NIST Special Publication 800
NIST SP 800-88r2

Guidelines for Media Sanitization

Ramaswamy Chandramouli
Eric A. Hibbard

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-88r2

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

NIST Special Publication 800
NIST SP 800-88r2

Guidelines for Media Sanitization

Ramaswamy Chandramouli
Computer Security Division
Information Technology Laboratory

Eric A. Hibbard
Samsung Semiconductor, Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-88r2

September 2025

U.S. Department of Commerce
Howard Lutnick, Secretary

National Institute of Standards and Technology
Craig Burkhardt, Acting Under Secretary of Commerce for Standards and Technology and Acting NIST Director

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on 2025-09-12
Supersedes NIST SP 800-88r1 (Revision 1) (December 2014) https://doi.org/10.6028/NIST.SP.800-88r1

How to Cite this NIST Technical Series Publication

Chandramouli R, Hibbard EA (2025) Guidelines for Media Sanitization. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-88r2. https://doi.org/10.6028/NIST.SP.800-88r2

Author ORCID iDs

Ramaswamy Chandramouli: 0000-0002-7387-5858
Eric Hibbard: 0009-0001-8112-1263

Contact Information

sp800-88-comments@nist.gov

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930

Additional Information

Additional information about this publication is available at https://csrc.nist.gov/pubs/sp/800/88/r2/final, including related content, potential updates, and document history.

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

Media sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. This guide will assist organizations and system owners in setting up a media sanitization program with proper and applicable techniques and controls for sanitization and disposal based on the sensitivity of their information.

Keywords

Cryptographic erase; ensuring confidentiality; media sanitization; media sanitization program; media types; sanitization methods; secure erase.

Reports on Computer Systems Technology

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

Patent Disclosure Notice

NOTICE: ITL has requested that holders of patent claims whose use may be required for compliance with the guidance or requirements of this publication disclose such patent claims to ITL. However, holders of patents are not obligated to respond to ITL calls for patents and ITL has not undertaken a patent search in order to identify which, if any, patents may apply to this publication.

As of the date of publication and following call(s) for the identification of patent claims whose use may be required for compliance with the guidance or requirements of this publication, no such patent claims have been identified to ITL.

No representation is made or implied by ITL that licenses are not required to avoid patent infringement in the use of this publication.

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. Thanks to their diligent and detailed reviews, we expect this document to serve as a useful guide for developing an effective media sanitization program.

Executive Summary

Protecting the confidentiality of information should be a concern for everyone, from federal agencies and businesses to home users. Media disposition and sanitization decisions need to consider the confidentiality obligations associated with recording or storing sensitive information on hard copy media or information storage media (ISM). To help ensure media disposition and sanitization are effective and traceable, consideration should be given to implementing a media sanitization program.

The modern storage environment is rapidly evolving. Data may pass through multiple organizations, systems, and ISM in its lifetime. Data propagation has continued to increase as the internet and data storage systems have moved toward a distributed cloud-based architecture. As a result, more parties are responsible for effectively sanitizing ISM (i.e., eliminating sensitive data), and the potential is substantial for sensitive data to be collected and retained on the ISM. This responsibility lies with organizations that are originators (i.e., sources), users, 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.

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 ISM that has left an organization without being sufficiently sanitized. Consequently, effective sanitization techniques and the tracking of ISM 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).

An organization may choose to dispose of ISM by charitable donation, internal or external transfer, or recycling if that ISM 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 ISM's final intended destination, organizations should use approved sanitization methods and techniques to ensure that no reconstructible residual representation of the sensitive data is stored on ISM that has left the control of the organization.

Sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort (i.e., constraints on time, budget, and resources). This document outlines the important elements of a media 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.

1. Introduction

1.1. Purpose and Scope

The information security concern regarding disposal and sanitization revolves around the recorded information rather than the media itself. The media used on an information system (i.e., ISM) should be assumed to contain information commensurate with the security categorization (low, moderate, or high) of the system's confidentiality. If not handled properly, the release of such ISM 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.

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* [5], which states:

> The sanitization process removes information from system media such that the information cannot be retrieved or reconstructed. Sanitization techniques—including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction—prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods, recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization.

This document will assist organizations in implementing a media sanitization program for media before disposal, reuse, or leaving the effective control of an organization. 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 the guidelines in this document to make effective, risk-based decisions on the ultimate sanitization and/or disposition of media and data throughout the system life cycle.

Before applying any sanitization efforts to ISM, 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. 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.

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 exchanges are critical to the delivery of government services, and the guidelines in this document 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 [8]. This critical initial step is outside of the scope of this document, but without this identification, the organization will likely lose control of some ISM containing sensitive data.

This document does not claim to cover all possible media that an organization could use to store or record information, 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 information contained in the media.

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 Systems to Security Categories* [7], 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 [5] provides minimum recommended security controls, including sanitization, for federal systems based on their overall system security categorization.
- SP 800-53Ar5, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans* [6], 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* [10], provides guidelines for selecting and using storage encryption technologies.

- SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* [11], provides guidelines for protecting the confidentiality of PII in information systems.

1.5. Document Structure

This document is divided into the following sections and appendices:

- Section 1 describes this document's 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 identifies a set of device-specific characteristics of interest that users should request from ISM vendors.
- Appendix C 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 ISM used in the system. Some ISM support enhanced interface 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 ISM types. Without an effective command or interface-based sanitization technique, the ISM may have to be destroyed. In that event, the ISM cannot be reused by other organizations that could have benefited from receiving the repurposed ISM.

During the requirements phase, other types of ISM 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 ISM 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).

2.1. Need for Proper Information Disposition and Media Sanitization

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].

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 is enough to be considered a data breach. Understanding where this sensitive information is stored and systematically tracking the media on which it is stored can be important safeguards against data breaches.

For organizations to have appropriate controls on the information for which they are responsible, they must properly safeguard used media. Potential misuse of information collection can result from improperly disposed hard copy media, the acquisition of improperly sanitized ISM, or laboratory reconstruction of ISM 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, 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.

2.2. Types of Media

This document focuses on two primary types of media in common use:

- **Hard copy.** Hard copy media refers to physical representations of information, typically paper printouts, film, microfiche, etc. 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.
- **Information storage media (ISM).** ISM commonly[2] takes the form of:
    - Devices that contain bits and bytes, such as hard disk drives (HDDs), solid state drives (SSDs), random access memory (RAM), read-only memory (ROM), optical disks, magnetic tape, 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.

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 sanitization 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 of the user data stored on the ISM. If the target data cannot be selectively or partially sanitized, sanitization operations should be expanded to cover all user data instead (see Sec. 4.2).

Some types of ISM can contain more physical storage than the user addressable capacity (e.g., overprovisioning) for endurance and performance purposes. For example, an ISM can have 1024 GB of total physical capacity but only 900 GB of available capacity (i.e., user accessible storage). If the ISM implements data reduction techniques (e.g., data compression) internally, it is also possible for the user-addressable capacity to exceed the total physical capacity. In either case, user data may be stored on the full 1024 GB because of the mechanisms in the ISM, and the entire contents should 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. Organizations retain the ability to increase the level of sanitization applied if that is reasonable and indicated by an assessment of the existing risk.

Organizations should consider other factors, including:

- The types (e.g., hard copy, ISM), physical sizes, density (e.g., high resolution film), or capacities (e.g., megabyte, gigabyte, terabyte for ISM) of the media to be sanitized
- The confidentiality requirement for the information recorded or stored on the media
- Whether the media will be processed in a controlled area
- Whether sanitization techniques should be conducted by the organization or a third party
- Whether sanitization is performed on-site or off-site[3]
- 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 or tools
- How much time the complete sanitization technique will take (i.e., duration)
- The cost of sanitization when considering tools, training, verification, and re-entering ISM into the supply stream

[3] An organization's loss of control of an ISM that contains certain types of sensitive data may constitute a data breach.

3. Summary of Sanitization Methods

The level of effort applied when attempting to retrieve data can vary widely, especially for ISM. Interested parties may attempt simple data retrieval from an ISM (e.g., reads) without the use of specialized tools, skills, or knowledge, or they can have extensive capabilities that enable them to apply state-of-the-art laboratory techniques.[4]

Users of this document should categorize the information (e.g., low, medium, and high security categorizations) to be disposed of, assess the nature of the media 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.

3.1. Sanitization Methods

Three different sanitization methods are defined to sanitize media: clear (see Sec. 3.1.1), purge (see Sec. 3.1.2), and destroy (see Sec. 3.1.3). In addition, one or more technology-specific sanitization techniques may be available for each sanitization method. As storage technology evolves, these sanitization techniques need to be updated on a regular basis, so the latest version of standards (e.g., IEEE 2883 [13]) should be consulted.

ISM sanitization techniques are one of the following:

- **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. The intent of logical sanitization is to leave the ISM in a usable state.
- **Physical techniques.** External physical measures are applied to eliminate data or the ISM. With few exceptions, physical techniques typically leave the ISM in an unusable state and involve some form of destruction.

Except for cryptographic erase (see Sec. 3.2), technology-specific sanitization techniques are out of scope for this document.

3.1.1. Clear Sanitization Method

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

[4] "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 high-value sensitive data that has been sanitized.

Clear sanitization techniques are 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 ISM to the factory state if rewriting is not supported. Clear sanitization techniques typically have no impact on the usability of the ISM.

One clear sanitization technique 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 ISM. This process can include overwriting both the file metadata (e.g., file allocation table entry) 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.

In the past, hard drives were often erased using multiple overwrite passes (e.g., based on DoD 5220.22-M[5]) 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. For certain ISM (e.g., SSDs with overprovisioning), such practices should be avoided as very little confidentiality protection is achieved. If additional assurances are needed, 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.

Overwriting cannot be used on a non-rewriteable ISM or one that is damaged to the point of being inoperable and, therefore, cannot address all areas of the ISM 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 that contain spare cells and perform wear levelling make it infeasible for a user to sanitize all previous data using this approach because the device cannot 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) can be exposing their data to increased risk of unintentional disclosure. Although the host interface can be the same or very similar across ISM 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 ISM vendor that the commands have been implemented as expected.

Clear sanitization techniques can vary contextually for ISM other than dedicated storage devices, where the ISM (e.g., a basic cell phone, a piece of office equipment) only provides the ability to return the ISM 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 clear sanitization technique options for the ISM. These still meet the

[5] The U.S. Department of Defense (DoD) Manual 5220.22, or National Industrial Security Program Operating Manual (NISPOM), is now Part 117 of Title 32, Code of Federal Regulations. In 2006, DoD removed overwriting specifications from NISPOM.

definition for the clear sanitization method as long as the device interface available to the user does not facilitate retrieval of the original data.

3.1.2. Purge Sanitization Method

The purge sanitization method is *not* appropriate for hard copy under any conditions but may be appropriate for some ISM. Purge sanitization techniques apply 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. When possible, the purge sanitization method should be used instead of the clear sanitization method.

Logical purge sanitization techniques can vary by ISM type, so IEEE 2883 [13]should be consulted to determine acceptable purge sanitization techniques, which can include overwrite, block erase, and cryptographic erase using 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 sanitization technique increases the likelihood of preserving the storage device in a usable state.

Of the logical purge sanitization techniques, cryptographic erase is noteworthy in its ability to rapidly sanitize target data. However, the effective use of cryptographic erase depends on the pedigree of cryptographic capabilities and meeting certain pre-conditions. Section 3.2 addresses these dependencies.

For an ISM that takes the form of logical/virtual storage (e.g., cloud storage), cryptographic erase may be the only viable purge sanitization technique option. Typically, the underlying physical ISM is abstracted such that the data owner has no direct access to the physical ISM, and sanitizing them is not possible. As such, organizations should clearly understand their purge sanitization technique options and the effectiveness of the technique prior to storing sensitive data on such ISM.

Physical purge sanitization techniques historically included degaussing for magnetic tapes, magnetic removable disks, and magnetic hard disk drives [19]. Degaussing should not be used for non-magnetic ISM (e.g., flash storage, such as SSDs). The use of degaussing as a purge sanitization technique has become more complicated as ISM have evolved to use hybrids of magnetic and non-magnetic storage as well as variations of magnetic recording technologies with higher coercivity[6] (i.e., magnetic force)[18]. As a result, many existing degaussers [19] do not have sufficient force to effectively degauss such ISM. Additionally, degaussing can damage (i.e., make unusable) some types of ISM, potentially rendering them inoperable (e.g., if the servo tracks are damaged), but fail to sanitize the target data. At the time of this writing, degaussing is not considered an approved destroy sanitization technique (see Sec. 3.1.3), but IEEE 2883 [13] and/or NSA/CSS Policy Manual 9-12 [16] should be consulted for further clarification.

Other physical purge sanitization techniques can also exist.

[6] Degaussing potentially renders a magnetic ISM purged when the strength of the degausser is carefully matched to the ISM coercivity.

3.1.3. Destroy Sanitization Method

The destroy sanitization method is appropriate for all hard copy and most ISM, except for logical/virtual storage. Destroy sanitization techniques render 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.

There are many different types, techniques, and procedures for media destruction. While some techniques can render the target data infeasible to retrieve through the device interface and unable to be used for subsequent storage of data, the ISM is not considered destroyed unless target data access or recovery is infeasible using state-of-the-art laboratory techniques. The application of destructive techniques may be the only option when the ISM fails or is obsolete (e.g., the ISM interface is no longer supported) and other clear or purge sanitization techniques cannot be effectively applied to the ISM.

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

- *Disintegrate.* Process that 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 destroys the media by burning it to ash.
- *Melt*. Process that destroys the media by liquefying it (i.e., loses intactness or solidness), generally through the application of extreme heat.
- *Pulverize.* Process that destroys the media by reducing it to a fine powder or dust through crushing, grinding, or other mechanical means.
- *Shred*. Process that destroys the media by cutting or tearing it into small particles.

Techniques like bending, cutting, or some emergency procedures (e.g., shooting or drilling a hole through a storage device) may only partly damage the ISM, leaving portions of it accessible using state-of-the-art laboratory techniques.

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

3.2. Use of Cryptography and Cryptographic Erase

Increasingly, ISM have integrated encryption and key-management capabilities. Under the correct conditions and with strong cryptography, these capabilities can be used to sanitize ISM with a purge sanitization technique known as cryptographic erase (CE). At a basic level, CE is based on the sanitization of keys used to encrypt data or to prevent access to the keys that encrypt data. Thus, with CE, sanitization can 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 the guidelines in this document. Federal agencies must use

encryption modules[7] validated to the current FIPS-140 standard [1] in order to have assurance that the conditions stated above have been verified for the self-encrypting drive (SED).

Further elaboration on CE and guidance is covered in this section.

3.2.1. Strength of Cryptography for CE

CE is based on symmetric-key encryption and associated key management. In order for encryption to provide confidentiality, the cryptographic algorithm (e.g., the Advanced Encryption Standard [30]) used for encryption and its mode of operation must be designed and implemented so that an unauthorized party cannot determine the decryption key associated with the encryption or be able to derive the plaintext directly without using the appropriate key to decrypt the encrypted information (i.e., ciphertext) [31].

ISO/IEC 27040 [15] addresses the strength of cryptography for CE by specifying:

- The security strength of the cryptographic algorithm (including the mode of operation) used to encrypt the target data is at least 128 bits.
- The level/bits of entropy of the random number sources are at least the number of bits of the cryptographic keys (e.g., encryption keys, wrapping keys, or keys used to derive these keys).

Confidentiality assurances for CE depend on other cryptographic considerations. While ISO/IEC 27040 [15] approaches cryptography from an international perspective, this document narrows the approved cryptography to a smaller set of options, which are reflected 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 the key-generation procedures applied to the random data. This applies to the cryptographic keys and any wrapping keys affected by the cryptographic erase operation.	SP 800-90A [9] SP 800-90B [23] SP 800-90C [24] SP 800-133 [25]
ISM Encryption	The security strength and validity of the implementation of the encryption algorithm/mode used to protect the target data.	FIPS 140-3[8] [1] FIPS 197 [30] SP 800-38A[9] [4] SP 800-38E [27]

[7] NIST maintains lists of validated cryptographic modules and cryptographic algorithms.
[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).
[9] Electronic codebook (ECB) mode is not allowed.

Area	Considerations	Relevant Docs
Key Level and Wrapping	The key being sanitized might not be the symmetric data-encryption key but a key used to wrap (i.e., encrypt) it. 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 encryption operation.	FIPS 197 [30] SP 800-38A [4] SP 800-38F [26] SP 800-131A [29]
Key Derivation	The methods for deriving additional keys from an existing cryptographic key.	SP 800-90A [9] SP 800-108 [28] SP 800-133 [25]

3.2.2. Applicability of CE

As a pre-condition for using CE, ISO/IEC 27040 [15] specifies that no sensitive data has previously been stored[10] on the ISM in plaintext form (i.e., not encrypted) as CE can only sanitize keys related to encrypted data. Sanitizing sensitive data stored as plaintext requires the use of other storage sanitization techniques that are appropriate for the ISM. For ISM consisting of virtual/logical storage, there may not be a purge sanitization technique alternative to CE.

As mentioned earlier, many ISMs have integrated symmetric-key encryption that is implemented such that it is always active and encrypts all data stored on the ISM. These ISM are often known as self-encrypting drives (SEDs), and they typically include sanitization capabilities as well.

When considering the applicability of CE, the sensitivity of the information is an important factor. Some sensitive information can be long-lived, and confidentiality protections need to span decades. In such cases, future recovery of the data can be a concern because the data still resides in the ISM as ciphertext. If cryptographic weaknesses in the algorithms used in those ISM were found in the future or computational capabilities (e.g., quantum computing) made it feasible to recover keys, the sensitive data can become recoverable in those ISM. For such situations, CE may not be an acceptable sanitization technique.

Sanitization using CE should not be trusted on ISM 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 ISM. Such backed up or escrowed copies of data, credentials, or keys should be subject to a separate ISM sanitization policy.

3.2.3. Sanitization of Keys

The objective of CE is to permanently prevent the decryption of ciphertext associated with sensitive information. CE is achieved through the sanitization of keys used to encrypt data or prevent access to the keys that encrypt data, which are collectively referred to as target cryptographic keys.

[10] For an ISM that was previously sanitized with an appropriate technique, this prohibition applies since the last sanitization of the ISM.

The recommended key sanitization technique is zeroization, as described in ISO/IEC 19790 [14] (e.g., overwriting with all zeros, all ones, or random data), of the target cryptographic keys. ISO/IEC 27040 [15] further specifies that all copies of the target cryptographic keys must be able to be sanitized.

The following key types are potential target cryptographic keys for CE, as described in SP 800-57pt1r5 [31]:

- Symmetric data-encryption keys are used with symmetric-key algorithms to apply confidentiality protection to data (i.e., encrypt plaintext data).

  When symmetric data-encryption keys are sanitized or ciphertext (i.e., wrapped) versions of these keys are sanitized, the corresponding ciphertext cannot be decrypted.

- Symmetric key-wrapping keys (sometimes called key-encrypting keys) are used with symmetric-key algorithms to encrypt other keys. The key-wrapping key used to encrypt a key is also used to decrypt the encrypted key.

  When key-encrypting keys are sanitized or ciphertext (i.e., wrapped) versions of these keys are sanitized, the protected symmetric data-encryption keys cannot be decrypted and, therefore, the ciphertext corresponding to these symmetric data-encryption keys cannot be decrypted.

- Symmetric master keys or key-derivation keys are used to derive other symmetric keys (e.g., data-encryption keys, key-wrapping keys) using symmetric cryptographic methods. There are many instances where one or more key-derivation keys are jointly[11] used to derive a symmetric key (often a key-encrypting key).

  When at least one of these key-derivation keys is sanitized or ciphertext (i.e., wrapped) versions of these keys is sanitized, the key derivation cannot be correctly completed, and the relevant symmetric data-encryption key or key-wrapping key cannot be derived. When such keys are not available, the ciphertext containing sensitive information cannot be decrypted.

- Private key-transport keys are the private keys of asymmetric-key pairs that are used to decrypt keys that have been encrypted with the corresponding public key using a public-key algorithm. Key-transport keys are usually used to establish symmetric keys (e.g., key-wrapping keys, data-encryption keys, key-derivation keys) and, optionally, other keying material (e.g., initialization vectors).

  There are also situations in which public-key cryptography is used such that a public key (i.e., public key-transport key[12]) encrypts (i.e., encapsulates) a key that is "transported" and subsequently decrypted (i.e., decapsulated) by the corresponding private key (i.e., private key-transport key). The transported key can serve as a symmetric data-

[11] As an example, a cloud service provider could offer cloud storage, built upon multiple SSDs that employ encryption, wherein keys supplied by a customer, by the cloud service provider, and a unique key contained each SSD are cryptographically combined to produce a wrapping key that protects the keys used for encryption. If any one of these keys are sanitized, the encrypted data protected by these combined keys is not available (i.e., it has been sanitized).

[12] The sanitization of public key-transport keys is not considered a valid form of sanitization because these keys are not typically protected, and there may not be a way to eliminate all copies of them.

encryption key, a key-wrapping key, or a key-derivation key. When the private key or a ciphertext (i.e., wrapped) version of the key is sanitized, the "transported" key cannot be decrypted (i.e., decapsulated), so the ciphertext protected by this key cannot be decrypted

In addition to performing appropriate key sanitization on the target cryptographic keys, it is imperative that all keys hierarchically below the target cryptographic keys are eliminated or actively erased. Such actions can provide an additional measure of protection, if the target cryptographic keys are ever recovered.

As part of a CE operation, steps should be taken to guard against continued use of keys that may have been recovered prior to the CE operation. For example, if the wrapped versions of keys had previously been unwrapped and the keys inside them stored to volatile memory or written into a register in a data encryption engine, the elimination of all unwrapped versions of the key must also be assured, preferably by direct key sanitization, but may require a hard reset or powering off the ISM for some period of time.

When deciding whether to rely on CE, ISO/IEC 27040 [15] recommends considering whether the target cryptographic keys can be recovered internally or externally (e.g., injected from a key management server or from a key escrow service). If the target cryptographic keys (or any key at or below the level of key sanitized during CE) exists outside of the ISM, there is a possibility that the key can be used in the future to recover encrypted data stored on the ISM.

3.2.4. Quality of Cryptographic Implementations

ISO/IEC 27040 [15] recommends organizations that choose to apply CE to seek either independent validation [15] of the following assurance areas or ask the ISM vendor to identify which mechanisms are used to ensure that these concern areas have been addressed:

- The level of entropy of the random number sources and the quality of whitening procedures applied to the random data (e.g., key generation). This applies to the cryptographic keys and, potentially, to wrapping keys affected by the CE operation.
- The security strength and validity of implementation of the encryption algorithm/mode used to protect target data.
- The technique used for key sanitization of keys associated with CE is sufficient to prevent recovery of the target keys.
- The security strength and level of assurance of the wrapping techniques used are commensurate with the level of strength of the cryptographic encryption operation.

Generally accepted and standardized mechanisms should be used, as applicable. For example, cryptographic requirements are specified in ISO/IEC 19790 [14], and test requirements for cryptographic modules are specified in ISO/IEC 24759 [32]. These test requirements and tests cover some but not all of the concern areas.

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

3.2.5. Traceability of CE Operations

Documenting a storage sanitization operation is often a component of an organization's media sanitization program (see Sec. 4.6). When CE is used as the purge sanitization technique, the evidence or documentation may need to be augmented with additional details, including:

1. **Make, model, version, or ISM type.** The product and versions to which the statement applies and the type of storage technology that the ISM uses (e.g., magnetic disk/tape, solid-state drive, hybrid). Many ISMs store the target data (see Sec. 2.3) in several different ISM components (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 [9]) was used and how it was validated.
3. **Media encryption.** Identify the algorithm, key strength, mode of operation, and any applicable validations.
4. **Key wrapping.** Identify whether the symmetric data-encryption key, key-wrapping key, or key-derivation key is sanitized. A description of the wrapping techniques only applies if a key-encryption key (KEK) is sanitized. When applicable, details about the key-wrapping key and/or key-derivation key algorithms used should be provided, including their strengths and (if applicable) their mode of operation.
5. **ISM areas addressed.** Describe which areas are encrypted and which are not. For any unencrypted areas (i.e., not used for user data), 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.
7. **Key sanitization technique.** Describe the ISM-dependent key sanitization technique used to sanitize the key (see Sec. 3.2.3).
8. **Key escrow or injection.** Identify whether the ISM 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 ISM.
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 symmetric data-encryption keys, identify whether all symmetric data-encryption keys are changed using the host interface commands available and any additional commands or actions necessary.

When the target cryptographic keys for CE are stored in an external key management system (KMS) and then provided to the ISM, the documentation trail for key sanitization within the KMS may be limited to the details contained in the KMS (i.e., the ISM may have no visibility into key sanitization on the KMS). Further, the key may have been escrowed, backed up, and/or stored elsewhere, so the documentation needs to reflect how these potential sources for key recovery have been addressed as well.

CE's effectiveness as a purge sanitization technique does not depend on documentation. However, CE acceptance by an organization can be influenced by the documentation that can be produced for CE operations.

4. Media Sanitization Program

A media sanitization program can help ensure the consistent and appropriate disposal of storage assets and avoid data breaches due to mishandling. ISO/IEC 27040 [15] states that storage sanitization should be an element of the organization's data governance process, which should include the following at a minimum:

- Specifying policies that set the expectations associated with storage asset disposal (i.e., transfer, reuse, destruction) 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:

- 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 [13])
- 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

For federal organizations, unclassified ISM that are never used in a classified information system or that do not contain For Official Use Only (FOUO) information, Privacy Act information, or personally identifiable information (PII) do not require sanitization [17].

For most sanitization operations, the target data of the operation ultimately includes all user data stored on the ISM and not just the sensitive data. However, there may be a desire or need to sanitize a subset of the ISM. Selective sanitization focuses on sanitizing specific sensitive data wherever this data resides in the ISM.[13] Partial ISM sanitization focuses on sanitizing a subset or region of the ISM.

Partial ISM sanitization comes with some risks, as it can 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 or overprovisioning). In addition, the dedicated interfaces provided by ISM vendors for sanitization typically operate at the device level and cannot be applied to a subset of the ISM.

On ISM with integrated encryption capabilities, CE provides a unique mechanism for supporting some types of partial ISM sanitization. These ISM can 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 ISM sanitization via CE is possible. As with any other sanitization technique applied to ISM, 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 can 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 of reliably ensuring that partial ISM sanitization effectively addresses all sensitive data, sanitization of the whole ISM is preferred to partial ISM sanitization whenever possible. Organizations should understand the potential risks of this approach and make appropriate decisions that balance missions and specific use cases. For example, an ISM in a data center can 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 ISM sanitization, if possible, in order to retain the data of other customers. The organization may also choose to apply partial ISM sanitization because the ISM 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 ISM sanitization mechanism that is available for that specific ISM. If the alternative to partial ISM sanitization is not performing sanitization at all, partial ISM sanitization provides benefits that should be considered.

4.3. Storage Sanitization and Disposition Decision Framework

An organization may maintain ISM with differing levels of confidentiality, and it is important to understand what types of data can be stored on the ISM in order to apply the security 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]. Additionally, SP 800-60r2 [7] describes mapping information types to security categories.

[13] An example of selective sanitizing is sanitizing the contents of a single file that is encrypted with a unique key using CE.

While most ISM support some form of clear sanitization technique, not all ISM have a reliable purge sanitization technique. For moderate sensitivity 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, equipment, and skills to do so (see IEEE 2883.1 [22] for additional guidance).

Purge sanitization techniques (and clear sanitization techniques, where applicable) may be more appropriate than destroy sanitization techniques when factoring in contractual obligations (e.g., lease returns), 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 can vary between different environments.

Organizations can refer to Fig. 1 and the descriptions in this section to make sanitization decisions that are commensurate with the security categorization (i.e., low, medium, and high) of the confidentiality of information contained on their media.

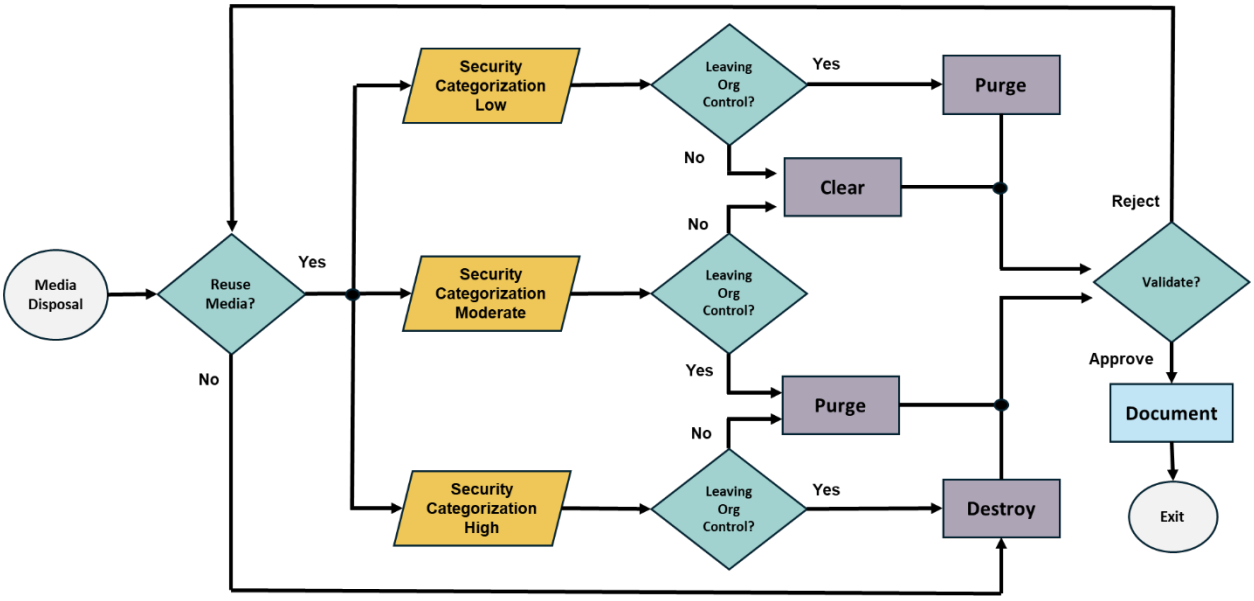

Fig. 1. Sanitization and disposition decision flow

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 [12].

One of the key decisions that will affect the ability to conduct sanitization is choosing what ISM 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.

An organization can ask an ISM vendor for assistance in identifying components of ISM that may potentially contain sensitive data, which is typically documented in a Statement of Volatility (SoV).[14] 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 can state volatility details differently.

A list of device-specific characteristics of interest for the application of sanitization techniques is included in Appendix B. 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 ISM 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 available degaussers can effectively degauss the ISM.

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

The increasing availability of rapidly applicable sanitization 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.

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 sensitive 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.

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 [7], or CNSSI 1253 [12], including the security categorization for the system's confidentiality (i.e., low, medium, and high security categorizations). This security

[14] A Statement or Letter of Volatility (SOV/LOV) is a specification issued by device manufacturers. An SOV/LOV generally includes the following information: 1) list of all volatile and non-volatile memory components or locations, 2) the nature of data stored in the memory, 3) whether the memory is accessible by the user, and 4) how the data can be erased or sanitized.

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 ISM with their internal operating confidentiality levels and associate a type of sanitization described in this document.

4.3.3. Reuse of Media

A key sanitization decision is whether the media (i.e., rarely other than ISM) is planned for reuse (e.g., internal transfer, donations, refurbishment). 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 can be to destroy the media.

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.

Media control can change when an ISM is returned from a leasing agreement, donated, resold to be reused outside of the organization, or sent to a recycling facility. For example:

- ISM under organizational control
    - ISM that are turned over (and securely transported) to a maintenance provider may still be considered to be under organizational control if contractual agreements are in place with the organization and the maintenance provider that 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.
- ISM not under organizational control (i.e., external control)
    - ISM 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.

The examples above do not consider relevant legal, regulatory, or statutory requirements associated with certain types of sensitive data, which can treat the loss of organizational control of ISM that have not been sanitized as a data breach.

4.3.5. Data Protection Level

Varying data protection policies may be established within an organization. For example, an organization can have an engineering department and a sales department, where the sales personnel do not need to access detailed proprietary technical data (e.g., source code, schematics), and the engineers do not need to access the PII of the organization'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.

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 (see IEEE 2883.1 [22] for additional guidance). Again, certain factors and media types might cause the sanitization method to change.

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.

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 [13].[15] or a standard that is identified as acceptable by organizational policy (e.g., NSA/CSS Policy 6-22 [17], NSA/CSS Policy Manual 9-12 [16]). Depending on the media type (i.e., hard copy or ISM) and selected sanitization method, there can be multiple sanitization technique options. The option that provides the most confidentiality protection should be used. When the purge sanitization technique of CE is used for an ISM, Sec. 3.2 should be consulted for additional considerations or requirements.

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.

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 Defense Information Systems Agency

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

Security (DISA) Security Technical Implementation Guides (STIGs) [21], for additional information about recommended settings. Sanitization techniques typically play no role in configuring ISM. A frequent misconception is that a sanitized ISM will resemble a factory-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 [15], verifying the adequacy or effectiveness of sanitization outcomes is an important aspect of a media sanitization program. The results of attempted sanitization techniques are inspected (see Sec. 4.5.1), and a decision on the adequacy of the results is made (see Sec. 4.5.2). These activities are shown as the "Validate" decision point in Fig. 1. 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 reusability of media because a previous sanitization technique may have rendered the media unusable or inoperable.

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 destructive sanitization methods applied to either hard copy or ISM, this verification involves inspecting the remnants of a destruction technique and identifying the equipment used with it.

For non-destructive sanitization methods for ISM, verification can be more complex and typically depends on the type of ISM. Clear and logical purge sanitization 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 sanitization 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 can be limitations on further inspections of the ISM.

Unless explicitly required by organizational policy, elaborate sampling of an ISM's contents (e.g., full or representative) after clear or purge sanitization techniques is not necessary.

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.

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).

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 information. For example, a sanitization operation that degausses an SSD can complete successfully, but no sensitive data is sanitized.
- The sanitization may have been performed by unqualified personnel, or the tools and/or equipment used were not approved and/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 sanitized using clear sanitization technique based on 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 operation is deemed sufficient to ensure the confidentiality of the data.

4.6. Documentation

Following sanitization, a certificate of sanitization (see Appendix C) should be completed for each ISM that has been sanitized, per the organization's policies. A certification of sanitization may be a physical (e.g., piece of paper) or electronic record of the action taken. For example, some ISM include bar codes on the label for the model and serial numbers, so 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.

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

- Manufacturer

- Model
- Serial number
- Organizationally assigned media or property number (if applicable)
- Media type (i.e., hard copy or ISM)
- 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, CE)
- Tool used, including version
- Verification method
- Information of individuals performing verification and validation:
    - Name of person
    - Position/title of person
    - Date
    - Location
    - Contact information (e.g., phone number)
    - Signature

If the ISM has been successfully validated (see Sec. 4.5) and the sanitization results in a lower confidentiality level for the ISM, all markings on the ISM that indicate the previous confidentiality level should be removed.

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

4.7. Roles and Responsibilities

A successful media sanitization program depends on the sustained efforts and oversight of many individuals, and this section describes example roles and responsibilities. These roles focus on assuring programmatic success as opposed to operational responsibilities, which are not addressed.

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. Allocated resources should correctly identify the types and locations of information.

4.7.2. Chief Information Officer (CIO)

The CIO[16] 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.

4.7.3. Information System Owner

The information system owner[17] 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.

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.

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.

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

[16] 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.
[17] 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."

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.

4.7.7. Property Management Officer

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

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.

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.

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.

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. 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] 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

[5] 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

[6] 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

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

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

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

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

[16] National Security Agency/Central Security Service (2020) NSA/CSS Storage Device Sanitization and Destruction Manual. NSA/CSS Policy Manual 9-12, December 4, 2020. Available at https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/NSA-CSS-Policies/

[17] 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

[18] NSA/CSS (2021) Requirements for Magnetic Degaussers. Available at https://www.nsa.gov/portals/75/documents/resources/everyone/media-destruction/NSA_CSS%20Requirements%20for%20Magnetic%20Degaussers.pdf

[19] 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/

[20] "Chapter 33 – Disposal of Records," Title 44 U.S. Code, Sec. 3301. 2018. Available at https://www.gpo.gov/

[21] Defense Information Systems Agency Security (DISA) Security Technical Implementation Guides (STIGs). Available at https://public.cyber.mil/stigs/

[22] IEEE Standards Association (2022) *IEEE 2883.1– IEEE Recommended Practice for Use of Storage Sanitization Methods* (IEEE Standards Association, Piscataway, New Jersey). Available at https://standards.ieee.org/ieee/2883.1/11015/

[23] Turan M, Barker E (2018) Recommendation for the Entropy Sources Used for Random Bit Generation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-90B. https://doi.org/10.6028/NIST.SP.800-90B

[24] Barker E, Kelsey J (2025) Recommendation for Random Bit Generator (RBG) Constructions. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-90C. https://doi.org/10.6028/NIST.SP.800-90C

[25] Barker E, Roginsky A (2020) Recommendation for Cryptographic Key Generation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-133r2. https://doi.org/10.6028/NIST.SP.800-133r2

[26] Dworkin M (2012) Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-38F. https://doi.org/10.6028/NIST.SP.800-38F

[27] Dworkin M (2010) Recommendation for Block Cipher Modes of Operation: the XTS-AES Mode for Confidentiality on Storage Devices. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-38E. https://doi.org/10.6028/NIST.SP.800-38E

[28] Chen L (2022) Recommendation for Key Derivation Using Pseudorandom Functions. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-108r1. https://doi.org/10.6028/NIST.SP.800-108r1-upd1

[29] Barker E, Roginsky A (2019) Transitioning the Use of Cryptographic Algorithms and Key Lengths. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-131Ar2. https://doi.org/10.6028/NIST.SP.800-131Ar2

[30] National Institute of Standards and Technology (2001) Advanced Encryption Standard (AES). (Department of Commerce, Washington, D.C.), Federal Information Processing Standards Publications (FIPS) NIST FIPS 197-upd1, updated May 9, 2023. https://doi.org/10.6028/NIST.FIPS.197-upd1

[31] Barker E (2020) Recommendation for Key Management: Part 1 – General. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-57pt1r5. https://doi.org/10.6028/NIST.SP.800-57pt1r5

[32] International Organization for Standardization/International Electrotechnical Commission ISO/IEC 24759:2025 – *Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules* (ISO, Geneva, Switzerland). Available at https://www.iso.org/standard/82424.html

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.

coercivity
A measure of the ability of a ferromagnetic material to withstand an external magnetic field without becoming demagnetized.

cryptographic erase (CE)
A purge sanitization technique in which key sanitization is applied to one or more keys providing confidentiality protections for the encrypted target data, making recovery of the decrypted target data infeasible.

cut/cutting
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
A representation of information, including digital and non-digital formats, from which understandable information is derived.

degauss
To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field that is matched to the ISM coercivity.

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.

disintegration/disintegrate
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/incinerate
A physically destructive method of sanitizing media. The act of burning completely to ashes.

infeasible
Infeasible acknowledges the possibility of data recovery with future, more advanced technology. It simply means that, for a given level of effort and using current "state of the art" techniques, recovery cannot be done.

information
A meaningful expression of data.

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.

key sanitization
A technique for zeroization (e.g., overwriting with all zeros, all ones, or random data) of the target cryptographic keys.

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

media sanitization
The actions taken to render data written on media unrecoverable by both logical and state-of-the-art laboratory techniques.

medium/media
Material on which data may be recorded, such as paper, punched cards, film, magnetic tape, magnetic disks, solid state devices, or optical discs.

melting/melt
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.

Personally identifiable information (PII)

Any data that can be used to distinguish or trace an individual's identity, either alone or in combination with other information.

pulverization/pulverize
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 ISM to a requester.

read-only memory (ROM)
A pre-recorded ISM that can only be read from and not written to.

record
To write data on an ISM, such as a magnetic tape, magnetic disk, or optical disk.

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 protected with confidentiality measures, such as encryption and sanitization.

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. Device-Specific Characteristics of Interest

ISM 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 ISM vendors may have implementations that apply sanitization 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, ISM 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 [13]. 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:

- Media type (e.g., legacy/conventional magnetic recording, heat-assisted magnetic recording, magnetic shingle, 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 C. 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.

CERTIFICATE OF SANITIZATION	
PERSON PERFORMING SANITIZATION	
Name:	**Title:**
Organization:	**Location**
Phone:	**Email:**
MEDIA INFORMATION	
Vendor/Make:	**Media Type:**
Model Number:	**Serial Number:**
Property Number:	**Source:**
Classification:	**Operational/Damaged:**
SANITIZATION DETAILS	
Sanitization Method: ☐ **Clear** ☐ **Purge** ☐ **Destroy**	
Sanitization Technique:	
Tools Used (include version):	
Verification/Status:	
Validation:	
Notes:	
MEDIA DESTINATION/DISPOSITION	
☐ **Internal Reuse** ☐ **External Reuse** ☐ **Recycling Facility** ☐ **Manufacturer** ☐ **Other (Specify)**	
Details:	
SIGNATURE	
I attest that the information provided on this statement is accurate to the best of my knowledge.	
Signature:	**Date:**
Concurrence	
Name:	**Title:**
Organization:	**Location**
Phone:	**Email:**
Signature:	**Date:**

Fig. 2. Certificate of sanitization

Appendix D. Change Log

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

- Apart from CE, which is commonly used across all encrypted media, all sanitization technique and tool 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 hands-on sanitization decisions to maintaining confidentiality of sensitive information by establishing an agency or enterprise media sanitization program as part of media disposal or reuse.
- The term information storage media (ISM) replaces electronic (i.e., "soft copy") media in the document to accommodate logical storage (e.g., cloud storage) and other types of media (e.g., DNA, ceramic, glass-based).
- 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 obsolete DoD 5220.22-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.
- Guidance for degaussing as a physical purge sanitization technique has been updated to limit its applicability and clarifies that it does not currently constitute a destroy sanitization technique, even when it renders an ISM inoperable.
- For CE, the material was rewritten to consolidate and focus the content; Appendix D was integrated into the main body of the text.
- For CE, key sanitization has been defined to be based on ISO/IEC 19790 zeroization.

- For CE, the acceptable key types have been updated to include symmetric data-encryption keys, symmetric key-wrapping keys, symmetric master keys or key-derivation keys, and private key-transport keys as described by NIST SP 800-57 Part 1.
- 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.
- For a media sanitization program, the concept of sanitization assurance is introduced to verify the adequacy or effectiveness of sanitization outcomes. This sanitization assurance encompasses sanitization verification (determines the outcome of the sanitization technique used during the sanitization operation) as well as sanitization validation (decision process to either approve the sanitization as being effective or reject it).
- The sample "Certificate of Sanitization" form in Appendix C was updated.
- All content has been reformatted to follow the latest NIST technical report template.