How Blancco Helps Organizations Achieve Compliance with NIST SP 800-88

What is NIST SP 800-88?

Publications in NIST's Special Publication (SP) 800 series are targeted at providing "guidelines, recommendations, technical specifications and annual reports of NIST's cybersecurity activities." These publications are designed to support the needs of U.S. Federal government institutions, though they have been referenced by organizations in many different industries. NIST SP 800-88, specifically, was created by NIST in accordance with its statutory responsibilities under the Federal Information Security Management Act of 2002 (FISMA) to outline information security standards and guidelines around media sanitization. Compliance with the publication is mandatory by the U.S. Federal government but may also be used by nongovernmental organizations on a voluntary basis.

Blancco helps organizations across a wide range of industries comply with NIST SP 800-88. See the chart below for some examples of specific areas of the document and how Blancco can help address them.

FROM THE PUBLICATION	HOW BLANCCO HELPS
"Clear, Purge, and Destroy are actions that can be taken to sanitize media. The categories of sanitization are defined as follows: **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. **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." 'It is suggested that the user of this guide categorize the information, assess the nature of the medium on which it is recorded, assess the risk to confidentiality, and determine the future plans for the media. Then, the organization can choose the appropriate type(s) of sanitization. The selected type(s) should be assessed as to cost, environmental impact, etc., and a decision should be made that best mitigates the risk to confidentiality and best satisfies other constraints imposed on the process."	Blancco supports both NIST Clear and NIST Purge methods of data sanitization through its software-based data erasure solutions. Blancco Drive Eraser achieves Purge-level sanitization on SSDs, including NVMes, and on HDDs in SANs, servers, laptops and PCs. Additionally, Blancco LUN Eraser meets NIST Clear requirements for data sanitization of logical unit drives. Every Blancco erasure is verified and certified by an audit-ready, tamper-proof Certificate of Erasure. Additionally, Blancco software-based erasure enables improved operational efficiency, reduces handling costs and increases control of the data sanitization process.
(Referring to Cryptographic Erase): "Due to the difficulty in reliably ensuring that partial sanitization effectively addresses all sensitive data, sanitization of the whole device is preferred to partial sanitization whenever possible."	Blancco Drive Eraser targets every portion of the drive during erasure, including remapped sectors and remove hidden areas. In both magnetic and SSD dives, Blancco Drive Eraser offers overprovisioning to handle wear leveling. This guarantees 100% data sanitization and is backed by a tamper-proof report.

Continued...

FROM THE PUBLICATION	HOW BLANCCO HELPS
"Purge (and Clear, where applicable) may be more appropriate than Destroy 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 a media or media device, or difficulties in physically Destroying some types of media."	Blancco data erasure solutions permanently remove data from a wide range of end-of-life devices so that they can be safely reused, reassigned or resold into the second-hand market. This is good for the environment and encourages cost savings. It's also an established best practice, with 100s of millions of IT assets currently being securely redeployed across the globe.
"Verifying the selected information sanitization and disposal process is an essential step in maintaining confidentiality. Two types of verification should be considered. The first is verification every time sanitization is applied…" "Following sanitization, a certificate of media disposition should be completed for each piece of electronic media that has been sanitized." "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., magnetic, flash memory, hybrid, etc.) • Media Source (i.e., user or computer the media came from) • Pre-Sanitization Confidentiality Categorization (optional) • Sanitization Description (i.e., Clear, Purge, Destroy) • Method Used (i.e., degauss, overwrite, block erase, crypto erase, etc.) • Tool Used (including version) • Verification Method (i.e., full, quick sampling, etc.) • Post-Sanitization Confidentiality Categorization (optional) • Post-Sanitization Destination (if known) • For Both Sanitization and Verification: • Name of Person • Title of Person • Date • Location • Phone or Other Contact Information • Signature"	Every time an erasure is performed using Blancco software, a tamper-proof, audit-ready Certificate of Erasure is issued to verify and certify that the erasure was a success. These certificates may include custom fields and include important details about both the asset and the erasure standard used, along with a secure digital signature that fully complies with NIST requirements. Reports may be stored, managed and accessed at any time in the Blancco Management Console, available in on-premise or as a cloud service hosted by AWS.

Continued…

FROM THE PUBLICATION	HOW BLANCCO HELPS
"USB Removable Media- This includes Pen Drives, Thumb Drives, Flash Memory Drives, Memory Sticks, etc. **Clear:** Overwrite media by using organizationally approved and tested overwriting/methods/tools. The Clear pattern should be at least two passes, to include a pattern in the first pass and its complement in the second pass. Additional passes may be used."	To meet and exceed NIST 800-88 requirements, as well as other data erasure standards, Blancco Removable Media Eraser is designed to securely and permanently erase many different types of removable media, including SD cards, thumb drives, flash memory drives, etc. A Certificate of Erasure is issued upon verification of the erasure.
"Mobile Devices (If a device has removable storage – first check for encryption and unencrypt if so – then remove the removable storage prior to sanitization)." The special publication then goes on to describe specific methods of data sanitization for each major mobile device brand, including Apple, Android, Windows and Blackberry. Devices should be sanitized in one of the following ways: factory reset, overwriting,or Cryptographic Erase to meet Clear or Purge requirements. Alternatively (or in addition), these devices may also be physically destroyed if they cannot be reused, recycled or resold. When possible, verification of erasure should be provided.	Blancco Mobile Diagnostics & Erasure securely erases iOS, Android, Windows Phone and BlackBerry operating systems, meeting and exceeding the requirements set forth by NIST 800-88. **With BMDE you can:** • Choose the NIST data erasure standard, cryptographic erasure, verified factory reset and several other mobile erasure standards • Verify the overwriting standard was a success and written to all sectors of the device • Guarantee permanent data removal with a 100% tamper-proof audit trail • Experience full automation and volume processing Additionally, Blancco Mobile Diagnostics & Erasure offers capabilities to erase SD cards and other storage media while still residing inside the mobile device.
"Copy, print and fax machines- **Clear:** Perform a full manufacturer's reset to reset the office equipment to its factory default settings **Purge:** See Destroy. Most office equipment only offers capabilities to Clear (and not Purge) the data contents. Office equipment may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. Office equipment may have removable storage media, and if so, media-dependent sanitization techniques may be applied to the associated storage device. **Destroy:** Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator."	Blancco Drive Eraser securely wipes HDDs present in printer/fax/copy machines to Purge levels when NIST Purge is the chosen data erasure standard. A Certificate of Erasure is issued upon verification of the erasure. Blancco Removable Media Eraser is designed to securely erase many different types of removable media, including SD cards and other data storage in printers, fax machines, etc. A Certificate of Erasure is issued upon verification of the erasure.

Continued...

blancco

FROM THE PUBLICATION	HOW BLANCCO HELPS
"ATA Hard Disk Drives- This includes PATA, SATA, eSATA, etc. **Clear:** Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used." The text presents four options for sanitization: the ATA Sanitize Device feature set commands (via one or three overwriting wipes), the SECURE ERASE UNIT command, Cryptographic Erase through the Trusted Computing Group (TCG) Opal Security Subsystem Class (SSC) or Enterprise SSC interface or degaussing.	Blanco Drive Eraser software erases loose drives and HDDs within laptops, PCs, servers and more to support automated sanitization processes that fulfill NIST requirements for all drive types, including PATA, SATA, eSATA and Clear. **Key Benefits of Blancco Drive Eraser:** • Erases data permanently from multiple HDDs simultaneously • Automates the hard drive erasure process to remove BIOS freeze locks • Local and remote deployment • RAID dismantling and pass through • Identifies false positives during internal data erasure processes • Provides digitally-signed Certificate of Erasure for auditing and compliance • Compliant with all state, Federal and international data privacy regulations and guidelines Blancco Drive Eraser supports the NIST Purge and NIST Clear erasure standards, backed by verification and certification of the process.
"SCSI Solid State Drives (SSSDs) — This includes Parallel SCSI, Serial Attached SCSI (SAS), Fibre Channel, USB Attached Storage (UAS), and SCSI Express." The special publication suggests three methods of sanitization. The first is Clear, in which the user would "[o]verwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used." The second is Purge using the SCSI SANITIZE, BLOCK ERASE or CRYPTOGRAPHIC ERASE commands. The third is physical destruction. Similar options are then presented for NVM Express SSDs, with a change of NVM-specific commands for achieving Purge. "Verification must be performed for each technique within Clear and Purge. When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully...Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance. Degaussing must not be performed as a sanitization technique on flash memory-based storage devices."	Blanco Drive Eraser software erases loose drives and SSDs within laptops, PCs, servers and more using our patented SSD erasure method. **Benefits of Blancco Patented SSD Erasure:** • Firmware-Level Erasure: Leverages essential internal erasure commands to sanitize SSDs, including Block Erase and cryptographic erasure • Includes multiple random overwrites, freeze lock removal and full verification • Utilizes all supported SSD security protocols • Ensures all steps are performed and completed in proper order through an automated process • Prevents any compression or deduplication mechanism from being applied by SSD controller • Fills the whole logical capacity of the drive with a random data stream • Uses truly random/uncompressible data, not merely a repeating bit pattern • Ensures data is written across the full logical capacity of the SSD (and not just compressed) with double pass overwrites • Interface agnostic, covering all common SSD interfaces (including SATA, SAS, eMMC and NVMe) • Enables access to key internal SSD security features, which are necessary to ensure total and immutable erasure • Ensures operational validity of the drive • Detects any anomalies in the erasure process • Eliminates false positives • 100% tamper-proof audit trail through digitally signed proof of erasure

Continued...

When building your organization's data sanitization policies to achieve best practice across a variety of IT assets, consider adhering to the recommendations above—and carefully consider the inherent risks and opportunities for your business to best safeguard industry, customer and employee data. Download the IDSC's "Data Erasure Policies & Procedures for IT Assets" template for help getting started.

Why Blancco?

For more than 20 years, Blancco has offered solutions that support compliance with data protection and privacy regulations and guidelines across the globe. As the most certified data erasure software company on the market, with 15+ global approvals and certifications from the likes of NATO and Common Criteria, we support the need for heavily-regulated industries to stay compliant with data erasure solutions that satisfy (and often exceed) these requirements.

Learn more about NIST SP 800-88 Rev 1. Read the blog now.