STORAGE DEVELOPER CONFERENCE

SDC 22 | Fremont, CA
September 12-15, 2022

BY Developers FOR Developers

A SNIA. Event

Storage Sanitization

The Right Way to Make Data Go Away

Eric Hibbard, Director, Samsung Semiconductor

John Geldman, Director, Kioxia

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion, please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

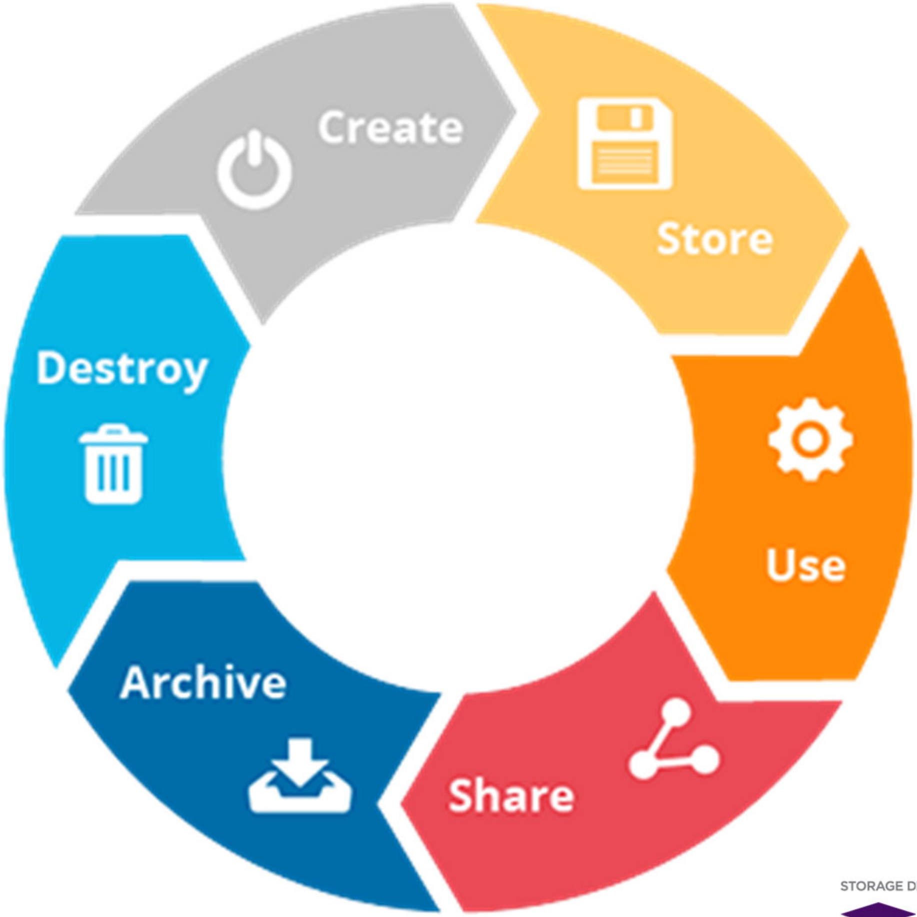
  NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Overview

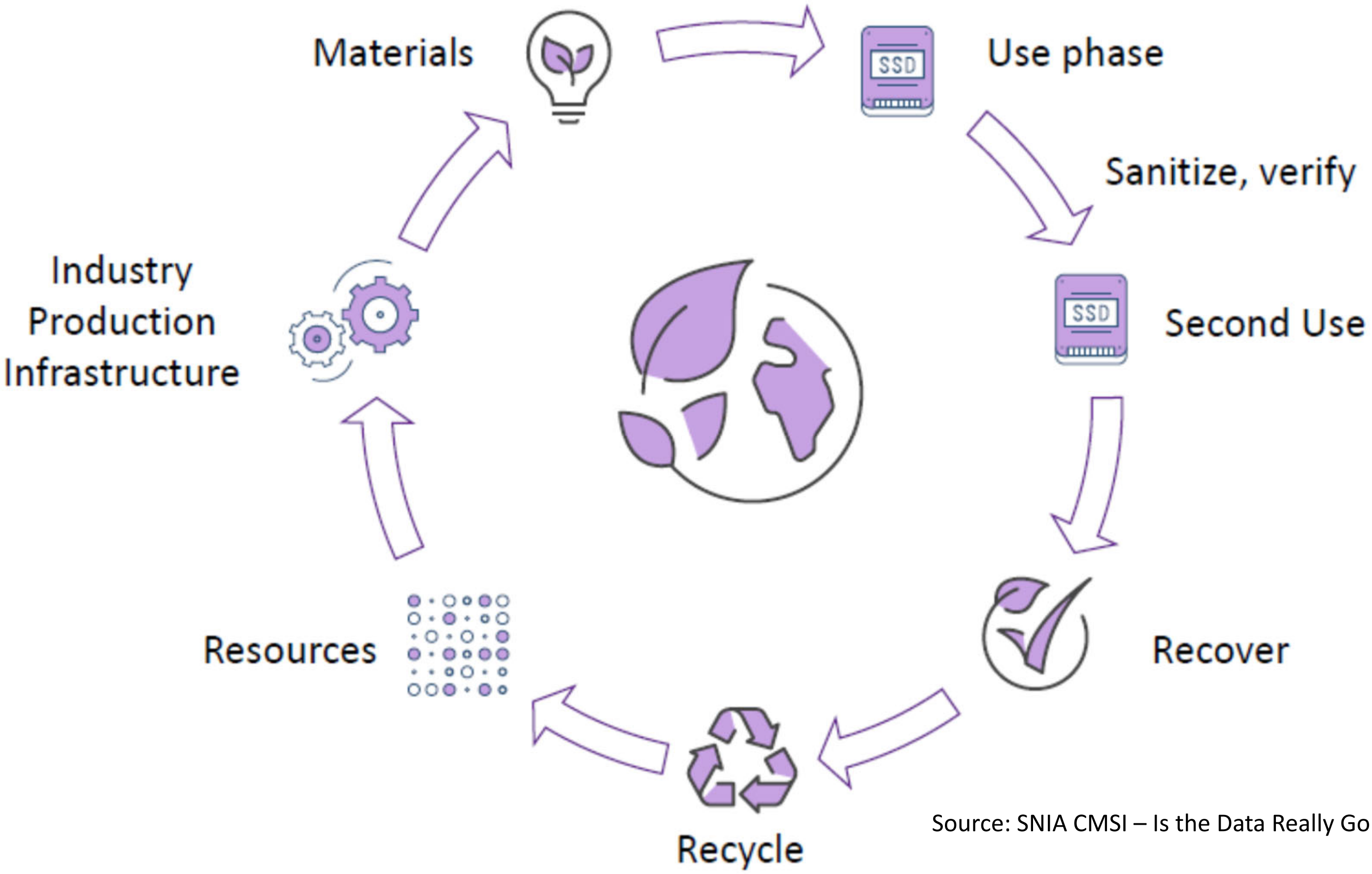
Data Lifecycle Management (DLM)

Data destruction/disposal is typically the last phase of DLM.

Necessary to avoid data breaches and to meet compliance obligations.



Circular Economy for Storage



Source: SNIA CMSI – Is the Data Really Gone?

Destroying/Eradicating Data

- Data eradication is non-trivial:
  - All copies must be located (e.g., backups, images of files, temp copies)
  - Data storage technologies are designed to guard against data loss
  - There may be specific compliance obligations (e.g., record keeping)
  - Advanced forensic tools exist to recover data

- The method of “eradicating” data is normally selected based on the:
  - underlying sensitivity of the data being eradicated, or
  - potential harm they could cause if they are recovered or inadvertently disclosed.

Confusing Language

- Data deletion
- Secure data deletion
- Data shredding
- Data wiping
- Data overwriting
- Data erasure
- Data clearing
- Data destruction
- Data sanitization

NOTE: Most of these are poorly and inconsistently defined and/or do not ensure the elimination of data.

Sanitization Defined

- Sanitization: process or method to render access to target data on storage infeasible for a given level of effort

- Wherefores and Provisos:
  - Access can mean the data no longer exists, the storage devices/media no longer exist, or there is something that permanently prevents access to the data
  - Target data refers to data stored and can also include metadata associated with the data
  - Infeasible for a given level of effort can mean computationally infeasible or the level of effort makes it near impossible or too complicated to be done; this language acknowledges that adjustments may be needed in the future

Forms of Sanitization

- ***Data sanitization:*** focused on all instances of stored data, wherever the data resides. Aligned with DLM Destroy.

- ***Storage sanitization:*** focused on data stored on ICT infrastructure that uses non-volatile storage
  - ***Logical sanitization:*** focused on data stored on logical/virtual storage
  - ***Media sanitization:*** focused on data stored on storage devices or storage media

Common Aspect of Storage Sanitization

- Identification of the form of storage involved: logical/virtual storage or media-aligned (media sanitization)
- Selecting the sanitization method that is appropriate for the type of storage and the data sensitivity
- Executing one or more of the selected storage sanitization techniques
- Verifying the results of the storage sanitization to determine the level of residual risk
- Producing evidence of the storage sanitization action that has been taken to meets compliance obligations (proof of sanitization)

Sanitization and Standards

Key Standards

- Current published standards:
  - ISO/IEC 27002:2022, *Information security, cybersecurity and privacy protection — Information security controls,* Soon to be Obsolete
  - ISO/IEC 27040:2015, *Information technology—Security techniques—Storage security*
  - IEEE 2883-2022, *IEEE Standard for Sanitizing Storage*
  - NIST SP 800-88 Revision 1, *Media Sanitization,* Obsolete

- Draft standards:
  - ISO/IEC DIS 27040 (2nd Ed.), *Information technology—Security techniques—Storage security,* ETA of Q1 2023

Revisiting Common Aspect of Storage Sanitization

- Identification of the form of storage involved: logical/virtual storage or media-aligned (media sanitization) ISO/IEC 27040
- Selecting the sanitization method that is appropriate for the type of storage and the data sensitivity ?? (risk based)
- Executing one or more of the selected storage sanitization techniques IEEE 2883
- Verifying the results of the storage sanitization to determine the level of residual risk ?? (ISO/IEC 27040 & IEEE 2883 make suggestions)
- Producing evidence of the storage sanitization action that has been taken to meets compliance obligations (proof of sanitization) ISO/IEC 27040

Storage Sanitization Methods

- **Clear**: sanitize using *logical techniques* on user data on all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same host interface available to the user
- **Purge**: sanitize using *physical or logical techniques* that make recovery of target data infeasible using state of the art laboratory techniques, but which preserves the storage media and the storage device in a potentially reusable state
- **Destruct**: sanitize using *physical techniques* that make recovery of target data infeasible using state of the art laboratory techniques and results in the subsequent inability to use the storage medium for storage

State of the art laboratory techniques

Technique examples:

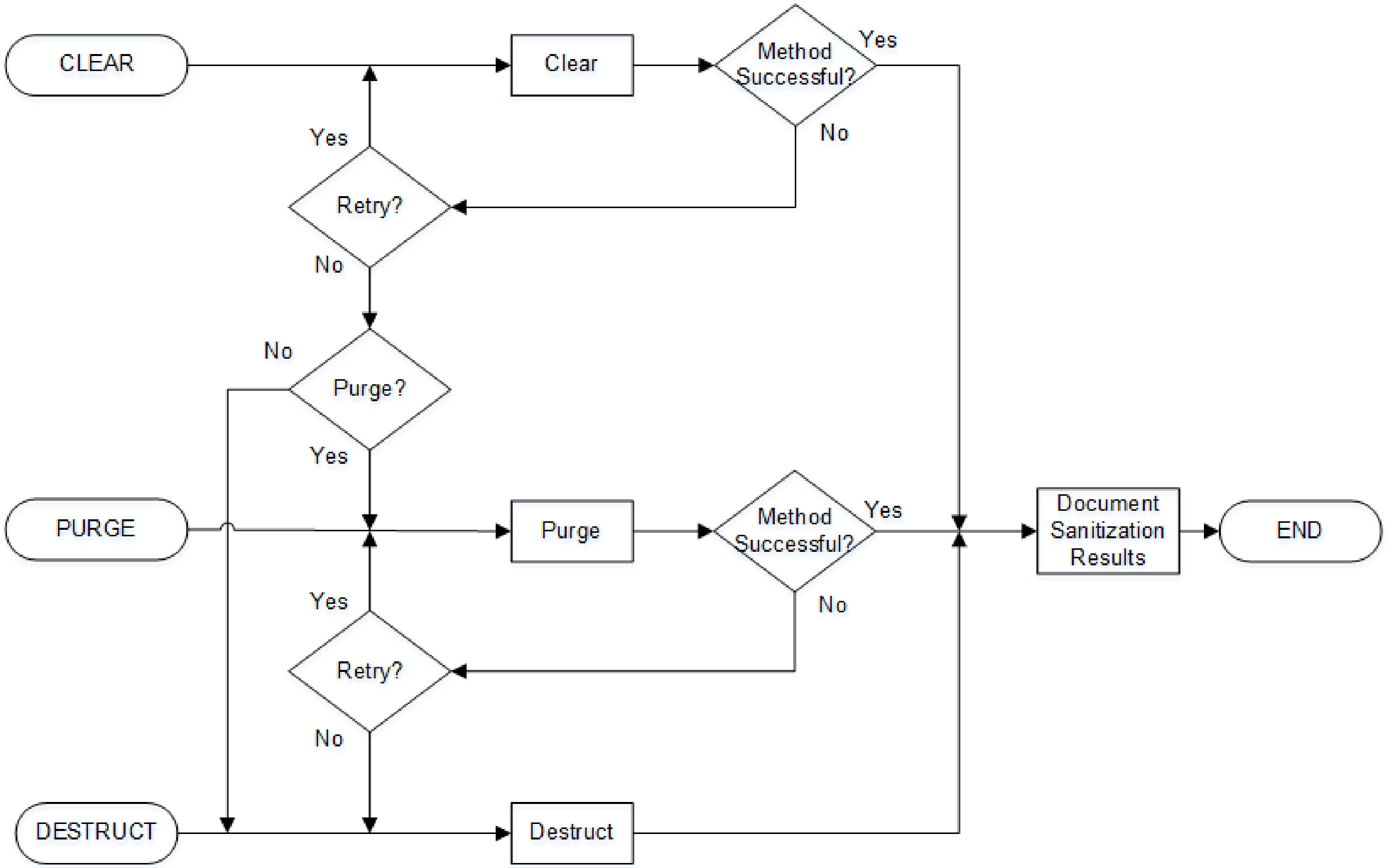
- Disassembly, and mounting a different circuit board to an HDD spindle
- Reading raw signal from an HDD platter on a spin stand
- Electron microscopy
- X-ray probing
- And many more things that a well funded adversary or a nation state has at its disposal

Selecting a Sanitization Method

- Considerations
  - Sensitivity of stored data
  - Organizational policies and risk appetite
  - Environmental impacts (reuse)
- Recommendations
  - Use sanitization to guard against data breaches due to media handling issues
  - Avoid Destruct if other methods are adequate
  - Seriously consider Purge, especially Cryptographic Erase

IEEE 2883-2022 Sanitization Process

The selected method may be different than the initial starting point.



Source: IEEE 2883-2022

Sanitization Techniques

Factors Affecting the Ability to Sanitize

- The storage media is not identifiable.
  - For example, tape cartridges are usually are labeled with the technology and generation, but some may not be labeled.
  - A storage device may be in an enclosure that is sealed (e.g., laptop, USB enclosure, mobile device)
  - A storage device may be embedded in a chip that is not accessible
- The organization lacks the expertise to sanitize the storage media (while leaving it usable) or to verify that sanitization was successful.
- The equipment is not working or is anticipated to not be working soon.
- The equipment or software needed to perform the operations is not available.
  - Examples include a storage device to access removable storage media, an interface for the storage device, a degausser with sufficient strength to erase newer magnetic storage media, etc.

Sanitization Techniques

Sanitation TECHNIQUES are media-specific and interface-specific techniques used to implement the Sanitization METHODS (Clear, Purge, Destruct)

Not all sanitization techniques are appropriate in all situations. Here are some examples.

Clear	Purge	Destruct
Simple overwrite	Sanitize overwrite Block erase Cryptographic erase Degauss (with special precautions)	Melt Incinerate Degauss (with special precautions) *Pulverize *Shred * These are obsolete techniques

Sanitization Techniques - Overwrite

- The term ‘overwrite’ has multiple meanings. A distinction has been made between
  - Simple overwrite: writing a pattern or deallocating only logical locations
    - Write commands
    - SECURITY ERASE UNIT (ATA), FORMAT UNIT (SCSI), Format NVM (NVMe)
    - UNMAP (SCSI), DATASET MANAGEMENT (ATA), Dataset Management (NVMe)
    - Note: there could be physical copies of data that are not erased
  - Sanitize overwrite: writing a pattern to all logical and physical locations within the scope of sanitize
    - Note: SCSI, ATA, and NVMe all have a special ‘Sanitize’ command that accomplishes this
- Overwrite is not appropriate for
  - Non-magnetic media (paper, optical media, etc.)

Overwrite For Flash: Write Amplification Myth

- NAND Flash has characteristics of interest for Sanitize Overwrite:
  - After a sanitize overwrite, before deallocation, 100% of the addressable media is available for verification
  - After sanitize verification, the device should be entirely deallocated to avoid useless write amplification related the obsolete FTL tables
  - Before a NAND erase block can be reused, it will need to be erased
- This adds up to an erase cycle across the device’s NAND erase blocks before the write operations and the typically necessary erase cycle before any NAND bock can be reused
- For some data sets, the value of the verification outweighs the value of the one additional device wide erase cycle
  - There is no write amplification penalty (unless deallocation is not performed).

Sanitization Techniques – Block Erase

- Block Erase
  - Allows a relatively large region of storage (e.g., an erase block) to be erased in a single operation
  - Doesn’t apply to magnetic media today
    - No mechanism currently exists to block erase magnetic media
  - Is useful for types of memory devices (e.g., NAND) that support it
  - The media may or may not be readable without errors after block erasure
    - Integrity structures (e.g., CRCs) are also erased
    - Integrity structures are created as part of subsequent write operations
  - The media may be all binary 0’s or all binary 1’s after block erasure (depending on the media vendor)
  - Reduces the negative impact on erase cycle use from the Overwrite technique
  - Myth: Some erased NAND media degrades if not written quickly
    - True but not applicable as such there are implementation specific mechanisms to stabilize the media that do not require additional erase cycles

Sanitization Techniques – Cryptographic Erase

- Cryptographic Erase
  - “Method of sanitization in which the encryption key for the encrypted target data is sanitized, making recovery of the decrypted target data infeasible using state of the art laboratory techniques”
  - media based cryptographic erase: Method of cryptographic erase in which the encryption key is only resident on the storage device.
  - Without the encryption key used to encrypt the target data, the data are unrecoverable
  - ISO/IEC 27040 pre-conditions for cryptographic erase:
    - encryption of all data intended for cryptographic erase prior to recording on the storage;
    - the strength of the cryptographic algorithm (including mode of operation) used to encrypt the target data is at least 128 bits;
    - the level of entropy of the encryption key used to encrypt the target data is at least 128 bits; and
    - all copies of the encryption keys used to encrypt the target data are sanitized; if the target data's encryption keys are, themselves, encrypted with one or more wrapping keys, it is acceptable to perform cryptographic erase by sanitizing a corresponding wrapping key.
  - Only <u>media-based </u>storage sanitization is defined in IEEE 2883-2022

Sanitization Techniques – Cryptographic Erase

- The level of effort needed to decrypt this data without the encryption key is the lesser of:
  - the strength of the cryptographic algorithm used to encrypt the data (including mode of operation);
  - the level of entropy of the target data's encryption.
- Sanitization may be performed with high assurance much faster than with other sanitization techniques. Cryptographic erase can be executed in seconds.
- Cryptographic erase can also be used as a supplement or in addition to other sanitization approaches.
- Some organizations perform an additional, but unneeded, sanitization using a clear method to reduce the attack surface by preventing access to the ciphertext.

Sanitization Techniques - Destruct

- Melting
  - “Destruct by changing storage media from a solid to a liquid state, generally by the application of heat”
- Incineration
  - “Destruct by burning a storage device completely”
- Both of these techniques are not ‘green’
  - environmental risks associated with disposing of potentially hazardous materials (e.g., plastics, lead, heavy metals)
  - no possibility of recovering valuable materials (e.g., gold, rare earth elements)
  - require large amounts of energy to perform

Sanitization Techniques - Destruct

- Shred
  - “An obsolete form of Destruct that cuts or tears a storage device or storage media into small particles”

- Pulverize
  - “An obsolete form of Destruct that grinds a storage device to a powder or appropriately small particles”

With the increased density of data in all types of media, shredding and pulverizing can leave significant amounts of information on the remaining particles.

Verification and Documentation

Verification of Sanitization

Just because the device SAID it sanitized the data doesn't mean it really DID !

- Verification of the sanitization outcomes can be an important element of a data sanitization program when a determination as to the adequacy or effectiveness of the storage sanitization is required.
- Verification differs depending on the sanitization method

- For clear or purge:
  - Verification that a command was performed
  - Full verification of addressable media is typically recommended for clear or purge, but representative sampling may be adequate
- For destruct:
  - Physical inspection is used to check the sanitization outcomes

Documentation Sanitization Results

Failure to properly record the sanitization could result in data breach protocols

- ISO/IEC 27040 (not IEEE 2883) identifies specific information that should be recorded
  - When did this happen
  - Who performed it
  - Where was it performed
  - What equipment performed the sanitization
  - Which sanitization method was used: clear, purge, or destruct
  - Which sanitization technique was used, and the result
  - What verification method was used, and the result
  - The final disposition of the storage media
- Proof of sanitization takes on at least two forms:
  - an audit log trail
  - a certificate of sanitization

Summary

Conclusions

- Storage sanitization is an important security control to avoid data breaches
- Adequate documentation is a critical element
- IEEE 2883 is the go-to document on how to sanitize specific storage media
- Increased use of Purge as opposed to Destruct can be good for the environment

More Storage Sanitization Issues to be Addressed

- Persistent memory (NVDIMM-N)
- Energy assisted magnetic recording (HAMR, MAMR)
- DNA storage
- Logical storage (cloud storage)
- Holographic storage
- Storage attached to a fabric (SAN)
- Object storage (key/ value)
- Encrypted storage with keys managed outside the storage device
- Post-quantum cryptography
- Medical equipment
- Automotive equipment and self-driving vehicles
- … and others that cannot be discussed at this time…

How to participate further

- SNIA Security TWG
  - https://www.snia.org/securitytwg
- IEEE Cybersecurity & Privacy Standards Committee (CPSC)
  - IEEE Security In Storage WG (C/CPSC/SIS-WG)
    - https://development.standards.ieee.org/myproject-web/app#interests
- ISO/IEC JTC 1/SC 27 (Information security, cybersecurity, privacy protections) ISO/IEC 27000-series security standards
  - INCITS Cybersecurity and Privacy Technical Committee (formerly CS1)
    - https://www.incits.org/committees/cs1

Additional Resources

- SNIA standards
  - https://www.snia.org/tech_activities/standards/curr_standards
- ISO/IEC standards
  - https://www.iso.org/standards.html
- IEEE standards
  - https://standards.ieee.org/
- ETSI
  - https://www.etsi.org/standards
- CEN-CENELEC
  - https://www.cencenelec.eu/
- NIST
  - https://www.nist.gov/publications

Thank You!

Please take a moment to rate this session.

Your feedback is important to us.