Complying with Evolving Modern-Day Data Sanitization and Verification Standards

Presenter: David Logue

Operations Manager/Lead Data Recovery Engineer

Why Choose ‘Reuse’?

- Cheaper
  - Cost of Data Storage
  - Cost of New Hardware
- Faster
  - Supply Chain Issues
- Greener
  - Lower Environmental Footprint
  - Preserves Resources
  - Reduces Emissions

What's at Risk?

- What do we protect?
  - Client Data
  - Intellectual Property/Trade Secrets
  - Financial Data
  - Protected Data - PII, PHI, PCI, HIPAA, etc
  - Protected Data - GDPR, CDPA, etc
- Why do we protect?
  - Reputation
  - Cyber Crime
  - Corporate Espionage
  - Federal, State, Local Regulations
  - Legal Liability

What are Penalties?

- Civil Penalties

  HHS - USD 100 to USD 50,000 per violation, with a total of USD 25,000 to USD 1.5 million for all violations

  CCPA provides for fines of up to USD 2,500 per violation or USD 7,500 per intentional violation, but notably does not place a cap on the total amount of fines.

  Example: Morgan Stanley $60 million in fines + legal settlements (i.e. $6.5 mil to NY)

- Administrative Remedies

  Including rescission or reformation of contracts; monetary refunds or return of real property; restitution; disgorgement or compensation for unjust enrichment; monetary penalties; public notification of the violation; and limits on the violator's functions

- Criminal Liability

  Violations of HIPAA can include criminal penalties, including up to ten years imprisonment in certain cases

What are the Challenges?

- Data
  - Must ensure no previous user data exists across multiple locations/types
- Stakeholder Support
  - Senior Management, InfoSec, Legal, Users, etc
- Time
  - Do more with less
- Standards
  - DoD, NIST, IEEE, ISO, etc
- Software/Hardware
  - Unknown implementation of Sanitization commands in Software
  - Unknown implementation of Sanitization commands in Hardware
    - Implementation up to manufacturer

How to Protect?

- Develop a Written Plan
- Choose a Standard
  - NIST, IEEE, ISO, other
- Choose Level of Media Sanitization
  - Clear
  - Purge
  - Destroy/Destruct
- Choose Method of Verification
  - Software
  - Hardware
- Engage 3rd Party Verification

What are the Sanitization Standards?

Standard	DoD 5220.22-M	NIST SP 800-88 Rev1	IEEE 2883 - 2022
Name	U.S. Dept. of Defense	National Institute of Standards and Technology (U.S. Dept. of Commerce)	Institute of Electrical and Electronic Engineers
Established	1995	2006 (rev 1 = 2014)	2022
Organization	U.S. Government	U.S. Government	Private Professional Org.
Highlights	3-pass, 7-pass	Clear, Purge	Clear, Purge
Limitations	Not suited for Flash	No NVMe	
	Overwrite only		
	Time consuming		
Status	Old and Outdated	Current but Limited	Modern

Additional Standards?

Standard	ISO 27040:2024 (Storage Security)
Name	International Org. for Standardization
Established	2015
Organization	Private Professional Org.
Highlights	Clear, Purge, Destroy
Limitations	High level policies, not sanitization specific standards
	Includes routers, microfilm, CD/DVD, etc.
Status	Published 2024

Additional Standards?

- Common Criteria (ISO 15408)
- HIPAA
- R2
- ANSSI (France)
- STQC (India)
- TTA (Korea)
- NYCE (Mexico)

Sanitization Method

- Once you have a standard selected, choose a sanitization method

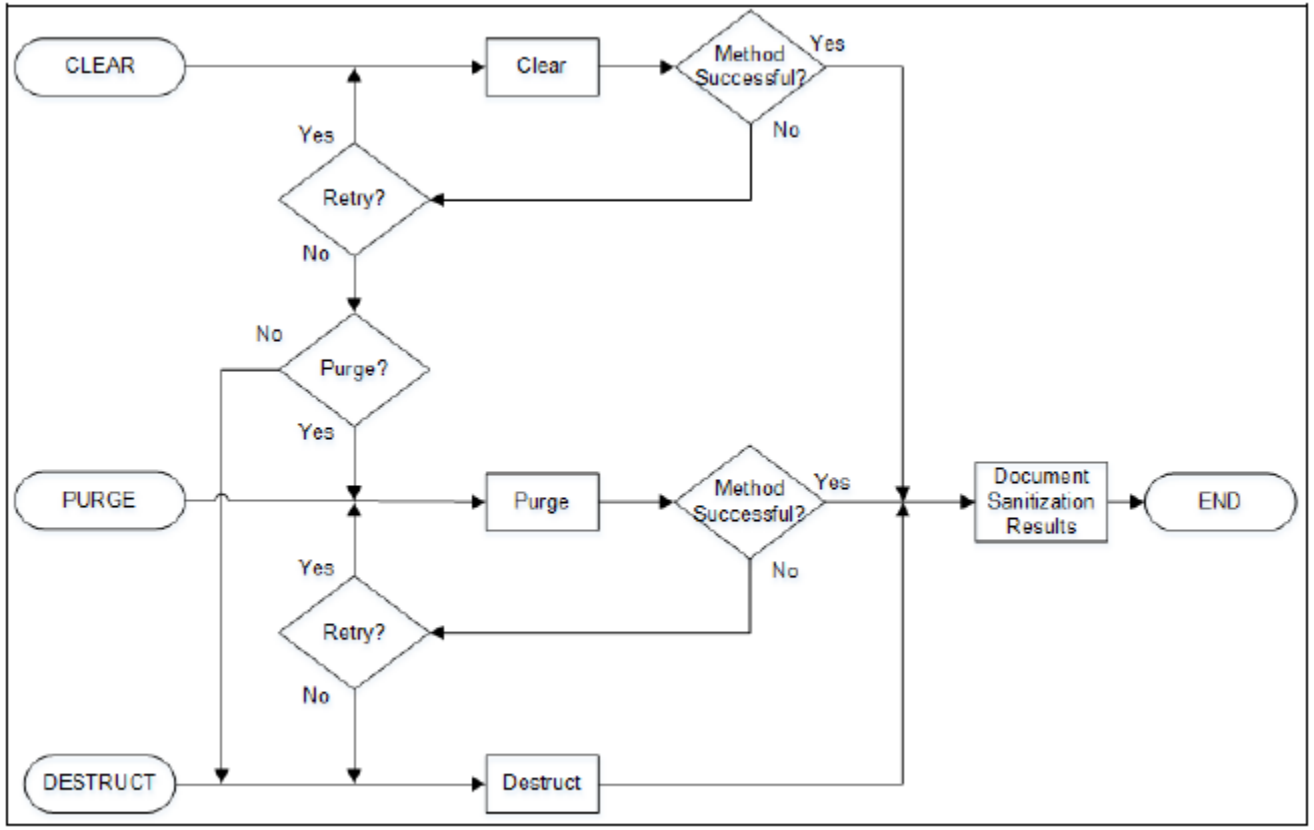

Figure 1—Sanitization process

Clear vs. Purge

- Clear

  In general, Clear is simpler standard, easier to comply, offers basic protection (against commercially available recovery software)

  NIST: 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

  In general, Purge more complex, harder to comply, offers more protection (against state-of-the-art laboratory recovery techniques)

  NIST: Purge applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.

How to ensure compliance?

3rd Party Verification

- Verification of the software/firmware via a code review
  - Drive Identification
  - Erasure Commands
  - Error Handling
  - Logging
  - Verification
  - Hidden Areas/NVMe Namespaces
- Forensic verification that the media is sanitized
  - Logically via the standard user interface
  - Physically directly from the NAND
  - Hidden area/NVMe Namespace examination

Verification Case Studies

- Drive Manufacturer
  - -New sanitization product (hardware and software)
  - -Looking to ensure IEEE 2883-2022 Purge compliance
  - -Code review was performed
  - -Numerous non-compliant sections discovered
  - -Manufacturer was able to remedy all of the open issues
  - -Verified IEEE Purge compliant
- Storage Manufacturer
  - -New SAN storage platform
  - -Looking to ensure NIST 800-88r1 Purge compliance
  - -Required custom verification plan to address native compression, deduplication and encryption
  - -Plan required sampling before and after encryption and crypto-erasure
- SSD Manufacturer
  - -Firmware Review
  - - Not erasing all copies of keys

Summary

- Reusing storage media an important piece in sustainability
- Complete sanitization is critical
- 3rd party erasure verification is the only way to ensure compliance with the Sanitization Standards.

Questions?

Future of Media Sanitization

- Build verification into sanitization command
  - Output log page that list all steps performed
    - user area
    - dedicated cache (if any)
    - bad blocks/pages
    - areas skipped (System Area)
      - Not as good as 3rd party verification, but would be more transparent
      - Current command need polling to verify % completed, and contains no details
  - Erasure pattern of other than 0x00 or 0xFF
  - Seeding for Erasure and CryptoErase commands
  - HASH of key storage area (verify keys overwritten)
  - Some form of verification built into the Sanitization command or a separate command.
    - Sample pages to confirm now all format pattern (00s)
    - Hash of sample pages to confirm data data changed (for cryptoerase)

Ontrack®

Find us at booth 1146

*Near the FMS Theater