



SNIA<sup>®</sup> STORAGE  
SECURITY SUMMIT  
Wednesday, May 11, 2022 • Virtual

# IEEE Std 2883

Standard for Sanitizing Storage

Presented by Jim Hatfield, Seagate Technology



A SNIA<sup>®</sup> Event

# About the Speaker



**Jim Hatfield**

Firmware Engineer  
Standards Engineer

**james.c.hatfield@Seagate.com**

IEEE Security In Storage WG (SISWG)

- chair, editor of IEEE 2883

Trusted Computing Group

- co-chair of Storage WG

SATA-IO

- president, chair of Digital WG

Active participant of:

- SNIA Security TWG
- NVM Express
- INCITS T13 (SATA)
- INCITS T10 (SCSI)
- Open Compute Project (OCP)

# Abstract

This session gives an overview of a new security standard: IEEE Std 2883 – Standard for Sanitizing Storage

- What is Sanitization? and what is it not ?
- What is IEEE 2883 ?
- Why is IEEE 2883 needed ?
- Sanitization methods
- What can be sanitized
- Verification and documentation
- How to participate further ?

# 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 containin 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.

# Attributions

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

NVM Express and NVMe are registered trademarks in the U.S. Patent & Trademark Office, owned by NVM Express, Inc.

TCG and Trusted Computing Group are registered trademarks in the U.S. Patent & Trademark Office, owned by Trusted Computing Group.



# What is Sanitization?

## And what is it NOT ?

# What is Sanitization? And what is it not?

- Sanitization is
  - A process or method to render access to target data on storage media infeasible for a given level of effort.
- Sanitization Methods (each with a different 'level of effort')
  - Clear
  - Purge
  - Destruct

# What is Sanitization? And what is it not?

- Sanitization is NOT:
  - Related to FIPS or Common Criteria compliance
  - Simply deleting files
  - Trim/Unmap/Deallocation of storage
  - Fuzzy industry terms without a clear definition, and do not ensure the elimination of data
    - Secure data deletion, data clearing, data erasure, data destruction, data wiping, data overwriting, Data shredding
  - Blindly degaussing, shredding, pulverizing, disassembling a storage device
  - Scratching the media with a screwdriver (or) shooting it with a shotgun (these really do happen!)
  - Cutting a floppy disk with scissors (but it can be recovered by taping the pieces together)
  - Powering off a device
  - Exposure to radiation
  - And many more things....

# Scope of Sanitization

All physical and logical locations that:

- currently contain user data
- used to contain user data (e.g., deallocated data, data reallocated because of media errors)
- could contain user data (e.g., overprovisioning, unused capacity, spare pools)
- are able to contain data that discloses information about user data (e.g., data that is useable to direct forensic analysis)

# Barriers to Reuse and Recycling



SUSTAINABILITY

- Perceived data security risks
- Government regulations around proof of data destruction
- Technological challenges in HDD separation
- Lack of supply chain coordination
- Users demand physical destruction even when complete, verifiable data wiping is possible

*This leads to widespread HDD shredding, which precludes reuse, harvesting of components for, and recovery of critical and strategic materials including rare earth magnets*



***Creating a sustainable Datasphere requires effort and a new mindset***

***10's of millions of drives are destroyed each year.***

The paranoid choose degaussing, followed by shredding, followed by disintegration.















# What is IEEE 2883 ?

# What is IEEE 2883 ?

- IEEE Std 2883 Standard for Sanitizing Storage

- A new international security standard
- Is a standalone standard
- Describes what sanitization is and is not
- Defines the elements of sanitization in general terms
- Contains conformance requirements
- Describes the sanitization methods: Clear, Purge, and Destruct
- Specifies media-specific and interface-specific techniques to implement Clear, Purge, and Destruct
- Contains guidance for composite devices (printers, fax, scan, copiers, mobile devices, gaming consoles, etc.)
- Describes how to properly use cryptographic erase
- Lists some evolving storage technologies that you should be aware of, and that could be in a future revision

> 	1. Overview
	2. Normative references
> 	3. Definitions, acronyms, and abbreviations
> 	4. Conventions
> 	5. Storage sanitization
> 	6. Sanitization methods and techniques
> 	7. Verification of sanitization outcomes
> 	8. Media type-specific sanitization
> 	Annex A (normative) Storage devices with embedded storage
	Annex B (informative) Cryptographic erase
	Annex C (informative) Developing storage technologies
	Annex D (informative) Bibliography

# 1 **P2883™/D18**

## 2 **Draft Standard for Sanitizing Storage**

3 Developed by the  
4  
5 **Cybersecurity and Privacy Standards Committee**  
6 of the  
7 **IEEE Computer Society**

8  
9  
10 Approved <Date Approved>

11  
12 **IEEE SA Standards Board**

13  
14 Copyright © 2022 by The Institute of Electrical and Electronics Engineers, Inc.  
15 Three Park Avenue  
16 New York, New York 10016-5997, USA

17 All rights reserved.

# Relationship to other data removal specifications

- ISO/IEC 27040
  - Information technology – Security techniques – Storage security
  - ISO/IEC 27040-2015
    - General guidance for storage security
    - There are no requirements, only recommendations
    - Contains media-specific and interface-specific guidance for sanitization techniques
    - Contains much common text with NIST SP800-88r1
      - they were written at the same time, and by many of the same authors
  - ISO/IEC 27040-202x
    - General guidance and requirements for storage security
    - Refers to IEEE 2883 for media-specific and interface-specific sanitization techniques

# Relationship to other data removal specifications

- NIST SP800-88r1
  - Guidelines for Media Sanitization
  - Contains guidance (no requirements) for storage security
  - Is a product of the US government. Many countries will not refer to US security standards
  - Contains much common text with ISO/IEC 27040-2015
    - they were written at the same time, and by many of the same authors
- ETSI Lot 9
  - Environmental Engineering (EE) Energy Efficiency measurement methodology and metrics for servers
  - Eco-design Technical Assistance Study on Standards for ErP **Lot 9** Enterprise Servers and Enterprise Data. Storage
  - ETSI EN 303 470 V1.1.0 (2019-01)
- CEN-CENELEC
  - Decides which standards become EU standards (not all are accepted)



# Why is IEEE 2883 needed ?

# Why is IEEE 2883 needed ?

- Since 2015, when ISO/IEC 27040 and NIST SP800-88R1 were published:
  - NVM Express (NVMe) defined a Sanitize command (modeled after the command in SAS and SATA)
  - NVMe defined several architectural elements within an NVM subsystem: CMB, HMB, PMR, Domains, Zoned namespaces, Key-Value namespaces
  - SAS and SATA defined/extended several new features: Zoned commands, Zone Domains and Realms, Mutate command
  - HDD recording techniques and densities came to market, or penetrated the market more:
    - Shingled Magnetic Recording (SMR)
    - Energy Assisted Magnetic Recording (HAMR and MAMR)
    - Mixed Conventional Magnetic Recording (CMR) and SMR on the same device
  - Recording densities increased for NAND, hard drives, and tapes
  - NVMe established a strong foothold in the global storage market
  - Many devices have been created that contain embedded storage: mobile devices, printer/fax/copy/scan, gaming devices, IoT, etc.

# Why is IEEE 2883 needed ?

- The demand for 'green technology' has grown greatly (e.g., discarding/destroying drives is highly discouraged by some)
  - Circularity
  - Disposal must be an informed risk-based decision
  - Reusing rare elements
  - Reducing landfill and contamination issues

# Why is IEEE 2883 needed ?

Data destruction/disposal is typically the last phase of Data Lifecycle Management (DLM).

Necessary to avoid data breaches and to meet compliance obligations.



# Why is IEEE 2883 needed ?

- ISO/IEC 27040:2015 is a guidance document
  - There are no requirements in it. The storage and security industries now demand requirements.
- Other changes have been made to other ISO/IEC standards that 27040 depends upon
  - ISO/IEC 27001 Information technology – Security techniques – Information security management systems — Requirements
  - ISO/IEC 27002 Information technology – Security techniques – Code of practice for information security controls
- Other data removal standards and specifications are being developed in the European Union and elsewhere
  - It is desirable to have a single international standard that those documents could refer to

# Why is IEEE 2883 needed ?

- Standards need to keep pace with the industry
  - The storage industry evolves at a rapid pace, but standards do not.
  - Because of the new developments in storage technologies, the standards need to be updated.
  - ISO/IEC documents generally have a 10 year lifecycle, and take 2-3 years to publish
  - IEEE standards can be revised and published in 1 year, if needed.
- Users have requirements and need verification
  - The industry demands more than just guidance

# Why is IEEE 2883 needed ?

To identify 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.
- 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.

# Why is IEEE 2883 needed ?

- So, participants from the SNIA Security TWG and the IEEE Security In Storage WG (SISWG) decided to
  - Move the media-specific and interface specific material from ISO/IEC 27040 to a new IEEE standard
- In the revised ISO/IEC 27040:
  - Create a framework of requirements
  - Define high-level sanitize methods: Clear, Purge, and Destruct
  - Refer to IEEE 2883 for media-specific and interface-specific instructions to implement Clear, Purge, and Destruct
  - Make changes to intersect with the new ISO/IEC 27001 and ISO/IEC 27002 standards in development
  - Update guidance and requirements to better reflect the current state of technology

# Why is IEEE 2883 needed ?

- In the new IEEE 2883:
  - Add support for many technologies that were not in ISO/IEC 27040
    - TCG Opal family SSC (Opal, Opalite, Ruby, Pyrite) and Enterprise SSC
    - NVMe CMB, HMB, PMR, Sanitize command
    - Better requirements for sanitizing magnetic tapes
    - Composite devices
    - Devices with embedded media (mobile, game consoles, IoT, MP3 players, satellite/cable boxes, etc)
    - Additional hardcopy media
  - Update Destruct methods
    - Obsolete the Shred and Pulverize techniques of the Destruct sanitization method
    - Indicate the limitations of degaussing and give guidance on its proper use
  - Encourage the use of Purge to support environmental health/circularity through reuse vs. discarding
  - Consolidate HDD and SSD sanitization techniques to take advantage of commonality
  - List some evolving technologies that a security practitioner should be aware of, that are not covered yet



# Sanitization Methods

Section Subtitle

# Sanitization Methods

- Clear
  - Sanitize using logical techniques on user data on all addressable storage locations for protection against simple non-invasive data recovery techniques using the same host interface available to the user.
- Purge
  - Sanitize 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 (not 'Destroy')
  - 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 media for storage.
  - Use Melt or Incinerate
  - Use Degauss with the guidance provided
  - Shred and Pulverize techniques are now obsolete

# State of the art laboratory techniques

This includes such things as

- 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

# How to choose a sanitization method ?

1. Use ISO/IEC 27040
2. Use policies for your organization
3. Answer these questions
  1. Do you want the storage device to reusable after sanitization ? (choose Clear or Purge)
  2. Do you want to avoid discarding the device (environmental impacts) ? (choose Clear or Purge)
  3. If reuse is desired: Who will use it after sanitization? Another group in the same org ? Someone outside the org ? A stranger ?
  4. What is the risk if the information on the device were disclosed to an unauthorized party ?
    1. Low (e.g., Clear): mild impacts to the organization
    2. Medium (e.g., Purge): moderate impacts to the organization; and
    3. High (e.g., Destruct): severe impacts to the organization.
  5. Do you have the tools (hardware/software) to perform the chosen sanitization method ? and the verification ?

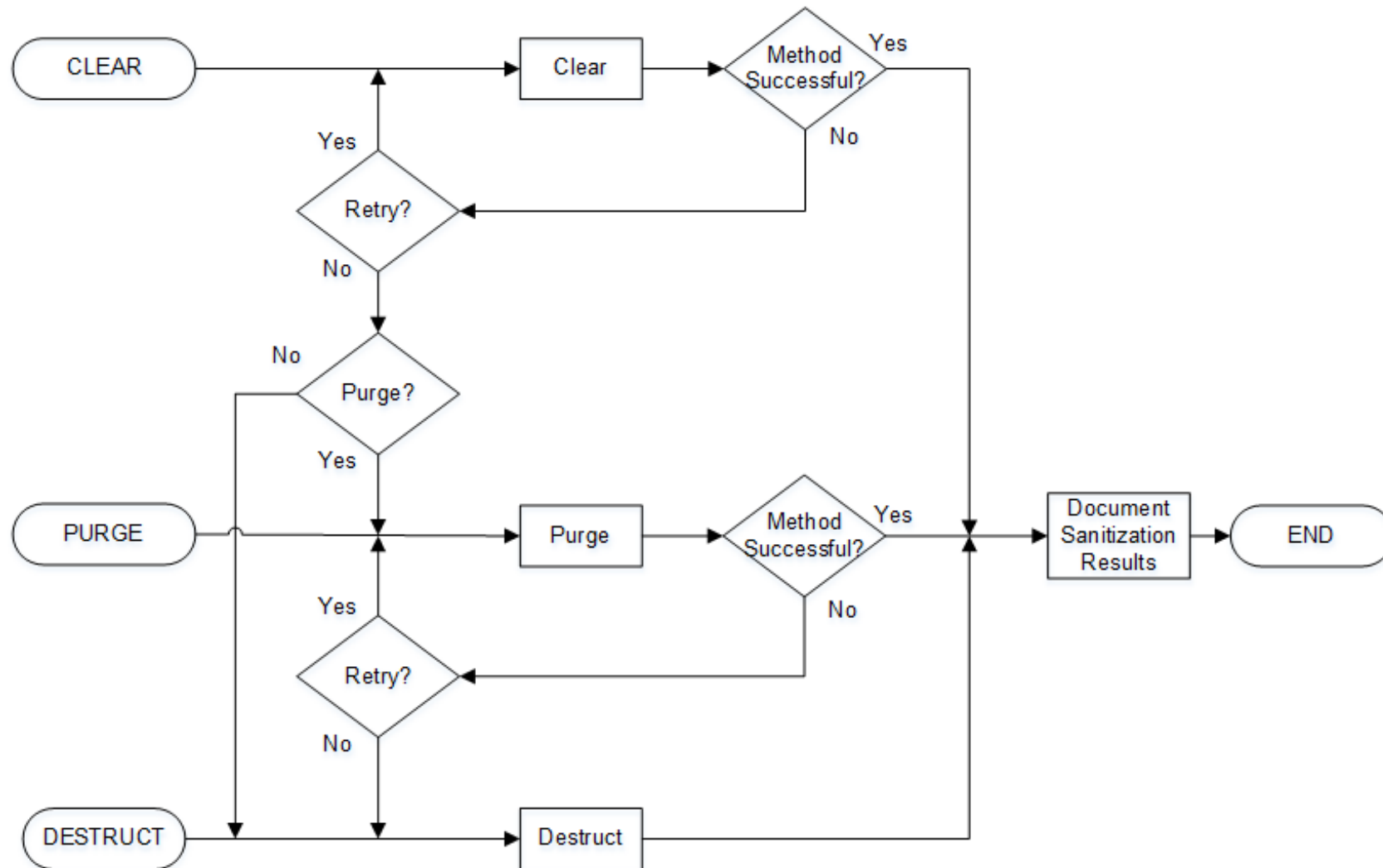
When you have chosen a method, use the process chart on the next slide

Regardless of the sanitization method that was first chosen, the media-specific and interface-specific sanitization techniques in IEEE 2883 may redirect you to use a different method that is more appropriate.

# Destroying Data

- Data destruction 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 “destroying” data is normally selected based on the:
  - underlying sensitivity of the data being destroyed, or
  - potential harm they could cause if they are recovered or inadvertently disclosed.

# The sanitization process





# Sanitization Techniques

Section Subtitle

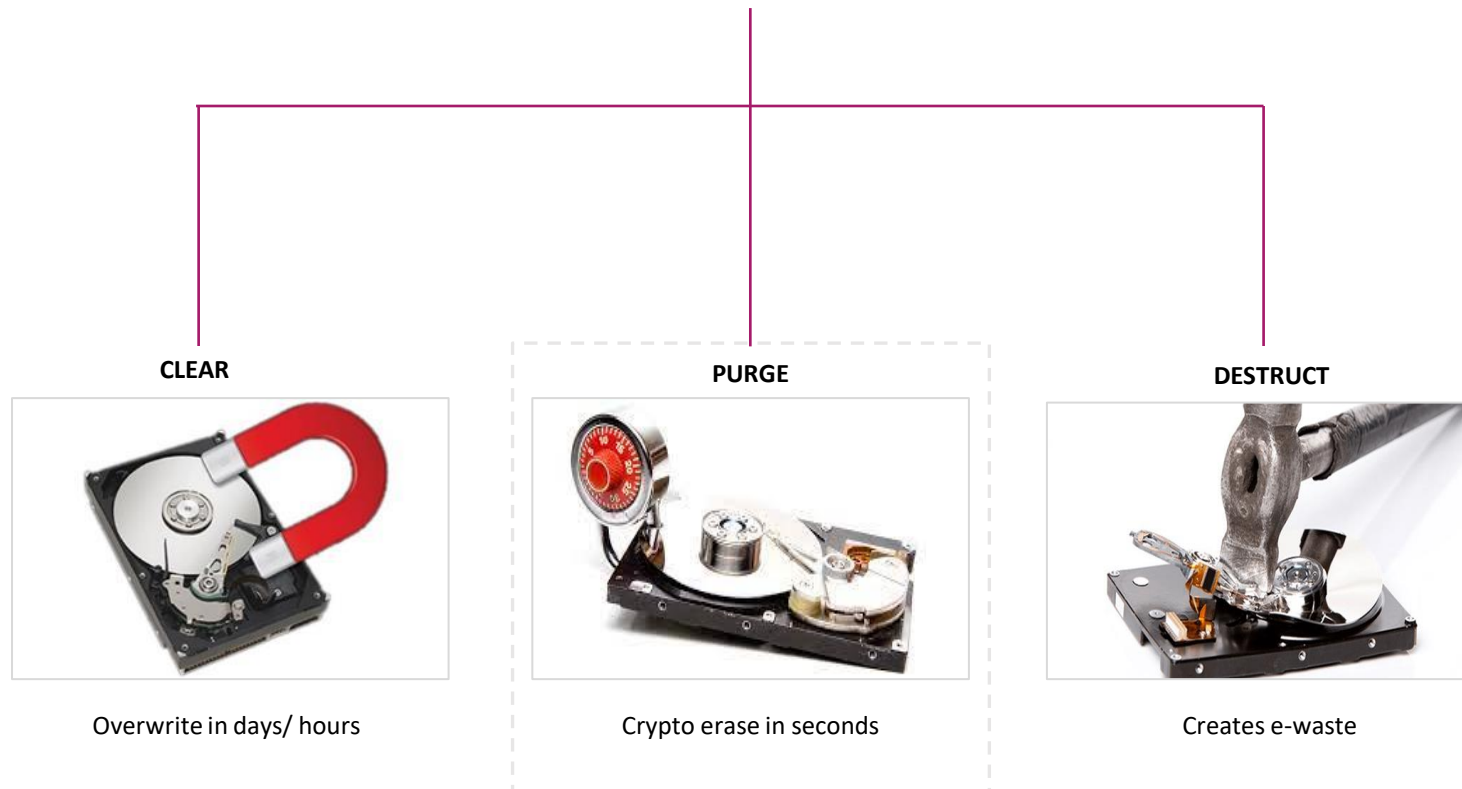
# Sanitization Techniques

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

## Methods of Sanitization



# 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 - 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.)
  - NAND flash: overwriting negatively affects write amplification and the endurance of the device

# 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
- Is not appropriate for 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 (because CRCs also be erased and may not recomputed)
- 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 write amplification that the Overwrite technique has

# 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 media-based storage sanitization is supported in IEEE 2883

# 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.

# Shred and Pulverize are insufficient with high data density



## Shred Risk

1 in<sup>2</sup> of hard drive = 1.3 Tb  
2,000 bytes per page = Paper Sheet Equivalent (PSE)  
1.3 Tb = 8,125,000 PSE  
1 mm<sup>2</sup> = 125,969 PSE

**NSA Shred Requirement is 2 mm<sup>2</sup>**

**2 mm<sup>2</sup> = 503,876 PSE**

2.52 Pallets of Paper or 15 Sets Encyclopedia Britannica



# Sanitization Techniques - Destruct

- Degauss

- “Render magnetically stored data unreadable by applying a strong magnetic field to storage media with an organizationally approved field strength”
- Degaussing generally results in rendering the storage device/media permanently inoperable (e.g., not Purge)
  - Degaussing IS an acceptable Purge technique for some media types
- Degaussing is only appropriate for magnetic media (no paper, NAND, memory, non-magnetic parts of SSHD, etc.)
- Device data densities vary widely
  - Newer HDD and tape densities are much greater than 10 years ago
    - HDD: 12 Gb/in<sup>2</sup> in 1998 compared to 2 TB/in<sup>2</sup> in 2020 .... and still growing
- Not all degaussing equipment will work for all densities
  - Higher density storage requires higher coercivity to fully degauss
- Degaussing may make the storage device or the media unusable
  - LTO tape may have servo tracks – degauss them and the tape is unusable
  - HDD has magnetic media, heads, and magnets (motors, head mechanism)
    - It is possible to damage the mechanism without degaussing the data

- IEEE 2883 has special guidance for degaussing



# What can be sanitized ?

# Media Types Covered (items in red are new)

## SSD/HDD/SSHD:

- HDD: CMR, **SMR, HSMR**
- SSD: NAND memory (**all types**)
- SSHD (**HDD and SSD in one unit**)

## ■ Hard Copy:

- Paper, microforms, microfilm, microfiche, photo negatives, **printer/fax ribbons, drums, platens**

## ■ Optical Media:

- CD, DVD, Blu-ray, etc.

## Other Magnetic

- Floppy disk, removeable flexible or rigid magnetic disc
- Tape: cassette, **video**, 8mm, **LTO**, DDS, DAT, DLT, QIC

# Media Types Covered

## Memory Cards

- SD, SDHC, MMC, CompactFlash, Microdrive, MemoryStick, e•MMC

## Embedded Flash:

- Motherboards, peripheral cards, network adapters, etc.

## Memory Chips

- RAM/ROM
- DRAM
- EAPROM
- EEPROM
- NAND flash

# Media Types Covered

## Devices with Embedded Storage

- Mobile device sanitization has been generalized (instead of instructions per manufacturer)
- Mobile phone, tablet, game console, digital TV, satellite/cable box, iPod, MP3 player, etc.
- Internet of Things (IoT)
- Commercial printer or copy machine
- Multi-function print/ copy/scan/fax

## Office Equipment:

- copier, printer, scanner, fax
- Network hub, router, switch

# Host interfaces and Transports covered

- SCSI
  - SAS, USB, UAS, IEEE 1394 (FireWire), ATAPI, Fibre Channel, iSCSI, UFS, Parallel SCSI
- ATA
  - PATA, SATA, eSATA, CompactFlash, CFast
- NVM™ Express
  - PCIe, RDMA, TCP, Fibre Channel
- SD Card
- e•MMC
- Floppy disk
- Memory access from the host



# 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 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

After your storage has been sanitized, a record of the sanitization should be made.

- 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



# Sanitization standards are never done !

# Emerging technologies that IEEE 2883 does not cover

- 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 Security In Storage WG (C/CPSC/SIS-WG)
  - <https://development.standards.ieee.org/myproject-web/app#interests>
- 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](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>

# Additional Resources

- ANSI has MANY standards in many categories (e.g., published ATA and SCSI standards)
  - <https://webstore.ansi.org/>
- NVMe specifications
  - <https://nvmexpress.org/>
- SCSI (draft) specifications
  - <https://www.t10.org/>
- ATA (draft) specifications
  - <https://t13.org/>
- TCG specifications
  - <https://trustedcomputinggroup.org/>



# Thank you !

Section Subtitle



# Please take a moment to rate this session.

Your feedback is important to us.