Overview of SP800-88rev1: *Guidelines for Media Sanitization*

Andrew Regenscheid

Computer Security Division, ITL, NIST

National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Media Sanitization

Refers to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

NIST SP800-88

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Why Sanitize?

National Institute of Standards and Technology
U.S. Department of Commerce

NIST SP 800-53rev4

Media Protection Family

MP-6 MEDIA SANITIZATION

Control: The organization:

a. Sanitizes [*Assignment: organization-defined information system media*] prior to disposal, release out of organizational control, or release for reuse using [*Assignment: organization-defined sanitization techniques and procedures*] in accordance with applicable federal and organizational standards and policies; and

b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

Media is Everywhere



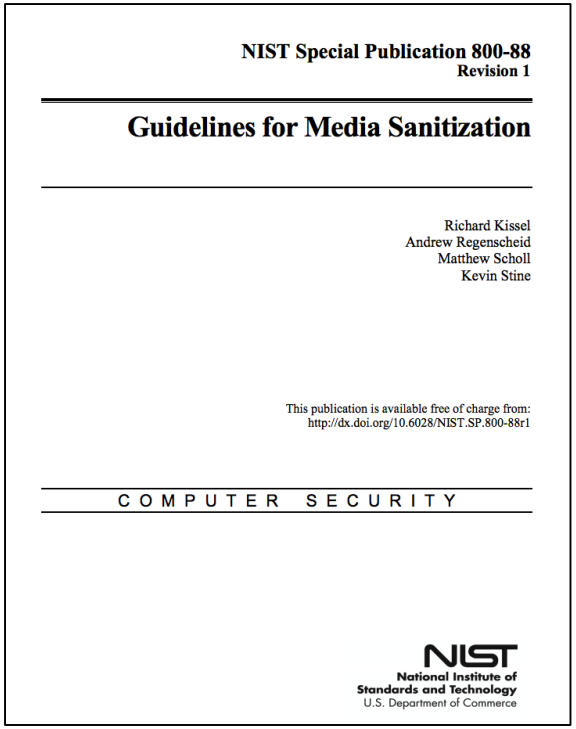




NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST SP 800-88rev1

- Revision released- December 2014
- Provides guidelines for organizations making practical sanitization decisions
  - Considerations for sanitization and disposal
  - Recommended sanitization methods
- Security categorization of information should drive sanitization decisions
- Technical guidelines cover full sanitization of media


NIST Special Publication 800-88
Revision 1

Guidelines for Media Sanitization

Richard Kissel
Andrew Regenscheid
Matthew Scholl
Kevin Stine

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

COMPUTER SECURITY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Document available at:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Roles and Responsibilities

- **Information System Owner**
  Ensures that maintenance or contractual agreements are in place and are sufficient in protecting the confidentiality of the system media and information.
- **Information Owner/Steward**
  Ensures appropriate onsite media maintenance while understanding sensitivity of information under their control.
- **Senior Agency Information Security Officer**
  Ensures that IT security requirements for disposal and sanitization are implemented in a timely and appropriate manner.
- **Property Management Officer**
  Responsible that for ensuring that reused/donated/destroyed media are properly accounted for.

Categorize Data- FIPS 199

Security Objective	Impact levels Low	Moderate	High
Confidentiality	Unauthorized disclosure could have **limited** adverse effect.	Unauthorized disclosure could have **serious** adverse effect.	Unauthorized disclosure could have **severe or catastrophic** adverse effect.
Integrity	Unauthorized modification/destruction could have **limited** adverse effect.	Unauthorized modification/destruction could have **serious** adverse effect.	Unauthorized modification/destruction could have **severe or catastrophic** adverse effect.
Availability	Disruption of access could have **limited** adverse effect.	Disruption of access could have **serious** adverse effect.	Disruption of access could have **severe or catastrophic** adverse effect.

Sanitization Types

Clear

- Resistant to keyboard attacks.

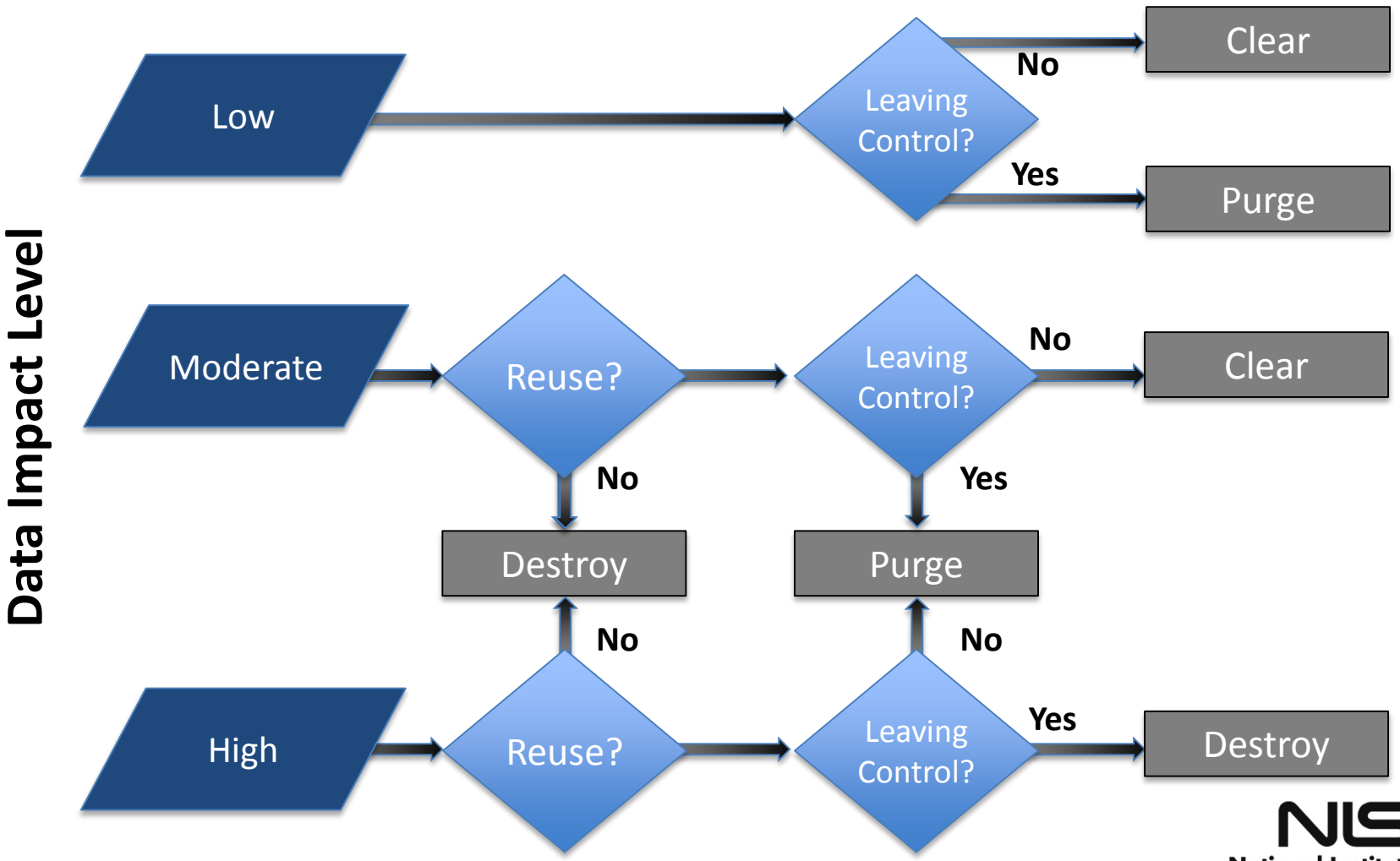
Purge

- Resistant to laboratory attacks.

Destroy

- Resistant to recreation of media

Decision Flow



Summary

- **Security categorization of data**
- **Determine sanitization type**

  Considering:
  - Security categorization of data
  - Desire to reuse media
  - If you will retain control of the media
- **Select/perform media-appropriate method**
- **Verification of sanitization results**

NIST National Institute of Standards and Technology U.S. Department of Commerce

Challenge and Trends

- New Technologies
  - Advances in storage media
  - Storage interfaces
- User-inaccessible Regions
- Wear-Leveling in Flash Memory
- Self-Encrypting Drives & Cryptographic Erase

Sanitization Methods

Examples:

- Destroy methods
- Degaussing
- Overwriting/Block Erase
- Cryptographic Erase

Destroy

- **Definition:** *A method of sanitization that renders data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data*

- **Examples**:
  - Shred
  - Disintegrate
  - Pulverize
  - Incinerate

Degaussing

- **Definition:** *To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field*
- Uses a strong magnet to sanitize magnetic media
- Process may be destructive
  - Modern hard drives, some tape systems will be rendered unusable
  - Lower-tech magnetic media might be reusable

Overwriting/Block Erase

- **Overwrite**
  - *Writing data on top of the physical location of data stored on the media*
  - Single-pass typically sufficient for magnetic media
  - Supports CLEAR, possibly PURGE
- **Block Erase**
  - *Electrical erasure of individual blocks in flash memory, generally resetting bits to "1"*
  - Supports CLEAR or PURGE
- **SANITIZE Commands**
  - ATA and SCSI command sets support sanitization
  - May overwrite/erase user-inaccessible areas

NIST National Institute of Standards and Technology U.S. Department of Commerce

Cryptographic Erase

- ***Definition:*** A method where the cryptographic key used to encrypt data is sanitized, making recovery of the (plaintext) data infeasible.
- Supported by some forms of media that transparently encrypt all data written to the media.
- Strength of sanitization based on strength of:
  - Cryptographic algorithms and modules
  - Management of cryptographic keys
  - Sanitization of the key(s)
- Provides very fast sanitization
- Supports selective (partial) sanitization

NIST National Institute of Standards and Technology U.S. Department of Commerce

Media-Specific Recommendations

- **Appendix A** provides recommended sanitization methods for common media, e.g.,
  - Hard copy (e.g., paper)
  - Office equipment (e.g., copy/fax machine)
  - Magnetic media
  - Flash/Solid State media (e.g., SSDs, flash drives)
  - Mobile devices
  - Optical media

Magnetic Hard Drives

- **Clear**
  - Single-pass overwrite
- **Purge**
  - ATA/SCSI sanitize command (or similar) using OVERWRITE
  - Cryptographic Erase
  - Degauss
- **Destroy**
  - Shred/Disintegrate/Pulverize/Incinerate

Solid State Drives

- **Clear**
  - Single-pass overwrite
    Warning: Overwriting on SSDs may be unreliable due to wear leveling.
- **Purge**
  - ATA/SCSI sanitize command (or similar) using BLOCK ERASE
  - Cryptographic Erase
- **Destroy**
  - Shred/Disintegrate/Pulverize/Incinerate

USB Flash Drives

- **Clear**
  - Two-pass overwrite
- **Purge**
  - **Most do not support sanitize commands**
  - If supported, typically implemented using vendor-specific interfaces/methods
- **Destroy**
  - Shred/Disintegrate/Pulverize/Incinerate

Mobile Devices

- **Clear**
  - Perform a factory or data reset
  - Remote wipe
- **Purge**
  - Vendor-specific capabilities
  - Factory/data reset ***MAY*** effectively purge data using a block erase or cryptographic erase
  - Consult SP800-88rev1 and vendor for more information
- **Destroy**
  - Shred/Disintegrate/Pulverize/Incinerate

Verification

- Verification ensures target data was effectively sanitized
- What to sample?
  - If time/resources permit, verify each piece of media; or
  - Representative sampling
- Caveats
  - Not applicable to destructive methods
  - Verification may not be possible with Cryptographic Erase
- Document verification results

NIST National Institute of Standards and Technology U.S. Department of Commerce

Documentation

CERTIFICATE OF SANITIZATION		
PERSON PERFORMING SANITIZATION		
Name:	Title:	
Organization:	Location:	Phone:
MEDIA INFORMATION		
Make/ Vendor:	Model Number:	
Serial Number:		
Media Property Number:		
Media Type:	Source *(ie user name or PC property number)*:	
Classification:	Data Backed Up: ☐ Yes ☐ No ☐ Unknown	
Backup Location:		
SANITIZATION DETAILS		
Method Type: ☐ Clear ☐ Purge ☐ Damage ☐ Destruct		
Method Used: ☐ Degauss ☐ Overwrite ☐ Block Erase ☐ Crypto Erase ☐ Other:		
Method Details:		
Tool Used *(include version)*:		
Verification Method: ☐ Full ☐ Quick Sampling ☐ Other:		
Post Sanitization Classification:		
Notes:		
MEDIA DESTINATION		
☐ Internal Reuse ☐ External Reuse ☐ Recycling Facility ☐ Manufacturer ☐ Other *(specify in details area)*		
Details:		
SIGNATURE		
I attest that the information provided on this statement is accurate to the best of my knowledge.		
Signature:		Date:
VALIDATION		
Name:	Title:	
Organization:	Location:	Phone:
Signature:		Date:

ISO/IEC 27040:2015

- Storage security
- ISO/IEC 27040 covers:
  - Key storage and storage security concepts
  - Associated Risks
  - Security controls for storage architectures
  - Guidelines on design/implementation
  - ***Media-specific sanitization guidance***

Based on NIST SP800-88r1 Appendix A

Summary

- **Security categorization of data**
- **Determine sanitization type**

  Considering:
  - Security categorization of data
  - Desire to reuse media
  - If you will retain control of the media
- **Select/perform media-appropriate method**
- **Verification of sanitization results**
- **Documentation**

NIST National Institute of Standards and Technology U.S. Department of Commerce

More Information

NIST standards and guidelines available at:

http://csrc.nist.gov

Contact Information

Andrew Regenscheid

Andrew.Regenscheid@nist.gov