
# Standards Based Erasure of Solid State and Hybrid Devices

## Session 103-A: Flash Security Like You Mean It

Monty A. Forehand

Seagate Technology

Security Engineering Director


# Why do We Care?

- Data Loss Prevention !
- We all need high assurance sanitization of data.
- Media Sanitization Standards can provide this assurance – they are here now.

# Media Sanitization Standards

## NIST SP 800-88, Rev 1

Public Review
Sept. 2012

Publication
Summer 2013?

**NIST SP 800-88, Rev 1**: Guidelines for Media Sanitization

http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf

- Becomes THE Federal Media Sanitization Standard
- Referenced by other Federal Standards.
- Updated with sanction and guidance for Cryptographic Erase.
- Updated with specific guidance for SSD & Hybrid Devices.

# Media Sanitization Standards
## ISO / IEC 27040

| Comments Now | U.S. Vote & to ISO Sept. 2013 | Publication Planned 2013 |
|---|---|---|

**ISO / IEC 27040:** Information technology-Security techniques-Storage security

http://www.iso27001security.com/html/27040.html

- ISO / IEC 27040 adding requirements for Media Sanitization
- Becomes the international standard.

# NIST SP 800-88, Rev 1, pg. 8

Clear, Purge , and Destroy are actions that can be taken to sanitize media. The categories of Sanitization are defined as follows:

- Clear- A method of sanitization that 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- A method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.
- Destroy- A method of sanitization that 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.

- Purge for strong erasure with techniques that allow re-usability of media.

# NIST SP 800-88, Rev 1, p. 30

| **SCSI Solid State Drives (SSDs)** *This includes SCSI, SAS, Fibre Channel, etc.* | |
|---|---|
| **Clear:** | Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used. |
| **Purge:** | Two options are available:<br>1. Apply the SCSI sanitize command, if supported. One or both of the following options may be available:<br>a. The block erase command.<br>b. If the device supports encryption, the Cryptographic Erase (also known as sanitize crypto scramble) command.<br>*Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure could alternatively be applied.<br>2. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed. Refer to the TCG and vendors shipping TCG Opal or Enterprise storage devices for more information.<br>*Optionally:* After Cryptographic Erase is successfully applied to a device, use the block erase command (if supported) to block erase the media. If the block erase command is not supported, the Clear procedure is an acceptable alternative. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |

Note: TCG, SCSI (T10) and ATA (T13) Standards provide additional requirements for data to be erased by the erase Commands (primary, spares, retired, etc.).

# NIST SP 800-88, Rev 1, p. 10

As a result, sanitization of the target data is reduced to sanitization of the encryption key(s) used to encrypt the target data. Thus, with CE, sanitization may be performed with high assurance much faster than with other sanitization techniques. The encryption itself acts to sanitize the data, subject to constraints identified in this guidelines document. Federal agencies must use FIPS 140 validated encryption modules in order to have assurance that the conditions stated above have been validated for the SED.

- Cryptographic erase (CE) may be performed with high assurance & faster than other techniques.
- FIPS 140 validated modules provide assurance for Federal Agencies.

# NIST SP 800-88, Rev 1, Draft Appendix D

**Table D-1. Cryptographic Erase Considerations**

| Area | Consideration(s) | Relevant Doc(s) |
|---|---|---|
| **Key Generation** | The level of entropy of the random number sources and quality of whitening procedures applied to the random data. This applies to the cryptographic keys, and potentially to wrapping keys affected by the CE operation. | SP800-90[6], SP800-90A, SP800-90B, SP800-90C SP800-133 |
| **Media Encryption** | The security strength and validity of implementation of the encryption algorithm/mode used for protection of the Target Data. | FIPS 140[7], FIPS 197, SP800-38A (not including ECB), SP800-38E |
| **Key Level and Wrapping** | The key being sanitized might not be the Media Encryption Key, but instead a key used to wrap (that is, encrypt) the MEK or another key. In this case, the security strength and level of assurance of the wrapping techniques used should be commensurate with the level of strength of the CE operation | FIPS 197, SP800-38A, SP800-38F, SP800-131A |


# Conclusions

- Erase Standards are here for Solid-State and Hybrid Devices and readying for publication.
- Cryptographic Erase is a viable and sanctioned erase method.
- Work with your device vendors to ensure compliance to these standards – For High Assurance Erase.


# Acknowledgements


- Seagate Team
  - James Hatfield
  - Manuel Offenberg
  - Anthony Duran
  - Harshad Thakar
  - Christopher DeMattio
- Eric Hibbard – HGST, ISO
- Jorge Campello - HGST
- Jason Cox – Intel
- Dmitry Obukhov - Western Digital
- Danny Ybarra - Western Digital