Frequently Asked Questions for NIST SP 800-88r2, Guidelines for Media Sanitization

Point of Contact: Ramaswamy Chandramouli

Email: sp800-88-comments@nist.gov

Published Date: July 16, 2026

NIST Special Publication (SP) 800-88r2 (Revision 2), *Guidelines for Media Sanitization*, describes how to develop a media sanitization program, including techniques and controls based on the sensitivity of information. The following Frequently Asked Questions (FAQ) elaborates on the recommendations in SP 800-88r2 to provide clarity and address specific stakeholder queries. The questions and answers are organized under various focus areas.

1. Focus Area: General and Sanitization Program-Related 1

2. Focus Area: Sanitization Methods and Assurance 3

3. Focus Area: Clarifications on Specific Techniques for the Destruct Method 5

4. Focus Area: Sanitization of Virtual Media 7

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

1. Focus Area: General and Sanitization Program-Related

Q1: What is the primary difference between Revision 1 and Revision 2 of SP 800-88?

A: Revision 1 focused heavily on hands-on, media-specific techniques for media sanitization by using tables. Revision 2 shifts the focus to maintaining the confidentiality of sensitive information by:

- Establishing an agency or enterprise **media sanitization program**
- Describing sanitization assurance
- Navigating modern logical storage architecture
- Discussing three primary sanitization methods in detail: clear, purge, and destroy
- Introducing the term **information storage media (ISM)** to accommodate modern storage abstractions (e.g., cloud, container, object storage)
- Providing a decision flow diagram based on various parameters (e.g., sensitivity of stored information, reuse within or outside of the organization)

Q2: Does SP 800-88r2 recommend specific media sanitization techniques for each type of media?

A: No. For specific techniques for each type of media, SP 800-88r2 refers to evolving industry standards (e.g., IEEE 2883) and policy manuals for highly sensitive media used for government applications (e.g., NSA Policy Manual 9-22).

Q3: What is an "information storage media (ISM)" and why did NIST adopt this term?

A: ISM replaces the older term “electronic (soft copy) media.” NIST adopted this term in Revision 2 to properly account for the modern storage landscape, which includes physical hardware devices (e.g., SSDs, magnetic tape) as well as virtual or logical storage systems (e.g., cloud, object storage) that abstract the underlying physical media.

Q4: What core elements are required in a formal storage sanitization policy?

A: According to SP 800-88r2, an organization’s data governance process must establish a policy that outlines:

- Alignment of the organization’s data classification scheme (i.e., low, moderate, and high confidentiality) with acceptable sanitization methods (i.e., clear, purge, and destroy)
- Documentation and evidence requirements (i.e., certificates of sanitization)
- Defined roles, responsibilities, and mandatory personnel training
- Tool configuration, including equipment calibration, testing, and maintenance

- Specific validation and verification protocols to measure sanitization outcomes

Q5: How should an organization handle partial or selective sanitization?

A: Sanitizing the **entire ISM device is always preferred** due to data spilling risks, overprovisioning, and bad-block remapping. However, if partial sanitization is a business necessity (e.g., in a multi-tenant cloud environment or a shared data center drive), organizations can leverage CE to selectively sanitize specific cryptographic keys that are assigned to a singular partition or file, provided that they have absolute confidence that target data never escaped that encrypted boundary.

2. Focus Area: Sanitization Methods and Assurance

Q6: Does the "clear" method still require a multi-pass overwrite pattern as the old DoD 7-pass standard did?

A: No. Revision 2 clarifies that multi-pass overwriting is unnecessary. For modern storage technologies, such legacy practices achieve very little confidentiality protection and can significantly degrade the lifespan of flash-based media. Under the clear method, logical techniques apply standard read/write commands to overwrite user-addressable spaces, typically in a single pass, or to utilize manufacturer factory resets if rewriting is not supported.

Q7: What is the difference between sanitization verification and validation?

A: Revision 2 introduces **sanitization assurance** as a dual-phase process:

- **Verification:** The operational step of inspecting the immediate outcome of a sanitization technique to ensure that it has completed successfully without technical errors or anomalies
- **Validation:** A higher-level decision-making process in which an organization reviews verification data against the sensitivity of the data to formally approve the execution as effective, ensuring that any residual confidentiality risk is accepted

Q8: Is degaussing still considered an approved "destroy" method for media?

A: No. Revision 2 clarifies that degaussing currently operates as a physical **purge** technique for legacy magnetic media, but it does **not** constitute a true destroy method. While degaussing high-coercivity modern drives often disrupts internal servo tracks and renders the drive permanently inoperable, it can fail to sanitize the target data if applied to flash/hybrid components or if the degausser's magnetic field is mismatched to the media's coercivity.

Q9: What are the minimum requirements to use cryptographic erase (CE) as an approved purge method?

A: For CE to be valid under Revision 2, several stringent pre-conditions must be satisfied:

- **FIPS validation:** Federal agencies must use cryptographic modules that are validated to the current **FIPS 140** standard.
- **No prior plaintext:** No sensitive data can have been stored on the ISM in plaintext prior to the encryption keys being established.
- **Cryptographic strength:** The security strength of the algorithm (e.g., AES) must be at least 128 bits, and the entropy of the random number generator must match or exceed the key length.

- **Zeroization:** The target cryptographic keys (i.e., data-encryption keys, wrapping keys, or master derivation keys) must be permanently sanitized using zeroization methods.

3. Focus Area: Clarifications on Specific Techniques for the Destruct Method

Q10: On the effectiveness of certain destruct methods, Sec. 3.1.3 of Revision 2 states, "Pulverize and shred techniques for ISM should be avoided for anything but the lowest security categories of data." This appears counterintuitive since "shred and pulverization" reduces media material to small bits and would generally be considered the most suitable technique for ensuring the destruction of data in medium- and high-security categories.

A: Destructive techniques like pulverize and shred are ineffective for medium- and high-security categories due to data density because modern storage technologies can involve depth for writing data on media. Instead, high-powered degaussers in NSF's EPL must be used for magnetic media, and techniques like incineration (e.g., smelting, melting) should be used for all other media (e.g., SSDs).

Q11: Is a "shred AND smelting" technique acceptable for destroying ISM with high-security data?

A: "Smelting" (or "melting") is a recommended technique under "destructive" methods of media sanitization in the following standards:

1. ISO/IEC 27040:2024

   In the **2024 updated version** of the international standard for storage security, **melting** is categorized under physical destruction techniques:

   - **Section 10.6.4/Clause 10.6:** "Destruct applies physical techniques such as disintegration, incineration, melting, pulverizing, or shredding. It provides the highest assurance level and does not apply to logical storage."
   - **Context:** ISO/IEC 27040 identifies "destruct" as one of the three primary sanitization categories (alongside "clear" and "purge"). It recommends **melting** specifically when the media is **leaving organizational control and carries a high sensitivity classification.**

2. "Destruct" Methods in IEEE 2883

   IEEE 2883 defines **destruct** as physical destruction that leaves the device permanently unusable and data recovery infeasible, even for a state-of-the-art laboratory. The standard specifically lists **melt** as one of the methods. It is defined as "a sanitization method designed to completely destroy the storage media by **liquefying it**, generally through the application of heat." IEEE 2883 specifically **deprecates other destructive techniques** (e.g., **shredding**, **pulverizing**) as approved destruction methods for all modern HDDs and SSDs.

Q12: Why has NIST not provided recommendations on native methods or techniques (e.g., macOS-native commands, such as EraseDisk4) under clear or purge methods for specific ISMs (e.g., modern Apple devices, especially those using Apple silicon and SSDs using SATA or NVMe protocols)?

A: The intent of Revision 2 is to provide guidance on the applicability of specific sanitization methods (not sanitization techniques) based on a combination of factors (e.g., media reuse, security categorization of the data held in the media, whether the media goes outside or stays within the enterprise) and the overall organizational preparedness required to establish a sanitization program.

The only exception was the guidance provided for the **cryptographic erase (CE)** technique due to its ubiquitous use for all modern SSDs, which are self-encrypting. Therefore, the prerequisites outlined in Sec. 3.2.5 are part of due diligence measures for setting up a sanitization program for performing CE operations.

NIST refrains from endorsing specific product-related measures.

4. Focus Area: Sanitization of Virtual Media

Q13: How is purging accomplished if an organization does not own physical ISM (e.g., cloud storage)?

A: Because physical ISM is completely abstracted in a virtual or cloud environment, traditional physical destruction or overwrite commands are impossible for the data owner to execute. In these logical storage scenarios, **Cryptographic Erase (CE)** is often the *only* viable purge method. Organizations must review their cloud service agreements to ensure that keys are securely managed and that zeroization can be traceably validated.