EVALUATING STANDARDS OF DATA DESTRUCTION: DOD/NISPOM VS IEEE VS NIST

CentricsIT
SECURE SUSTAINABILITY

Cybersecurity is a multibillion-dollar industry, with Gartner estimating $215 billion spent globally in 2024.[1] Despite heavy investments, many overlook decommissioned assets. ITAD providers follow three standards: DOD 5220.22-M, NIST 800-88, and IEEE 2883-2022. These standards, created for different purposes, vary based on the hardware they address. Choosing the right one for your business and hardware is crucial for an effective ITAD program.

[1]Gartner. "Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024." Gartner.com. https://www.gartner.com/en/newsroom/press-releases/2023-09-28-gartner-forecasts-global-security-and-risk-management-spending-to-grow-14-percent-in-2024/

CONTENTS

OVERVIEW
DOD 5220.22/THE NISPOM RULE

DoD 5220.22/The NISPOM Rule

DoD 5220.22 was first published in 1995 and was replaced by the NISPOM rule in 2021.[2] DoD 5220.22 was created by the National Industrial Security Program (NISP), which was established by Executive Order 12829 in 1993.[3] The DoD 5220.22-M was also known also the NISP Operating Manual or NISPOM. For data sanitization, it requires three overwriting passes.[4] The DoD 5220.22-M ECE requires 7 passes.[5] Its successor, the NISPOM Rule (or 32 CFR Part 117, NISPOM) is required for all executive branch departments, agencies and contractors for the United States government.[6] Where DoD 5220.22 was a manual, NISPOM is now a federal rule, ramping up consequences for those bound by it that fail to maintain compliance.

NIST 800-88

NIST 800-88, originally published in 2006, was created by the National Institute for Standards and Technology (NIST).[7] The latest version is NIST 800-88 Rev.1 and was revised in 2014. NIST 800-88 differentiated itself by providing guidance for all types of storage devices, including chip-based storage like SSDs, flash-based storage and mobile devices.

NIST 800-88 has three methods for erasing data: Clear, Purge and Destroy. The below definitions are quoted directly from NIST 800-88.

[1]Defense Counterintelligence and Security Agency. "32 CFR Part 117 NISPOM Rule." 32 CFR, Part 117. dsca.mil. https://www.dcsa.mil/Industrial-Security/National-Industrial-Security-Program-Oversight/32-CFR-Part-117-NISPOM-Rule/
[2]U.S. National Archives. "Ex. Ord. No. 12829, Jan. 6, 1993, 58 F.R. 3479, as amended by Ex. Ord. No. 12885, and further amended by Ex. Ord. No. 13691, Feb. 20, 2016." Archives.gov. https://www.archives.gov/files/isoo/policy-documents/eo-12829-with-eo-13691-amendments.pdf
[3]Defense Counterintelligence and Security Agency. "Defense Counterintelligence and
[4]Security Agency Assessment and Authorization Process Manual, Version 2.2." Page 127. dcsa.mil.
https://www.dcsa.mil/Portals/91/Documents/CTP/tools/DCSA%20Assessment%20and%20Authorization%20Process%20Manual%20Version%202.2.pdf
[5]Blancco. "Everything You Need to Know About the DoD 5220.22-M Disk Wiping Standard & Its Applications Today." Blancco.com. https://www.blancco.com/resources/blog-dod-5220-22-m-wiping-standard-method/
[6]Federal Register. "National Industrial Security Program Operating Manual." Federalregister.gov. https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom
[7]National Institute of Standards and Technology (NIST). nist.gov. https://www.nist.gov/

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

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

Destroy: *Destroy renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.*[8]

NIST 800-88's instructions for different forms of data-bearing devices set it apart from DoD 5220.22. Its clear delineations between clear, purge and destroy invite IT decision makers to approach data destruction in terms of data confidentiality and to reuse hardware when possible.

IEEE 2883-2022

IEEE 2883-2022 was published in August 2022 by the Institute of Electrical and Electronics Engineers (IEEE).[9] Meant to address the newer forms of data that NIST doesn't cover, it provides clear instructions and clarification around data destruction methods for different types of data-bearing devices.

[8]National Institute of Standards and Technology (NIST). "NIST Special Publication 800-88, Revision 1; Guidelines for Media Sanitization." Page 17. nist.gov. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf
[9]Institute of Electrical and Electronics Engineers (IEEE). ieee.com. https://standards.ieee.org/

Much like NIST 800-88, IEEE 2883-2022 approaches data sanitization with three categories: Clear, Purge and Destruct. While it may appear that IEEE is using NIST's framework, it makes several significant changes.[10]

Clear: Under IEEE 2883-2022, clearing data uses factory reset features or overwrites data with binary on hard drives and SSDs. Equipment that has been cleared can be reused. However, there may be hidden or inaccessible data, and it does not address this data.

Purge: IEEE's definition of purging is slightly different than NIST's. Under IEEE, purge is defined as sanitizing using logical techniques or physical techniques that make recovery of target data infeasible using state-of-the-art laboratory techniques, but that preserves the storage media and the storage device in a potentially reusable state.

Destruct: IEEE also makes distinctions when it comes to its definition of destruct. Its definition of destruct is very similar to NIST's, however, IEEE considers shredding and crushing to be obsolete. It only accepts incineration, melting and disintegration. It understands that these methods of destruction generate ewaste and release carcinogens, which is why it recommends purging whenever possible and only recommends data destruction when the information is extremely sensitive.

[10]Institute of Electrical and Electronics Engineers (IEEE). "IEEE 2883-2022: IEEE Standard for Sanitizing Storage." Section 3.1. ieee.com. https://standards.ieee.org/2883/10277

POINTS TO CONSIDER

TECHNOLOGY IN PLAY

The type of data-bearing device plays a role in the method of data destruction that should be used. Though all three methods are considered industry standards, each was produced by different groups for their own purposes.
If the devices in question belong to executive branch departments, agencies or contractors for the United States government, NISPOM is compulsory.[11] Its predecessor, DoD 5220.22-M, was adopted as one of the first standards of data destruction and sanitization released, so some consider it to be outdated with modern data-bearing devices.

NIST and IEEE give lists of technology and provide guidance for clearing, purging and destroying/destruction. However, IEEE was published more recently and contains guidance on more recent forms of data bearing devices that NIST does not, like office equipment, printers, tablets and gaming consoles.

INTENDED AUDIENCE

DoD 5220.22-M/NISPOM: United States Government

The DoD 5220.22-M and later the NISPOM Rule were created for use by the United States government and contractors. NISPOM is not a document dedicated to data destruction, but rather information security as a whole, and

[11]Federal Register. "National Industrial Security Program Operating Manual." Federalregister.gov. https://www.federalregister.gov/documents/2020/12/21/2020-27698/national-industrial-security-program-operating-manual-nispom

it includes sections on security clearance, reporting requirements, security education and training. NISPOM points to NISP for more detailed instructions on data security.

NIST 800-88: United States Government/Public Sector

NIST 800-88, like DoD 5220.22-M and NISPOM, was created by the government for the government, but it considers itself for everyone looking for guidance on sanitizing data.[12] Similar to DoD and NISPOM, NIST 800-88 was adopted by the private sector to address data security during the disposition of IT assets.

IEEE 2883-2022: Private Sector

The IEEE 2883-2022 was created by the IEEE which has been creating standards since it began in 1963. Unlike NISPOM or NIST 800-88, IEEE standards are designed for the private sector, and 2883-2022 in particular is designed to provide clarity into data sanitization and destruction.[13]

PROCESS

NISPOM

The NISPOM standard, like DoD 5220.22, does not lay out detailed guidelines for the data destruction process, saying only:

[12] National Institute of Standards and Technology (NIST). "NIST Special Publication 800-88, Revision 1; Guidelines for Media Sanitization." Section 1.2. nist.gov. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf

[13] IEEE Standards Association. "IEEE 2883-2022: IEEE Standard for Sanitizing Storage." ieee.org. https://standards.ieee.org/ieee/2883/10277/

> *Classified information identified for destruction shall be destroyed completely to preclude recognition or reconstruction of the classified information in accordance with procedures and methods prescribed by agency heads. The methods and equipment used to routinely destroy classified information include burning, cross-cut shredding, wet-pulping, melting, mutilation, chemical decomposition or pulverizing.* [14]

For more detailed instructions, it refers readers to other government organizations.[15]

NIST 800-88

Where the NISPOM standard gives little direction, the NIST 800-88 gives more detailed instructions throughout the document. In Appendix A, instructions are laid out for hard copy storage, networking devices, mobile devices, office equipment, magnetic media, external hard drives, optical media like DVDs, flash memory-based storage devices, and RAM and ROM-based storage devices, breaking these categories up to give more detailed directions for the equipment that falls under each category.[16]

NIST's standards of clearing, purging and destroying data-bearing devices are also given in detail. These guidelines are mentioned earlier in this document, but the practicalities are further detailed below.

[14]eCode of Federal Regulations. "National Industrial Security Program Operating Manual (NISPOM)." 32 CFR 2001.47. Ecfr.gov. https://www.ecfr.gov/current/title-32/subtitle-B/chapter-XX/part-2001/subpart-E/section-2001.47

[15]eCode of Federal Regulations. "National Industrial Security Program Operating Manual (NISPOM)."32 CFR Part 117. Ecfr.gov. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117#p-117.18(b)

[16]National Institute of Standards and Technology (NIST). "NIST Special Publication 800-88, Revision 1; Guidelines for Media Sanitization." Appendix A. nist.gov. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf

Clear: Clearing often involves a factory reset where applicable, but for hard drives and storage disks, it requires overwriting with a single pass.

Purge: Purging for NIST overlaps with destruction, so some purging guidelines call for the destruction of the hardware or call for methods that may render the device unusable. Often it requires cryptographic erase or degaussing for magnetic media.

Destroy: Destroying, depending on the media, typically involves shredding, disintegration, pulverizing or incineration.

Because NIST provides a philosophy in how to securely deal with data-bearing devices, its standards apply to devices not listed in Appendix A. However, many organizations turn to these standards to ensure that they are aligning with best practices and seek confirmation about their data destruction methods. Giving extra guidance on the most effective methods to deal with different types of data-bearing devices helps IT leaders align with best practices and be reassured that their methods are effective.

IEEE 2883-2022

The IEEE recommends using data sanitization techniques that enable the reuse

of IT hardware but when devices contain extremely sensitive information, it recommends destruction.[17] IEEE provides media-specific and interface-specific techniques, providing more comprehensive instructions than NISPOM, and it also provides instructions for data-bearing devices that were not covered under NIST.

Clear: For clearing, IEEE states that the device must be sanitized using logical techniques on user data on all addressable storage locations. This protects against non-invasive data recovery techniques.

Purge: Purging requires sanitization using logical techniques or physical techniques that make data recovery infeasible using laboratory techniques. Under IEEE, purging processes must leave the device in a state where it can be reused, taking a step away from NIST's guidelines where purging methods may destroy the device.

Destruct: Unlike the other standards listed, accepted destruct methods do not include shredding or pulverizing, and IEEE acknowledges the limitations of degaussing and gives additional guidance for when it is used. Acceptable methods include melting, incineration and degaussing.

[17]Bitraser, "NIST 800-88 Vs IEEE 2883-2022 | A Comparison of Data Sanitization Standards." Bitraser.com. https://www.bitraser.com/blog/nist-800-88-or-ieee-2883-a-comparison/

DOCUMENTATION REQUIREMENTS

NISPOM

The NISPOM standard requires documentation on each data-bearing device destroyed or sanitized, but it does not give specific guidelines on what should be included. It requires the records of destruction to be maintained.[18]

NIST 800-88

NIST documentation asks that a certificate of media disposition be completed for each piece of electronic media that has been sanitized. The relevant passage is excerpted below:

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

[18]Bitraser. "DoD 5220.22 Vs IEEE 2883-2022 | Data Sanitization Standards Comparison." Bitraser.com. https://www.bitraser.com/blog/dod-5220-22-vs-ieee-2883-2022-comparison/

data to record depends on the confidentiality level of the data on the media. For a large number of devices with data of very low confidentiality, an organization may choose not to complete the certificate.[19]

When fully completed, the certificate should record at least the Manufacturer, Model, Serial Number, the number the equipment was assigned by the organization, Media Type (i.e., magnetic, flash memory, hybrid, etc.), Media Source (i.e., user or computer the media came from) Sanitization Description (i.e., Clear, Purge, Destroy), Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.), Tool Used (including version), and Verification Method (i.e., full, quick sampling, etc.).

For the person who completed the data destruction, information should include: Name of Person, Position/Title of Person, Date, Location, Contact Information and Signature.

Optional information includes Pre-Sanitization Confidentiality Categorization, Post-Sanitization Confidentiality Categorization, Post-Sanitization Destination, and if/where the data was backed up.

After being sanitized, quality control measures should verify the sanitization of the data.[20]

[19]National Institute of Standards and Technology (NIST). "NIST Special Publication 800-88, Revision 1; Guidelines for Media Sanitization." Section 4.8. nist.gov. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf
[20]National Institute of Standards and Technology (NIST). "NIST Special Publication 800-88, Revision 1; Guidelines for Media Sanitization." Section 4.8. nist.gov. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf

IEEE 2883-2022

IEEE does not require documentation but recommends documenting anyway to maintain compliance with other regulations organizations may be governed by.[21] These regulations may include internal policies; regulations imposed by law, including HIPAA or FACTA; and regulations from voluntary certifications, like the R2 certification governing participating ITAD providers.

SUSTAINABILITY

NISPOM

NISPOM, like DoD before it, does not take a stance on sustainability initiatives. Its guidance for more passes during wipes wears out the storage devices more quickly, but its policies often allow for equipment reuse.

NIST

Clear and purge methods may be more appropriate than destroying data-bearing decives when factoring in environmental concerns, the desire to reuse the media (either within the organization or by selling or donating the media), the cost of media devices, or difficulties in physically destroying some types of media.[22]

[21]Bitraser, "NIST 800-88 Vs IEEE 2883-2022 | A Comparison of Data Sanitization Standards." Bitraser.com. https://www.bitraser.com/blog/nist-800-88-or-ieee-2883-a-comparison/

[22]National Institute of Standards and Technology (NIST). "NIST Special Publication 800-88, Revision 1; Guidelines for Media Sanitization." Section 4. nist.gov. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-88r1.pdf

IEEE

IEEE is clear about its intentions regarding sustainability, preferring equipment to be kept in a reusable state whenever possible. However, its destruction methods exclude shredding and crushing, popular methods for data destruction that allow for material recovery. Instead, IEEE calls for melting and incineration which require more energy and do not allow for any material recovery.

LIMITATIONS

The trend in hardware disposal and data sanitization is toward risk-based security rather than compliance-based. This philosophy helps to keep data secure, no matter where it is housed. However, each of the data detruction guidelines is limited by the time in which it was written, and while each aims to have a forward thinking-approach towards the sanitization of emerging technologies, they may not have guidelines that advise how to sanitize equipment produced after its publication.

NISPOM

NISPOM does not give clear instructions about data destruction and pushes users to look at other government sites.[23] It does not mention devices in particular or give examples of effective methods. However, to sanitize data, it requires three passes minimum, not just a factory reset, so its minimum form of clearing data is the highest among those listed.

[23]eCode of Federal Regulations. "National Industrial Security Program Operating Manual (NISPOM). Ecfr.gov. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-117

NIST

The NIST standard gives clearer data about hardware, providing helpful charts about what methods should be used for different types of equipment. It is also clear about providing verification that equipment has been sanitized. However, its specificity causes problems with equipment that is not mentioned. For certain types of equipment, it gives no middle option between clearing and destroying which some may find confusing or limiting.

IEEE

IEEE is the only standard discussed that is not government-sponsored. It was created entirely for the private sector. It aims to be even more specific than NIST, and while this is helpful now, it may cause it to age more quickly. It considers crushing and shredding to be ineffective forms of data destruction, preferring melting and incineration. These processes are more expensive, requiring more energy than shredding and crushing, and they completely eliminate material recovery. Though encouraged, IEEE does not require documentation, which may cause inefficiencies in verification. Quality ITAD providers will generate these documents for you anyway upon request.

MAKING THE RIGHT DECISIONS

NISPOM, NIST and IEEE guidelines all offer guidance for organizations looking to safely dispose of data. All have their specific use cases, so when choosing

between these standards, it is important to take into account. Where the equipment comes from, the type of equipment, the type of data and location.

To ensure alignment with data sanitization best practices, many organizations turn to ITAD providers. ITAD companies provide data sanitization, destruction, ewaste management, and equipment and materials recovery for businesses across all industries.

Vetting an ITAD provider can be overwhelming if you don't know what you're looking for. CentricsIT has more than 17 years of global ITAD experience, offering sustainable and secure ITAD services. With a reputation for excellence, CentricsIT has been profiled by Gartner and CRN. Our team prioritizes customer service and making the ITAD process as simple—and secure—as possible. We maintain multiple certifications, including ISO 9001, ISO 14001, ISO 45001 and R2v3 to demonstrate our commitment to our clients, to our employees and to the environment.

CentricsIT
SECURE SUSTAINABILITY

WE ALL KNOW HOW IT ENDS.

Even the most cutting-edge equipment becomes obsolete, but it still contains data that needs to be protected. A good ITAD plan keeps data safe, preventing breaches and leaks from your old devices. To learn more about ITAD planning, contact our team.