CIGENT®
AlwaysPROTECTED™

Verified Storage Device Sanitization

White Paper for Utilization of Verified Storage Device Sanitization Technology as an Alternate Approach to current NSA PM 9-12 guidance on Solid-State IS Device Sanitization

Cigent Technologies, Inc.
2211 Widman Way, Suite 150 Fort Myers, Florida 33901 Cage Code: 84DR8
Contact: Tom Ricoy | Tom.Ricoy@cigent.com | 512.529.4439 Technical Contact:
Tony Fessel | Tony.Fessel@cigent.com | Phone: 699.400.8127

Executive Summary

Problem Statement

Sensitive data must be properly secured throughout its lifecycle including ensuring proper disposal. To avoid data compromise, processes and technology need to be in place to verify data erasure during device transitions between personnel or locations, at the conclusion of a mission, when devices are decommissioned, when there are limited resources for destruction, or in emergency situations. Additionally, this destruction must not add to the cost or environmental waste produced by the organization.

An effective approach is required to meet the increasing requirements of data sanitization. The approach must provide unequivocal verification that data has been successfully eradicated, be resource efficient, provide straightforward execution, and support emergency situations. Verified Storage Device Sanitization delivers against these requirements.

Verified Storage Device Sanitization (VSDS)

VSDS provides a capability that scans block-by-block to ensure all user data has been permanently erased. The technology displays results allowing operators to quickly ascertain if all data has been erased. *The effective, efficient approach validates that all data has been erased removing the need for physical destruction.*

Key benefits of verified storage device sanitization:

- Effective emergency data sanitization while minimizing personnel risk
- Increase data sanitization by providing simple process
  - Field situations where physical destruction is difficult or impossible
  - Organizations more likely to adopt and follow streamline process
- Eliminates need to physically destroy drives
  - Reduces expense of replacing storage devices
  - Allows for recycling of precious earth metals
- Complies with NIST SP 800-88

This is an existing capability on Cigent Secure Storage Solutions that also deliver AES 256 hardware full drive encryption. The drives are FIPS, NIAP, and CSfC DAR certified. They are available from PC manufacturers including Dell, HP, Getac, Rave Computers, and are deployed at scale and in use across USG DoD, IC, and Defense Industrial Base (DiB) users.

Verified Storage Device Sanitization as a Reliable Alternative to Device Destruction

Problem Statement

Existing guidance requiring the physical destruction of storage devices to prevent data compromise is no longer the optimal approach for ensuring data sanitization. This requirement emerged from studies showing that standard industry methods such as ATA Security Erase, Sanitize, and Format NVM often produced inconsistent results in fully erasing data. Research demonstrated that performing these techniques could not guarantee complete data removal, leading to the development of policies like NSA CSfC DAR (Data at Rest) and NSA/CSS Storage Device Sanitization Manual PM9-12, which mandate physical destruction in specific scenarios.

While physical destruction *may* eliminate the risk of data recovery, its effectiveness varies based on the method and type of media. The approach is neither cost-effective or scalable and is not optimal in emergency situations. Physical destruction is time consuming potentially creating challenges in emergency situations that may put human lives at risk. Additionally, organizations may not follow the guidance due to availability of resources, ignorance, or neglect. For organizations adhering to the protocol, the approach has high costs due to labor, equipment, and disposal. It also permanently destroys valuable storage hardware that could be reused within the same organization. Finally, the physical destruction of hard drives exacerbates environmental issues by wasting precious metals, such as gold, platinum, and rare earth elements.

Given these limitations, Verified Storage Device Sanitization (VSDS) offers a superior solution by allowing users to visually verify complete data removal without the need for physical destruction. VSDS provides a more reliable, efficient, cost effective, and environmentally conscious alternative. Most importantly, the technology can improve data sanitization in emergency solutions and improve adoption of strong data sanitation hygiene, Organizations can meet stringent data sanitization requirements without resorting to costly and wasteful device destruction.

Physical Destruction Limitations

The proliferation of types and volume of devices with sensitive data is increasing the need to update data sanitization guidance. The physical destruction approach is no longer optimal as illustrated in the following scenarios:

1. **Emergency situations**: Physical destruction requires multiple steps that may be unable to be performed in time, compromising sensitive data. Emerging technology – including manned and unmanned vehicles and missions are complicating this risk.

   *Real-World example***:** On April 1, 2001 a US Navy EP-3E Aries II made an emergency landing on Chinese controlled Hainan Island following a mid-air collision with a Chinese aircraft. Despite the crew's efforts they were only partially successful in their destruction of classified material. Some of the material they failed to destroy included cryptographic keys, signals intelligence manuals, and the names of National Security Agency employees.[1]

Real-World example: When an unmanned vehicle loses connection with its pilot or detects an imminent crash landing, SOF teams are sent to retrieve and destroy remaining sensitive data. One such mission involved eight personnel conducting free fall operations in a contested environment to ensure sensitive data was destroyed. Not only was sensitive data on the UAV susceptible to compromise prior to recovery, but securing data required an expensive and risky operation that put lives at risk.

1. **Operators in the field:** The growing mission demands and advancing technical capabilities are leading to an increasing amount of sensitive data being generated at the edge. Operators need to sanitize data but often lack the resources or time to comply with current sanitization guidelines.

   Real-World example: Forces store sensitive data on a device that needs to be wiped prior to exiting their assigned country. Lacking access to physical destruction equipment they may rely on ineffective tools or simply forego any data sanitization. As a result, sensitive data may remain on the drive when passing through a security checkpoint.

2. **Resource intensive:** The process of device destruction is expensive and can unnecessarily deplete resources and budgets. With edge devices collecting, processing, and storing more data at the 'tip of the spear' more storage devices will require physical destruction thus increasing associated costs.

   Real-World example: Standard practice is for pilots to load mission data on external media and upload the information to their airframe computer systems. According to PM9-12, this external media device would . With VSDS it can be reused for the next mission.

4. **Increased resource cost:** A multitude of sources including Forbes and Cybernews forecast a 50% increase in the cost to manufacture storage devices in 2025 due to a reduction in NAND chip production. This increase may remain consistent over time with supply chain shortages causing an astronomical price increase. Reusing these devices will prevent an increased budgetary requirement.

Existing software best practices are unable to consistently ensure data is sanitized. Physical destruction of storage devices is a complex, time-consuming process that is challenged by growing data and device requirements. A new approach to data sanitization is required.

NIST SP 800-88

NIST (National Institute of Standards and Technology) Special Publication 800-88 Revision 1 was written to provide industry guidelines for media sanitization. These guidelines follow

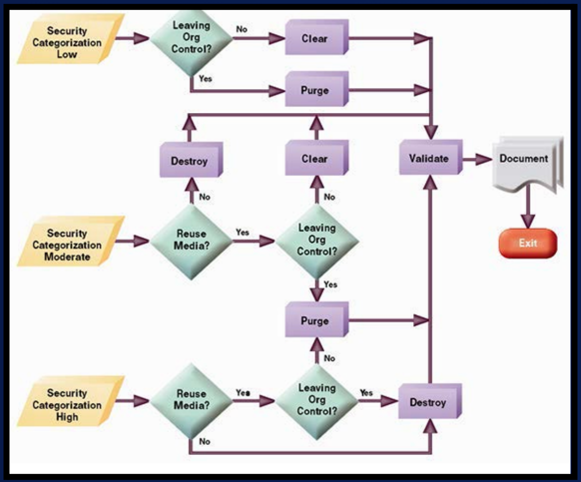
[1] https://en.wikipedia.org/wiki/Hainan_Island_incident

different standards based on the security necessary for the organization. This is broken into low, moderate, and high. The publication provides the following methods of sanitization with their definitions:

- **Clear** - “Applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple, noninvasive data recovery techniques; it is 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” (This is the category referring to VSDS which is described in detail in a later section).
- **Destroy** - “Renders target data recovery (using state-of-the-art laboratory techniques) infeasible and results in the subsequent inability to use the media for storage of data.”
- **Validate** - “The step in the media sanitization process flowchart which involves testing the media to ensure the information cannot be read.” NIST 800-88 also says that verification should be performed “every time sanitization is applied” if possible. VSDS provides a means to both purge and validate the data on storage devices.

NIST SP 800-88 contains a flowchart to depict when a user should use each of the sanitization methods. This flowchart shows that in the highest security categorization (PM9-12 use cases) drives do not need to be destroyed if they can be purged and validated with software. VSDS technology was created for this purpose. Additionally, as previously stated destruction alone should not be the only source of data sanitization.

Cigent believes the appropriate approach for devices intended to be repurposed within the organization should be to purge and then visually verify that the data has been removed. If the device is to be decommissioned, it should be purged, verified, and then destroyed.

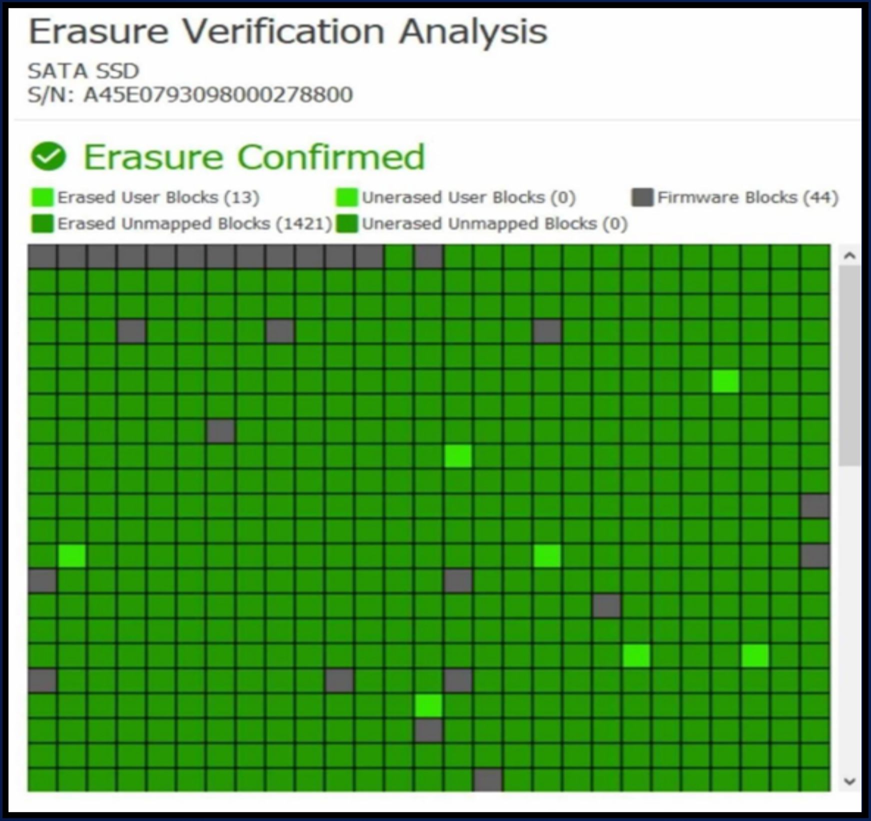


Verified Storage Device Sanitization

Verified Storage Device Sanitization (VSDS) provides firmware-based verification that scans every block on a storage device to verify the block type and whether it has been erased. During development and testing several data recovery companies were hired anonymously to recover data from multiple drives utilizing this technology. They employed both basic and advanced data recovery techniques, including removing flash memory chips and verifying the absence of data. None of the companies were able to recover any user data, thereby confirming that all data had been successfully destroyed.

Using VSDS is straightforward with a Graphical User Interface (GUI) or Command Line Interface (CLI) providing local and remote execution capabilities. This eliminates concerns about data sanitization becoming too complex for the average user. Contributing to the ease of use are the graphical representations provided to the end user, simplifying the process.

Graphic one depicts a successful sanitization attempt as is indicated by the green blocks. User, unmapped and firmware blocks are displayed for the user.



Erasure Verification Analysis

SATA SSD
S/N: A45E0793098000278800

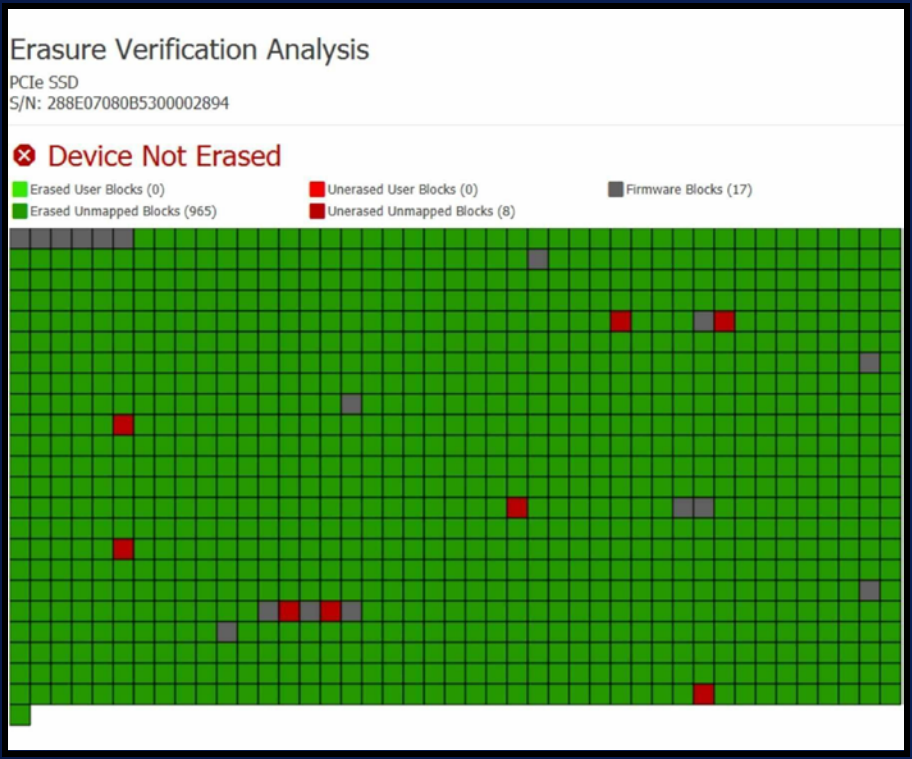
✓ Erasure Confirmed

🟩 Erased User Blocks (13) 🟩 Unerased User Blocks (0) ⬛ Firmware Blocks (44)
🟩 Erased Unmapped Blocks (1421) 🟩 Unerased Unmapped Blocks (0)

Graphic 1: Drive successfully erased

Graphic 2 shows an unsuccessful sanitization attempt and is more common if the storage blocks are reaching the end of their lifecycle. Additional attempts to sanitize the data using

VSDS can be made; however, at this stage, it may be necessary to destroy the drive using physical destruction methods.



Erasure Verification Analysis

PCIe SSD
S/N: 288E07080B5300002894

⊗ Device Not Erased

🟩 Erased User Blocks (0) 🟥 Unerased User Blocks (0) ■ Firmware Blocks (17)
🟩 Erased Unmapped Blocks (965) 🟥 Unerased Unmapped Blocks (8)

Graphic 2: Drive not erased

The drives and software are currently on the NSA CSfC data at rest (DAR) component lists and are successfully deployed in Federal and Defense Industry organizations including SecurView and District Defend.

Data on PC’s, servers, external media, industrial control systems and others can be protected by the VSDS technology.

Benefits of VSDS

1. Effective emergency data sanitization while minimizing personnel risk

As illustrated in real world examples, physical device destruction requirements can be a challenge to execute in an emergency. The multiple and time-consuming steps may increase personnel risk and result in a failure to complete the sanitization process. Cigent VSDS provides a simple and efficient approach, increasing likelihood of successful sanitization and reducing risk to personnel.

With the ability to initiate erasure protocols remotely VSDS addresses scenario where devices are attacked, co-opted, shot down, or otherwise exploited in the field. VSDS eliminates the need to send a team to a dangerous operating area to sanitize a device, aircraft, or drone.

2. **Increase data sanitization by providing simple process**

   VSDS provides a streamline, easy to use option vs the multi-step process of physical destruction that also requires physical equipment. Executing erasure and the verification that data has been eliminated is user friendly mitigating the risk of accidental erasure or the incomplete destruction of sensitive data.

   VSDS simplified approach will allow operators in the field to efficiently complete data sanitization that would be challenging with physical destruction. A simpler, more efficient process also increases the likelihood of organizations adoption of strong data hygiene practices.

3. **Eliminates need to physically destroy drives**

   Constantly destroying storage media is costly now and will continue to drastically increase with supply shortages. VSDS provides an alternative to physical destruction allowing devices to be reused.

   Without the need for physical destruction, end of life devices can be recycled reclaiming valuable precious and rare earth metals.

4. **Compliance with NIST SP 800-88**

   The NIST SP 800-88 gives guidelines for data sanitization which PM 9-12 historically has not been able to fully implement. VSDS technology allows for PM 9-12 to match the guidelines referencing the purge of the device instead of using destruction techniques in every instance.

Recommendation & Conclusion

Cigent recommends updating PM 9-12 to include Verified Storage Device Sanitization (VSDS) as an approved method for sanitizing sensitive and classified data. Recent RDT&E efforts demonstrate VSDS method ensures absolute data elimination and verification of its removal. This update to PM 9-12, enabled by the new technology, will align with NIST SP 800-88 standards for the highest security classifications. Compared to the physical destruction currently utilized, this method provides substantial advantages. In summary these advantages are:

- Effective emergency data sanitization while minimizing personnel risk

- Increase data sanitization by providing simple process
  - Field deployments where physical destruction is difficult or impossible
  - Organizations more likely to adopt and follow process that is streamline

- Eliminates need to physically destroy drives
  - Saves precious earth metals

    - Reduces expense of replacing storage devices

- Complies with NIST SP 800-88

The dual capability of sanitation and verification allows organizations to have assurance that VSDS will prevent instances of data leakage. VSDS will significantly contribute to supporting deployed warfighters with comprehensive data retention, removal, and data forwarding capabilities required in even the most extreme security environments.