DoD, NIST, or IEEE? Choosing the Most Secure Option from Modern Data Sanitization Standards

With data usage expected to reach **221 zettabytes** by 2026 and breach costs averaging **$4.88 million**, minimizing your attack surface by securely erasing outdated drives and devices is more important than ever. Choosing the right data erasure standard is crucial for securing end-of-life business data and maintaining compliance with applicable data privacy laws.

Unfortunately, one of the most commonly accepted data sanitization standards, the U.S. Department of Defense (DoD) 5220.22-M data erasure standard, is likely insufficient for most modern enterprise needs. It isn't recommended for modern asset sanitization, despite general industry recognition.

Instead, most organizations are turning to the National Institute of Standards and Technology (NIST) **Special Publication 800-88 "Media Sanitization Guidelines,"** updated in 2014. NIST 800-88 addresses most basic devices and drives but doesn't work for complex storage devices like SATA, SCSI, and NVME drives.

To address advanced storage needs, the Institute of Electrical and Electronics Engineers introduced the **IEEE 2883** standard in 2022, complemented by the **ISO 27040** standard published in January 2024. Together, these provide comprehensive guidelines for data sanitization on modern storage technologies.

The table below shows key differences between the DoD, NIST, and IEEE data sanitization standards.

	DOD 5220.22-M OR DOD 5220.22-M ECE	NIST 800-88, REV. 1	IEEE 2883-2022
NUMBER OF OVERWRITING PASSES	3 or 7	0-1	0-1
NUMBER OF FIRMWARE-BASED ERASURE PASSES	0	0-1	0-2
STANDARD LAST UPDATED	Feb 2006	Dec 2014	Aug 2022
CONSIDERS SSD ERASURE	No	Yes	Yes
CREATED FOR	U.S. government (specifically, Department of Defense)	Primarily U.S. government but open to all organizations	All organizations globally
VERIFIABLY SECURE METHOD OF ERASURE	Yes (HDDs only)	Yes	Yes
OUTLINES TECHNOLOGY-SPECIFIC DATA ERASURE METHODS	No	Yes	Yes
DETAILED GUIDANCE ON SANITIZING SATA, SCSI, AND NVME DRIVES	No	No	Yes

blancco

Common Questions About Data Sanitization Standards

How is data sanitization defined?

While the definition of data sanitization may vary based on organizational lexicons, Blancco uses terminology from the **International Data Sanitization Consortium (IDSC)**. "**Data erasure**" is one of three enterprise-acceptable methods for data sanitization. There are three steps required for data erasure:

1. The data must be successfully and permanently removed from the storage device (via at least one overwrite wipe).
2. The data's removal must be verified.
3. The data's removal must be certified via a tamper-proof report.

These steps ensure that data is both permanently and verifiably sanitized when it is no longer needed.

How many passes are recommended for data to be unrecoverable?

Many questions regarding DoD, NIST, and IEEE wipe standards focus on overwriting patterns or passes, suggesting that multiple passes are superior. However, this is inaccurate. The DoD standard, which mandates using three secure overwriting passes, is not capable of sanitizing many modern technologies. Meanwhile, both NIST and IEEE 2883 employ fewer passes but offer more thorough data destruction.

What is the difference between NIST 800-88 and IEEE?

NIST 800-88 offers comprehensive guidelines on clearing, purging, and destroying media to prevent unauthorized data retrieval. IEEE 2883 adopts a similar framework with categories of Clear, Purge, and Destruct. However, IEEE standards are often quicker to execute and incorporate newer data destruction capabilities introduced since 2015, such as restoring depopulated storage elements, resetting write pointers, and clearing NVMe buffers.

A notable distinction between the two is IEEE's deprecation of shredding and pulverizing as methods of sanitization. This change reflects the increasing density of information on modern storage devices and the consequent risk of data remnants on fragments. While NIST 800-88 remains a broader guideline for various media types, IEEE 2883 focuses on detailed technical standards tailored to contemporary storage technologies, making it a preferred choice in fast-paced and high-tech environments.

NIST 800.88 typically suffices for most organizations for now, but as technology grows in complexity, IEEE will most securely address modern sanitization needs. Organizations should integrate the IEEE 2883 standard into their processes to stay ahead.

blancco

Blancco's DoD, IEEE, and NIST-compliant Overwriting

Blancco's commitment to data security ensures that we meet and exceed the requirements of all major data sanitization standards, including DoD, NIST, and IEEE. By staying current with these guidelines, we guarantee that our solutions adapt to new technologies and effectively eliminate data risks.

For NIST standards, Blancco Drive Eraser provides both Clear and Purge levels of data sanitization. Our software has been rigorously tested and validated to comply with NIST 800-88 guidelines, ensuring that your data is rendered completely unrecoverable. Our software has undergone comprehensive testing under the ADISA Product Assurance certification scheme, verifying its capabilities to achieve both NIST Clear and Purge levels of sanitization across multiple drives and devices.

Blancco Drive Eraser is also fully compliant with IEEE standards, and again, has obtained ADISA certification verifying Clear and Purge capabilities. In fact, Blancco was one of the first data erasure vendors to achieve ADISA certification for both NIST and IEEE standards. Leveraging modern data destruction methods, Blancco ensures that even the most advanced storage technologies are thoroughly sanitized.

Finally, for clients who have not yet made the transition, Blancco Drive Eraser continues to support legacy DoD standards. Our software meets the stringent requirements once set forth by the Department of Defense, guaranteeing complete data destruction.

Blancco's software is designed with flexibility in mind, allowing it to easily adapt to all data sanitization standards that may be present in a tech environment. Whether you need to comply with NIST, IEEE, or legacy DoD standards, our solutions can be set to automatically erase data based on the specific guidelines you require, ensuring seamless integration and reliable data security.

For more information on permanent erasure through Blancco, request a **free trial** from our website.