is being applied across the enterprise if records are maintained when the ISM is introduced to the environment, when the ISM leaves the place where it was last used, and when it reaches the sanitization destination. If there is a breakdown in tracking at locations other than the sanitization destination, sanitization records will 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.

4.7. Roles and Responsibilities

This section describes example roles and responsibilities for sanitizing media.

4.7.1. Program Managers/Agency Heads

Program managers are responsible for establishing an effective information security governance structure, including the organization's computer security program and its overall goals, objectives, and priorities. Agency heads are responsible for providing adequate resources to the program to ensure its success. FYI Allocated resources should correctly identify the types and locations of information. Rec

4.7.2. Chief Information Officer (CIO)

The CIO[6] is responsible for promulgating the information security policy, which includes information disposition and media sanitization. As the information custodian, the CIO ensures that organizational and/or local sanitization requirements follow the guidelines in this document. FYI

4.7.3. Information System Owner

The information system owner[7] is responsible for ensuring that maintenance or contractual agreements are in place and sufficiently protect the confidentiality of the system ISM and information commensurate with the impact of disclosure. FYI

4.7.4. Information Owner/Steward

The information owner is responsible for ensuring the appropriate supervision of on-site ISM maintenance by service providers. The information owner should fully understand the sensitivity of the information under their control, its confidentiality, and the basic requirements for media sanitization. FYI Rec

4.7.5. 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. FYI

4.7.6. System Security Manager/Officer

The system security manager/office often is responsible for day-to-day security implementation and administration. Although not normally part of the computer security program management office, this person is responsible for coordinating the security efforts of particular systems. This role is sometimes referred to as the Computer System Security Officer or the Information System Security Officer. FYI

[6] 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.
[7] 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 information system owners as “program managers” or “business/asset/mission owners.”

4.7.7. Property Management Officer

The property management officer is responsible for identifying and tracking sanitized ISMs that are redistributed within the organization, donated to external entities, or destroyed. FYI

4.7.8. Records Management Officer

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

4.7.9. Privacy Officer

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

4.7.10. Users

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

References

[1] National Institute of Standards and Technology (2019) Security Requirements for Cryptographic Modules. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publications (FIPS) NIST FIPS 140-3.Federal Information Processing Standards (FIPS) Publication 140-3, *Security Requirements for Cryptographic Modules*, March 22, 2019 https://doi.org/10.6028/NIST.FIPS.140-3

[2] National Institute of Standards and Technology (2004) Standards for Security Categorization of Federal Information and Information Systems. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publications (FIPS) NIST FIPS 199. https://doi.org/10.6028/NIST.FIPS.199

[3] National Institute of Standards and Technology (2006) Minimum Security Requirements for Federal Information and Information Systems. (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publications (FIPS) NIST FIPS 200. https://doi.org/10.6028/NIST.FIPS.200

[4] Swanson M, Hash J, Bowen P (2006) Guide for Developing Security Plans for Federal Information Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-18r1. https://doi.org/10.6028/NIST.SP.800-18r1

[5] Dworkin M (2010) Recommendation for Block Cipher Modes of Operation: Methods and Techniques. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-38A. https://doi.org/10.6028/NIST.SP.800-38A-Add

[6] Joint Task Force (2020) Security and Privacy Controls for Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53r5. Includes updates as of December 10, 2020. https://doi.org/10.6028/NIST.SP.800-53r5

[7] Joint Task Force (2022) Assessing Security and Privacy Controls in Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-53Ar5. https://doi.org/10.6028/NIST.SP.800-53Ar5

[8] Joint Task Force (2024) Guide for Mapping Types of Information and Systems to Security Categories. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-60r2 iwd. https://doi.org/10.6028/NIST.SP.800-60r2.iwd

[9] Ross R, Winstead M, McEvilley M (2022), Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v1r1. https://doi.org/10.6028/NIST.SP.800-160v1r1

[10] Barker E, Kelsey J (2015) Recommendation for Random Number Generation Using Deterministic Random Bit Generators. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-90Ar1. https://doi.org/10.6028/NIST.SP.800-90Ar1

[11] Scarfone K, Souppaya M, Sexton M (2007) Guide to Storage Encryption Technologies for End User Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-111. https://doi.org/10.6028/NIST.SP.800-111

[12] McCallister E, Grance T, Scarfone K (2010) Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-122. https://doi.org/10.6028/NIST.SP.800-122

[13] Committee on National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, August 1, 2022. Available at https://www.cnss.gov/CNSS/issuances/Instructions.cfm

[14] IEEE Standards Association (2022) *IEEE 2883-2022 – IEEE Standard for Sanitizing Storage* (IEEE Standards Association, Piscataway, New Jersey). Available at https://standards.ieee.org/ieee/2883/10277/

[15] International Organization for Standardization/International Electrotechnical Commission (2025) *ISO/IEC 19790:2005 – Information security, cybersecurity and privacy protection – Security requirements for cryptographic modules* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/82423.html

[16] International Organization for Standardization/International Electrotechnical Commission (2024) *ISO/IEC 27040:2024 – Information technology — Security techniques — Storage security* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/80194.html

[17] National Security Agency/Central Security Service (2020) NSA/CSS Storage Device Sanitization and Destruction Manual. NSA/CSS Policy Manual 9-12, December 4, 2020.

[18] National Security Agency/Central Security Service (2019) Handling of NSA/CSS Information Storage Media. NSA/CSS Policy 6-22, November 21, 2019. Available at https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/NSA-CSS-Policies/#handling-sanitization-of-storage-media

[19] NSA/CSS Requirements for Magnetic Degaussers, May 2021. Available at https://www.nsa.gov/portals/75/documents/resources/everyone/media-destruction/NSA_CSS%20Requirements%20for%20Magnetic%20Degaussers.pdf?ver=GSo5EEFg-tTBI6fS8Dahmg%3D%3D

[20] National Security Agency/Central Security Service (2025) *NSA Evaluated Products Lists (EPLs)*. Available at https://www.nsa.gov/Resources/Media-Destruction-Guidance/NSA-Evaluated-Products-Lists-EPLs/

[21] U.S. Department of Defense (2005) “Clearing and Sanitization Data Storage,” Table C8.T1 in “National Industrial Security Program: Operating Manual”, DoD 5220.22-M-Sup-1, February 1, 2005.

[22] “Definitions,” Title 44 U.S. Code, Sec. 3542. 2006 ed. Supp. 5. Available at https://www.gpo.gov/

[23] Security Technical Implementation Guides (STIGs). Available at https://public.cyber.mil/stigs/

Appendix A. Glossary

bend
The use of a mechanical process to alter the physical shape of the storage media and make reading the media difficult or infeasible using state-of-the-art laboratory techniques.

clear
A method of sanitization that applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple, non-invasive data recovery techniques using the same interface that is 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.

cryptographic erase (CE)
A purge sanitization technique in which the encryption key (i.e., either the MEK or the KEK protecting the MEK) for the encrypted target data is sanitized, making recovery of the decrypted target data infeasible.

cut
The use of a tool or physical technique to break the surface of 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.

data
Material 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 will render the drive permanently unusable since these drives store 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 to store 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
A release outcome following the decision that media does not contain sensitive data. This occurs if the media never contained sensitive data or after sanitization techniques are applied and the media no longer contains sensitive data.

electronic media
Media on which data is recorded via an electrically based process.

hard disk
A rigid magnetic disk that is permanently fixed within a drive unit and used to store data. It could also be a removable cartridge that contains one or more magnetic disks.

incineration
A physically destructive method of sanitizing media. The act of burning completely to ashes.

information
A meaningful expression of data.

information storage media (ISM)
Data storage objects that are capable of being read from or written to by an information system, such as diskettes, optical disks, removable media, hard disks, SSDs, and other less common forms (e.g., DNA-based, ceramic/glass-based).

key encryption key (KEK)
A cryptographic key that is used for the encryption or decryption of other keys to provide confidentiality protection for those keys. Also known as a key-wrapping key.

magnetic media
A class of storage device that only uses magnetic storage media for persistent storage.

media encryption key (MEK)
A symmetric cryptographic key used to encrypt data stored on a specific piece of media (e.g., a hard drive or SSD).

media sanitization
The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

medium
Material on which data may be recorded, such as paper, punched cards, film, 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 liquid state, generally through 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 that applies physical or logical techniques to render target data recovery infeasible using state-of-the-art laboratory techniques.

read
A fundamental process in an information system that only results in the flow of information from storage media to a requester.

read-only memory (ROM)
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 that remains on storage media.

sanitization
A process or method to sanitize.

sanitization method
Actions that can be taken to sanitize media, such as clear, purge, and destroy.

sanitization technique
A technology-specific approach associated with a sanitization method that can be used to sanitize a specific type of media.

sanitize
To render access to target data on the media infeasible for a given level of effort.

security strength
The amount of computational work required to break a cryptographic algorithm or system, often measured in bits.

shred
A method of sanitizing media. The act of cutting or tearing into small particles.

solid-state drive (SSD)
A storage device that uses solid-state memory to store persistent data.

storage
The retrievable retention of data. Electronic, electrostatic, or electrical hardware or other elements onto which data may be entered and from which data may be retrieved.

target data
The stored, sensitive data to be eliminated by a sanitization operation.

validation
The process of determining whether a sanitization operation effectively sanitized the target data, resulting in a decision to either approve the sanitization as being effective or reject it, which requires repeating the sanitization method using a different sanitization technique or escalating to a more secure sanitization method.

verification
The process of inspecting the outcomes of a sanitization technique to determine whether it completed successfully.

write
A fundamental operation of an information system that only results in the flow of information from an actor to storage media.

Appendix B. Cryptographic Erase ISM Guidelines

B.1. Cryptographic Erase Considerations

The determination of whether to use CE on a given ISM depends on an organization's sanitization requirements as well as the end user's ability to determine whether the implementation offers sufficient assurance against future recovery of the data. The level of assurance is informed by the factors described in Table 1.

Table 1. CE considerations

Area	Considerations	Relevant Docs
Key Generation	The level of entropy of the random number sources and the quality of key generation procedures applied to the random data. This applies to the cryptographic keys and the wrapping keys (if any) affected by the cryptographic erase operation.	SP 800-90 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 to protect the target data.	FIPS 140-3[8] FIPS 197 SP 800-38A (not including electronic codebook (ECB)) SP 800-38E
Key Level and Wrapping	The key being sanitized might not be the media encryption key (MEK) but a key used to wrap (i.e., 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 cryptographic erase operation.	FIPS 197 SP 800-38A SP 800-38F SP 800-131A

Rec

Users who seek to leverage CE should identify and address the following mechanisms implemented by the storage device before relying on CE for media sanitization: Rec

1. **Make, model, version, or media type.** The product and versions to which the statement applies and the type of storage media that the ISM uses (e.g., magnetic, SSD, hybrid). Many ISMs store the target data (see Sec. 2.3) in several different media (e.g., a cache in addition to rotating platters in a hard drive).

2. **Key generation.** Identify whether a deterministic random bit generator (e.g., one listed in SP 800-90Ar1 [10]) was used and how it has been validated.

[8] Conformance testing for FIPS 140-3 is conducted within the framework of the Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP).

3. **Media encryption.** Identify the algorithm, key strength, mode of operation, and any applicable validations.

4. **Key wrapping.** Identify whether the MEK (either wrapped with a KEK or not) is directly sanitized or whether a key that wraps the MEK (i.e., a key encryption key [KEK]) is sanitized. A description of the wrapping techniques only applies if a KEK (and not the MEK) is sanitized. When provided, wrapping details should include the algorithm used, its strength, and (if applicable) its mode of operation.

5. **Media 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 keys on an ISM can have multiple wrapping activities (i.e., wrapping, unwrapping, and rewrapping) throughout the ISM's life cycle. Identify how the keys being sanitized are handled during wrapping activities that are not directly part of the CE operation. For example, a user may have received an SED that was always encrypting and can have simply turned on the authentication function. 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 ISM-dependent sanitization method for the key being sanitized. Some examples might include three inverted overwrite passes if the ISM is magnetic, a block erase for an SSD, or other media-specific techniques for other types of ISM.

8. **Key escrow or injection.** Identify whether the storage device supports key escrow or injection at or below the level of CE or whether the key has ever been escrowed from or injected into the storage device. Clearly identify whether the MEK is directly sanitized and only a KEK can be escrowed.

9. **Error condition handling.** Identify how the ISM handles error conditions that prevent the CE operation from fully completing, such as a defect encountered where an instance of the key to be sanitized is stored. For example, if the location where the key was stored cannot be sanitized, determine whether the CE operation can report success or failure to the user.

10. **Interface clarity.** Identify the host interface commands that support the features described in the statement. If the ISM supports the use of multiple MEKs, identify whether all MEKs are changed using the host interface commands available and any additional commands or actions necessary to ensure that all MEKs are changed.

B.2. Example Statement of CE Features

The following statements should be placed by the storage device vendor in an area that is accessible to potential users of a device, such as on the vendor's website or in product literature Rec *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+. Legacy Magnetic media.
2. **Key generation.** A DRBG is used as specified in SP 800-90A [10] 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 [5]. This device is FIPS 140-validated [1] with certificate [number].
4. **Key level and wrapping.** The MEK is sanitized directly during CE.
5. **Data areas addressed.** The ISM encrypts all data stored in the addressable space except for a pre-boot authentication and variable area and the device logs. Device log data is retained by the device following CE.
6. **Key life cycle management.** As the MEK moves between wrapped, unwrapped, and re-wrapped states, the previous instance is sanitized.
7. **Key sanitization technique.** Zeroization of the key, as described in ISO/IEC 19790 [15] (e.g., overwriting with all zeros, all ones, or random data).
8. **Key escrow or injection.** The ISM does not support escrow or injection of the keys at or below the level of the sanitization operation.
9. **Error condition handling.** If the ISM encounters a defect in a location where a key is stored, the ISM attempts to rewrite the location. The CE operations continues and reports success to the user if the operation is otherwise successful.
10. **Interface clarity.** The ISM has an interface that supports one or more CE commands that can be used sanitize the ISM, as described in the IEEE 2883 series [14].

Appendix C. Device-Specific Characteristics of Interest

Storage vendors implement a range of ISM types that can leverage the same standardized interface command sets. This can be useful when an organization has deployed drives from multiple vendors because it may be possible to use the same sanitization commands for specific interfaces without regard to the vendor. There may also be the same or similar commands across different interface types, but no assumptions should be made as to the functionality of these commands (i.e., the commands on two different interfaces may be the same, but they could perform very different sanitization operations). It is also important to verify the functionality of commands as the command name might imply a certain capability but not actually meet minimum requirements for the sanitization method. Some vendors may have implementations that apply techniques such as CE or block erase (for flash memory devices). 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 should be asked to provide information about how a specific device implements any dedicated sanitize commands supported by the device as well as compliance with standards such as IEEE 2883 [14]. 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:

Rec

Rec

- Media type (e.g., Legacy Magnetic, HAMR, magnetic shingle, SLC/MLC/TLC Flash Memory, hybrid)
    - Coercivity of any magnetic media to support an informed decision about whether to attempt to degauss the media
- Any supported sanitize commands and the following for each:
    - A list of any areas that are 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 D. Sample "Certificate of Sanitization" Form

This example certificate demonstrates 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 through a native application or by using a form with an automated data transfer utility (e.g., a PDF form with a button to send the data to a database or email address). If the records need to be referenced in the future, electronic records will likely provide the fastest search capabilities and the best likelihood of being reliably retained. FYI

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:	

Fig. 2. Certificate of Sanitization

Appendix E. Change Log

This publication revises SP 800-88r1 (2014) as follows: FYI

- Apart from Cryptographic Erase (CE), which is commonly used across all encrypted media, all sanitization technique details have been replaced with recommendations to comply with IEEE 2883, NSA specifications, or an organizationally approved standard.
- The document's focus has shifted from providing guidelines for making sanitization decisions to establishing an agency or enterprise media sanitization program
- Documents that were previously referenced in footnotes have been moved to the new "References" section and updated to refer to the latest revision. The Bibliography section was eliminated as many documents listed there were obsolete, and the documents referenced in the body of the text are now included in the "References" section.
- Appendices (Appendix A and C) that described media-specific sanitization techniques and tools were removed to improve the document's longevity. Sections that described trends in storage media (e.g., old Sec. 2.3) were also removed.
- The new sanitization process figure has an initial decision point focused on reusing media.
- Almost all "verification" language has been removed. Full/representative sampling is stated as not being needed unless required by the organization.
- Sanitization validation is described and focuses on checks (e.g., errors, anomalies, and other issues) to see whether the attempted sanitization was effective from a confidentiality and sensitivity perspective.
- The "clear" method was clarified such that multi-pass overwrite is not needed. This counters the DoD 5220.20-m language that mandates a certain number of overwrite passes and patterns.
- Laboratory attacks have been described.
- Logical versus physical sanitization techniques have been described.
- For CE, sanitizing a key has been clarified and is now based in ISO/IEC 19790 zeroization.
- For CE, there is now clarification regarding when the use of externally managed keys is potentially acceptable.
- The issue of trusting the vendor's implementation of sanitization techniques for clear and purge has been addressed.
- All content has been reformatted to follow the latest NIST technical report template.