blancco

NIST SP 800-88 “Media Sanitization Guidelines” Quick-Start Guide

An Overview of End-of-Life Digital Erasure According to the U.S. National Institute of Standards and Technology

October 2019

Table of Contents

When it comes to ensuring your data is completely and irretrievably removed from any digital storage device, the United States government has developed a couple of highly respected options.

One of them, NIST Special Publication 800-88 (NIST 800-88), Revision 1, "Guidelines for Media Sanitization," has gone beyond the federal sector into state and local government, education (both public and private) and private industry use. Highly regulated industries, such as healthcare and financial services and insurance, as well as others with rigorous standards for protecting confidential information, often require or refer to NIST guidelines to protect confidential data across the data lifecycle. It's use is also surpassing another popular, but now outdated standard, DoD 5220.22-M, which was published by the U.S. Department of Defense when magnetic hard disk drives—the only media addressed in the DoD standard—were the primary data storage devices used. The DoD standard has been updated multiple times and 1) no longer specifies a method of sanitization and 2) defers sanitization methods to other government organizations (Cognizant Security Agencies).

The DoD standard has been updated multiple times and 1) no longer specifies a method of sanitization and 2) defers sanitization methods to other government organizations (Cognizant Security Agencies).

Published by the National Institute for Standards and Technology, NIST SP 800-88 assists data custodians in determining how to treat media when the data it holds—particularly sensitive or confidential data—is either no longer needed or must otherwise be rendered irretrievable. "Media" can include hard copy paper media, printers and other hardware and digital storage devices. The publication's overall decision-making workflow applies to all of these.

Though NIST SP 800-88 (or simply, "NIST") covers several different forms of data sanitization, including physical destruction, in this paper our focus will be on digital storage devices. NIST addresses magnetic drives, flash-based drives (SSDs for example), optical media, devices using Crypto Erase and more. It covers everything from mobile devices and removable USB drives to servers—and even technologies not yet developed. It also lays out very clear actions for media sanitization: ***Clear, Purge or Destroy***. With these clear categories, both private and public-sector organizations can easily specify which level of sanitization best applies to the data and media in question.

In the following pages, we'll lay out the primary factors that NIST 800-88 relies on to determine the category of sanitization appropriate for your data destruction needs.

Types of NIST 800-88 Sanitization

Before diving into how NIST approaches protecting data on digital storage media, there are some important points to mention:

1. **NIST 800-88 applies throughout an information system's lifecycle:** It applies at the beginning, when system infrastructure is being planned, procured and deployed (these decisions will affect your data sanitization processes later); in the middle, when situations merit sanitizing media because of maintenance, outsourced projects or other interim data handling such as data management practices for retention and targeted erasure; and at the end, when media moves from a more secure setting (e.g., a highly protected data storage area) to a lesser one (e.g., to another department or outside the organization).

2. **Data sanitization crosses organizational roles.** Before any data manager moves forward with media sanitization, best practice is to involve key stakeholders within the organization: data retention specialists, privacy officials and those responsible for Freedom of Information Act or historical archives. See NIST SP 800-88 Rev. 1 Chapter 3, "Roles and Responsibilities" for more on this principle.

When media has reached end-of-life, one of three NIST 800-88 sanitization categories is often required to meet regulatory and internal data protection processes. Because reformatting, wiping and even encryption may not be enough to protect all information stored on digital devices, NIST 800-88 specifies these actions for end-of-life data: *Clear, Purge* and *Destroy.*

Table 1.

NIST Sanitization Actions Comparison Table

	CLEAR	PURGE	DESTROY
NIST Description + Process Notes	***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*** applies physical or logical techniques that render Target Data recovery infeasible using state-of-the-art laboratory techniques. The Purge process includes removing hidden drives (Host Protected Areas, or HPA) and Device Configuration Overlays (DCO), if they're present, triggering a firmware-based command, then verifying the write.	***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. More than simply making the media unusable via a standard user interface, NIST's "Destroy" process means that even state-of-the art techniques cannot retrieve data off any part of the residual media.
When to Use	Clear is typically appropriate when data is less confidential, or when any harm that would result from data exposure or access is more minimal. Clear is also often used for repurposing assets within an organization (i.e., sanitizing all data before a new user gets access to the asset).	Purge is used for data requiring higher levels of protection. It can be used alone or in conjunction with "Destroy" methods.	If media are not intended for reuse due to damage or other reason, the simplest and most cost-effective method of control may be destruction, depending on the media type. However, the cost and risk of applying only physical destruction methods depends on the confidentiality of the data stored, the value of the media type, and the sufficiency of the destruction methods available.
Pros	Most devices support some level of Clear sanitization. Clear provides a moderate level of data protection. Clear allows reuse of the device.	Purge provides a much more thorough level of sanitization than Clear and is used for more confidential data. Purge allows reuse of the device.	In some cases, "Destroy" can be less expensive than other methods, particularly if reuse is not a goal. It can also render data irretrievable when original media is too damaged to undergo other sanitization methods.
	In addition to allowing reuse, Purge (and at times, Clear) may be preferred over Destroy when factoring in environmental concerns, the cost of the media or device, or difficulties in physically Destroying some types of media.		
Cons	Clear does not affect all hidden or unaddressable areas on SSD drives. The Clear level of protection is not always suitable for more confidential data.	Purge cannot always be applied to all devices based on the firmware involved. However, Blancco's Research and Development teams regularly tackle such instances, and Blancco solutions support Purge for most HDD and SSD drives today.	Destroy renders media unusable for future data storage. Technology advances can outpace sufficient destruction methods. Examples include dense storage components damaging shredding equipment, insufficient shred size or degaussing techniques that can't overcome newer, stronger levels of coercivity (magnetic force). If destruction is inadequate, advanced recovery techniques may be able to access the data, leaving it vulnerable to unauthorized access even if the media itself is no longer usable. Destroyed hard drives also contribute to e-waste.

Note: In cases of highly confidential or high-risk data where the destruction method may still leave information vulnerable, coupling "Purge" methods with "Destroy" methods is the most secure option.

Appendix A in the NIST document lays out specific techniques and considerations for various media types. However, consistent with its future-forward approach, organizations have the freedom to choose methods not specifically listed in the NIST guide as long as they "satisfy the intent of Clear, Purge, and Destroy." Other methods may be suitable if they are 1) verified and 2) found satisfactory by the organization.

It's important to know that Clear, Purge and Destroy have specific meanings. For instance, when it comes to sanitization, NIST "Destroy" requires using techniques and equipment adequate to the task for each media type (See NIST SP 800-88 Appendix C), along with verifying that retrieval of target data is infeasible using state-of-the-art laboratory techniques. Simply rendering media or a media device unusable by destructive methods such as cutting, shredding, or using magnets does not guarantee NIST sanitization, particularly when the media type and destruction method are mismatched (i.e., destruction methods that may be effective for HDDs differ from those that are effective for SSDs).

Factors Influencing Media Sanitization Decision Making

The NIST definition of "sanitization" is "a process that renders access to target data on the media infeasible for a given level of effort."

The methods an organization might choose to use to sanitize its data depends heavily on the confidentiality level of the data it is trying to protect. NIST 800-88 outlines several decision-making factors:

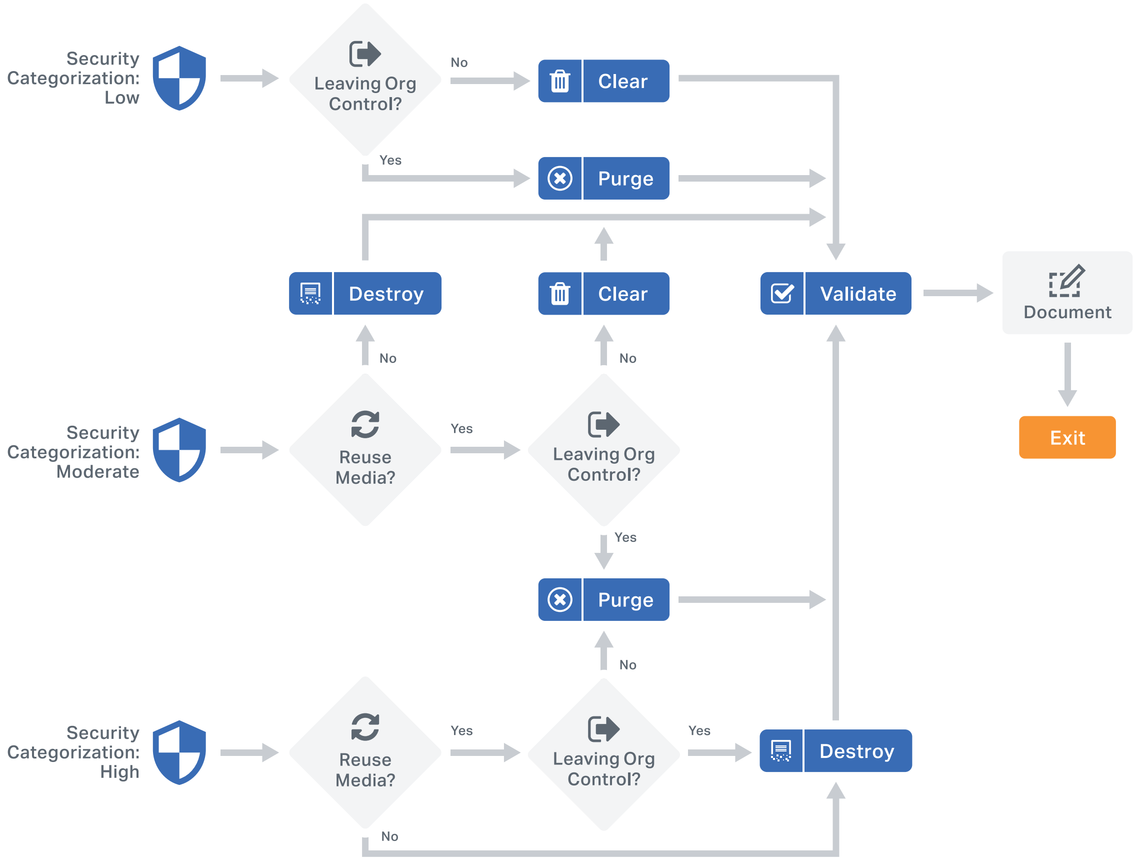
- ✓ Security categorization (based on confidentiality and risk of exposure)
- ✓ Intended future use (including reuse of media either external or internal to the organization and resulting protection levels)
- ✓ Anticipated volume of media by type of media
- ✓ Financial and time cost to sanitize
- ✓ Environmental impact of disposition
- ✓ Technology/sanitization tools available
- ✓ Personnel skills available

> The NIST definition of "sanitization" is "a process that renders access to target data on the media infeasible for a given level of effort."

Of the above list, the NIST 800-88 decision-making workflow relies heavily on security categorization and intended future use, as illustrated by the NIST "Sanitization and Disposition Decision Flow" graphic on the next page. We'll cover the primary decision points in the following pages.

Figure 1.

NIST Sanitization and Disposition Decision Flow



Security Categorization: Low, Moderate, High

NIST uses security categories from Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems" when determining confidentiality levels. FIPS 199 provides a matrix on how to prioritize the security ***category*** (based on potential impact of confidentiality loss), ***controls*** (prescribed management, operational and technical controls used to protect the security objective) and ***objective*** (confidentiality, integrity and availability) of the data or information system.

FIPS 199 security **categories** for the "Confidentiality" **objective**—the primary focus of end-of-life data destruction—are Low, Moderate and High:

Table 2.

Selection from FIPS 199 "Potential Impact Definitions for Security Objectives" table

SECURITY OBJECTIVE	POTENTIAL IMPACT		
	LOW	MODERATE	HIGH
Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe** or **catastrophic adverse effect** on organizational operations, organizational assets, or individuals.

> Whether choosing Clear, Purge, or Destroy, every resulting NIST 800-88 sanitization level decision ends the same: Validation and Documentation.

Intended Future Use: Organizational Control and Reuse

Once the security categorization, of Low, Moderate or High is determined for the media that is being disposed, the next decision-making factor is how that media is intended to be reused:

- ✓ Will it be provided to a different organization entirely, perhaps through sale, donation or return (if leased)?
- ✓ Will it be erased and used within the same department or another department, possibly to conserve resources?
- ✓ Are environmental concerns a priority, with recycling being a preferred option?

In each case, an organization must evaluate how critical it is to protect its Low, Moderate or High-confidentiality data when media changes hands—even internally. This typically means that data will no longer be protected at its original confidentiality protection levels once it is being reused elsewhere.

Other Factors

While the flowchart itself doesn't address the following items, other factors to consider include:

- **Anticipated volumes** (e.g., megabyte, gigabyte, and terabyte) of media by type (e.g., optical non-rewritable, magnetic) – Are you sanitizing a fleet of leased workstations, a trove of mobile phones, an entire data center or simply a moderate collection of SSDs used for a single department?
- **Financial and time costs to sanitize** – What is the cost of sanitization when considering tools, training, verification and reentering media into the supply stream? How long will it take? How will other business processes be affected while media is being processed? Can the process be automated?
- **Environmental impact of disposition** – Will components be able to be reused, repurposed or recycled, or will they be Destroyed and taken to a landfill?
- **Technology/sanitization tools available** – Whether done in-house or outsourced, are the tools available adequate to ensure complete sanitization? Is the equipment checked regularly to ensure it functions correctly?
- **Personnel skills available** – Are in-house or outsourced personnel trained in both conducting sanitization processes for the types of media in question, as well as evaluating that complete sanitization has taken place?

Ultimately, the purpose of the decision-making flow chart and the NIST Media Sanitization Guidelines is to help organizations choose a solution that best lessens the risk of breaching confidentiality while respecting any other constraints involved. But whether choosing Clear, Purge, or Destroy, every resulting NIST 800-88 sanitization level decision ends the same: Validation and Documentation.

Minimum Sanitization Requirements

Once an organization has decided what type of sanitization is needed based on the workflow and other considerations, NIST 800-88: Appendix A can be a valuable reference for determining recommended sanitization processes for specific media types.

Appendix A details applicable Clear, Purge and Destroy minimums for:

- **Hard Copy Storage** (paper and microforms)
- **Networking Devices** (routers and switches)
- **Mobile Devices** (Apple, Blackberry, Android, Windows and other smartphones, tablets, etc.)
- **Office Equipment** (copy, fax, print and multi-function machines)
- **Magnetic Media** (floppies, disks, tapes, ATA hard disk drives and SCSI hard disk drives)
- **Peripherally Attached Storage** (USB, firewire and other external locally attached hard drives)
- **Optical Media** (CD, DVD and BD)
- **Flash Memory-Based Storage** (ATA solid-state drives and SCSI SSDs, NVMes, USB removable media, memory cards and embedded flash memory on boards and devices)
- **RAM- and ROM-Based Storage** (DRAM, EAPRO and EEPROM)

Blancco's data erasure services support NIST Clear or NIST Purge across most digital media, including NIST-compliant data sanitization across loose drives and SSDs within laptops, PCs, servers and more using our patented SSD erasure method.

Verification Methods and Document Requirements

What Verification Entails

NIST Media Sanitization Guidelines lays out two options for verification:

- Verification that sanitization has been applied to all media in question (typically not applicable for each piece of media when using "Destroy")
- Verification of a sample of the media to show that no data is recoverable

If possible, the personnel who sanitize and the personnel who verify media sanitization should be different groups. For low-risk tolerance situations, where you may conduct both full verification and then sampled verification when erasing a set of devices, a different verification tool should be used for full than is used for sampled.

About full verification of a device – When supported by the device interface, the highest level of assurance outside of a laboratory is typically achieved by inspecting all accessible areas for the expected sanitized value.

About sampled verification of a device – If an organization chooses representative sampling, then NIST lays out three specific best practices for selecting locations to be sampled when verifying electronic media sanitization.

These media verification best practices are:

1. Selecting pseudorandom locations on the media each time the analysis tool is applied.
2. Selecting locations across the addressable space (user addressable and reserved areas) according to NIST parameters for sampling by subsections.
3. Following NIST's parameters for sample selections to cover at least 10 percent of the media.

Cryptographic Erase has different verification considerations, because the contents of the physical media following Cryptographic Erase may not be known and therefore cannot be compared to a given value. However, verifying Cryptographic Erase also involves selecting pseudorandom locations from sampled sections across the media.

A Note on Cryptographic Erase

Cryptographic Erase, which erases "keys" that allow access to the data rather than erasing the data itself, has different verification considerations.

Cryptographic Erase (or "Crypto Erase") can be used with other sanitization methods, but it's important to be fully confident on how well protected any "back-up keys" are, when Cryptographic Erase has been used, and how strong the algorithms are. NIST 800-88 provides best practices for this sanitization method and for verification in "Background: Use of Cryptography and Cryptographic Erase" as well as "Appendix D: Cryptographic Erase Device Guidelines."

Blancco solutions support NIST Purge cryptographic erasure for various devices, including for drives and mobile phones. We also invite you to download our technical white paper, "The Crypto Erase Conundrum: What's Your Organization's Risk Tolerance?" to dive into the technology behind cryptographic erasure and learn cryptographic erasure's strengths and weaknesses.

What Documentation Looks Like

Finally, proof of NIST 800-88 sanitization comes in the form of a detailed certificate for each piece of electronic media that has been sanitized. This certificate can be printed or electronic, but it is a critical element that validates that data has been rendered irretrievable from the media that has been sanitized.

Proof of sanitization, such as the tamper-proof certificates of erasure provided through Blancco erasure solutions, typically lists each storage device by serial number. A proper certificate also describes the type of sanitization (i.e., Clear, Purge, Destroy), method used (e.g., degauss, overwrite, block erase, crypto erase), the tools and the verification methods used and several other pieces of information.

Without proof of sanitization in the form of a NIST-compliant certificate, NIST sanitization is neither complete nor guaranteed.

For any organization that must prove compliance with data security regulations and guidelines (such as those in government or heavily regulated industries), it is especially important to maintain these records for audit purposes. Audit-ready certificates validate that the media has been adequately sanitized to NIST Clear, Purge or Destroy standards, no matter where along the media lifecycle that level of sanitization has occurred.

Conclusion

NIST 800-88 has become the go-to standard for ensuring that data is safe from unauthorized access when host storage devices transition to their next destination.

Whether you intended to reuse, return, recycle, sell or donate your digital storage media, or whether your final decision lands firmly in destroying it, we invite you to contact Blancco to ensure that your confidential data is securely and completely sanitized according to NIST 800-88 Clear or NIST 800-88 Purge standards before media leaves your control.

Need more information? Download our solution brief, "How Blancco Helps Organizations Achieve Compliance with NIST SP 800-88," or contact us for a free data erasure trial.

About Blancco

Blancco is the industry standard in data erasure and mobile device diagnostics software. Blancco data erasure solutions provide thousands of organizations with the tools they need to add an additional layer of security to their endpoint security policies through secure erasure of IT assets. All erasures are verified and certified through a tamper-proof audit trail.

Blancco data erasure solutions have been tested, certified, approved and recommended by 15+ governing bodies and leading organizations around the world. No other data erasure software can boast this level of compliance with the rigorous requirements set by government agencies, legal authorities and independent testing laboratories.

With Blancco Mobile Insurance, Blancco Mobile Buy-back/Trade-in and Blancco Mobile Retail solutions, organizations can achieve real-time valuation for mobile devices with a simple solution that enables consistent, accurate and measurable testing, including market-leading cracked-glass detection.

Additionally, mobile processors can achieve operational excellence while maximizing profits with Blancco Mobile Diagnostics & Erasure—a purpose-built solution that features our industry-leading Blancco Mobile Workflows for key processing insights across the entire mobile device lifecycle.

For more information, visit our website at www.blancco.com.

Contact Us

For Marketing, please contact:
Email: marketing@blancco.com

For Corporate Communications & PR, please contact:
Email: press@blancco.com