Introduction to:
NIST SP 800-88
Guidelines for Media Sanitization
“This guide will assist organizations... in making practical sanitization decisions based on categorization of information”
NIST 800-88

- Practical, real world reference for media sanitization guidance and compliance
- Introduced in 2006, updated 2012 to address changing technologies
- Replaced DoD 5220.22M standard in regulatory and certification practice
NIST 800-88

People

Process

Technology
NIST 800-88

Roles and Responsibilities
Media sanitization is a process by which data is irreversibly removed from media or the media is permanently destroyed.
Media Sanitization

Common Methods of Media Sanitization:
- Overwriting
- Cryptographic Erase
- Degaussing
- Physical Destruction
Classification or types of sanitization methods:

**Clear**: protection against a keyboard attack

**Purge**: protection against a laboratory attack

**Destroy**: media cannot be reused
NIST 800-88

Guidance on Sanitization and Disposition Decisions
Potential Impact Analysis:

<table>
<thead>
<tr>
<th>Potential Impact</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Loss of confidentiality, integrity, or availability could be expected to have a <em>limited</em> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>Moderate</td>
<td>Loss of confidentiality, integrity, or availability could be expected to have a <em>serious</em> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
<tr>
<td>High</td>
<td>Loss of confidentiality, integrity, or availability could be expected to have a <em>severe or catastrophic</em> adverse effect on organizational operations, organizational assets, or individuals.</td>
</tr>
</tbody>
</table>

NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
Under Organizational Control:

- Media are considered under organizational control if contractual agreements are in place with the organization and the [vendor] specifically provides for the confidentiality of the information.

- “Maintenance” being performed on an organization’s site, under the organization’s supervision.

Not Under Organizational Control:

- Media exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the organization.
Technology challenges:

• Evolutionary changes with storage media
  – Sanitization requirements must adapt
    • Overwriting, degaussing, encryption, destruction

• Introduction of alternative technologies
  – Flash memory-based storage/solid state drives (SSDs)

• Revolutionary changes with sanitization
  – Departure from hardware and software uniformity
  – Shifting burden of proof
NIST 800-88 Recommendations

**Hard Copy Storage**

*Includes paper and microforms*

**Clear** and **Purge** are not possible sanitization methods for these media. To **Destroy**, paper must be shredded using a cross cut process into particles 1mm x 5mm in size or smaller. Paper may also be pulverized through a 2.4mm screen. Microforms (microfilm, microfiche or photo negatives) are considered destroyed when burnt to a white ash.
NIST 800-88 Recommendations

Magnetic Media and Optical Media
Includes tape drives, floppies, CDs, and DVDs.

Clear and Purge are not possible sanitization methods for CDs or DVDs. Magnetic Media (tapes and floppies) can be Cleared through a one-pass overwrite and verification or can be Purged using a proper degausser. These media meet the Destroy method through incineration or shredding.
NIST 800-88 Recommendations

Office Equipment
Includes copiers, printers, and multifunction machines

These devices may contain flash memory or magnetic hard drives. Clear can generally be achieved by resetting to factory settings. Purge may be applicable to specific devices and is dependent on the firmware of the device. Units with removable storage media can follow the sanitization technique for the associated storage device. Destroy these devices by removing any storage media and shredding. The whole unit does not necessarily need to be shredded.
Networking Devices

Includes routers and switches

Routers and switches may contain IP addresses and other identifiable information that can facilitate hacking into a network. The Clear method of sanitization involves performing a full manufacturer’s reset back to default factory settings. Purge may be available on some devices using block erasing. Destroy is achieved through shredding.
NIST 800-88 Recommendations

Hard Drives using Magnetic Media Storage

*Includes ATA, SCSI and Fibre Channel drives*

A one-pass overwrite meets the **Clear** requirement; Secure Erase, Cryptographic Erase, or other embedded overwrite tools meet the **Purge** requirement; Shredding, disintegrating and burning meet the **Destroy** requirement. Verification must be performed for each **Clear** or **Purge** technique. Fibre Channel drives require specialized sanitization.
NIST 800-88 Recommendations

Flash Memory-Based Storage Devices
Includes Solid State Drives (SSDs), USB drives, SD cards, and embedded flash memory on boards

Clear may be achieved using validated overwriting tools and may require one or two pass sanitization. Some flash memory can be Cleared by resetting to factory state. Purge can be achieved on some devices with Block Erase or Cryptographic Erase features - but verification is required of each Purge. Each manufacturer has different sanitization requirements. Because these devices use chips and are small, the Destroy specification can only be met by running pins through chips, fine shredding, pulverizing and/or melting.
Mobile Devices with Flash Memory

*Includes smart phones and tablets*

**Clear** or **Purge** can generally be achieved by resetting to factory settings and/or selecting a full sanitize ("Erase All Content") option. Each manufacturer and Operating System requires a unique sanitization process. **Destroy** by shredding (remove batteries first!) - Ensure SIM cards are removed and destroyed as well.
Use NIST guidelines to:

- Set a policy for managing data risk on retired, repurposed and reused assets
- Provide a comprehensive review of what data bearing devices you own and manage
- Develop and implement training and controls (including sanitization methods) consistent with policy
- Ensure proper implementation within and outside of the organization's control
THANK YOU!!!

Contact Information:
TJ Barelmann, CSDS
Director of Operations
Cascade Asset Management
608-316-6634/608-280-1840
tj@cascade-assets.com
@TJBarelmann
Appendix of NIST sanitization tables
## NIST 800-88 Recommendations

### Hard Copy Storage

<table>
<thead>
<tr>
<th>Paper and microforms</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clear:</strong></td>
<td>N/A, see Destroy</td>
</tr>
<tr>
<td><strong>Purge:</strong></td>
<td>N/A, see Destroy</td>
</tr>
<tr>
<td><strong>Destroy:</strong></td>
<td>Destroy paper using cross cut shredders into particles that are 1mm X 5mm is size or smaller, or pulverize, disintegrate paper materials using disintegrator devices equipped with a 3/32 in. security screen. Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning.</td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
<td>When material is burned, residue must be reduced to ash</td>
</tr>
</tbody>
</table>

---

*NIST 800-88 Table A-1 ***Table is paraphrased/summarized for purposes of presentation*
# NIST 800-88 Recommendations

## Networking Devices

### Routers and Switches (home, home office, enterprise)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clear:</strong></td>
<td>Perform a full manufacturer’s reset to reset the router or switch back to its factory default settings.</td>
</tr>
<tr>
<td><strong>Purge:</strong></td>
<td>See Destroy. Most routers and switches only offer capabilities to Clear (and not Purge) the data contents. A router or switch may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Refer to device manufacturer to identify if the device has a Purge capability that applies media-dependant techniques to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.</td>
</tr>
<tr>
<td><strong>Destroy:</strong></td>
<td>Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.</td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
<td>For both Clear and Purge, refer to the manufacturer for additional information on the proper Sanitization procedure. Network devices may contain removable storage. The removable media must be removed and sanitized using media-specific techniques.</td>
</tr>
</tbody>
</table>

---

NIST 800-88 Table A-2 ***Table is paraphrased/summarized for purposes of presentation***

www.cascade-assets.com
## NIST 800-88 Recommendations

### Mobile Devices

<table>
<thead>
<tr>
<th>Apple iPhone and iPad (current generation and future iPhones and iPads)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clear:</strong></td>
</tr>
<tr>
<td><strong>Purge:</strong></td>
</tr>
<tr>
<td><strong>Destroy:</strong></td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
</tr>
</tbody>
</table>
# NIST 800-88 Recommendations

## Mobile Devices

### Devices running the Google Android OS

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clear:</strong></td>
<td>Perform a factory reset through the device’s setting menu...refer to the user manual. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results.</td>
</tr>
<tr>
<td><strong>Purge:</strong></td>
<td>The capabilities of Android devices are determined by device manufacturers and service providers. Some versions of Android support encryption, and may support Cryptographic Erase. Refer to device manufacturer to identify if the device has a Purge capability that applies media-dependant techniques to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.</td>
</tr>
<tr>
<td><strong>Destroy:</strong></td>
<td>Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.</td>
</tr>
</tbody>
</table>

**Notes:** For both Clear and Purge, refer to the manufacturer for additional information on the proper sanitization procedure.

---

NIST 800-88 Table A-3***Table is paraphrased/summarized for purposes of presentation
### Equipment

<table>
<thead>
<tr>
<th><strong>Office Equipment</strong></th>
<th><em>This includes copy, print, fax, and multifunction machines</em></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clear:</strong></td>
<td>Perform a full manufacturer’s reset to reset the office equipment to its factory default settings.</td>
</tr>
<tr>
<td><strong>Purge:</strong></td>
<td>See Destroy. Most office equipment only offers capabilities to Clear (and not Purge) the data contents. A router or switch may offer Purge capabilities, but these capabilities are specific to the hardware and firmware of the device and should be applied with caution. Office equipment may contain removable storage. The removable media must be removed and sanitized using media-specific techniques.</td>
</tr>
<tr>
<td><strong>Destroy:</strong></td>
<td>Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.</td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
<td>For both Clear and Purge, manually navigate to multiple areas of the device (such as stored fax numbers, network configuration information, etc.) to verify that no personal information has been retained on the device.</td>
</tr>
</tbody>
</table>
## NIST 800-88 Recommendations

### Magnetic Media

**ATA Hard Drives** *This includes PATA, SATA, eSATA, etc.*

<table>
<thead>
<tr>
<th>Clear:</th>
<th>Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge:</td>
<td>Four options are available: 1. Use the ATA Sanitize Device feature set of commands. 2. Use the ATA Security feature set’s SECURE ERASE UNIT command, if supported, in Enhanced Erase mode. 3. Cryptographic Erase through the Trusted Computing Group.... 4. Degauss in an organizationally approved automatic degausser or disassemble the disk drive and Purge the enclosed platters with an organizationally approved deguassing wand.</td>
</tr>
</tbody>
</table>

NIST 800-88 Table A-5***Table is paraphrased/summarized for purposes of presentation
### NIST 800-88 Recommendations

#### Magnetic Media – continued

<table>
<thead>
<tr>
<th>ATA Hard Drives</th>
<th>This includes PATA, SATA, eSATA, etc.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destroy:</strong></td>
<td>Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.</td>
</tr>
<tr>
<td><strong>Notes:</strong></td>
<td>Verification must be performed for each technique within Clear and Purge, except degaussing. The assurance provided by degaussing depends on selecting an effective degausser, applying it appropriately and periodically spot checking the results to ensure it is working as expected.</td>
</tr>
</tbody>
</table>

NIST 800-88 Table A-5***Table is paraphrased/summarized for purposes of presentation
## Peripherally Attached Storage

### External Locally Attached Hard Drives

*This includes, USB, Firewire, et. (Treat eSATA as ATA hard drive.)*

<table>
<thead>
<tr>
<th>Clear</th>
<th>Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros. Multiple write passes or more complex values may optionally be used.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purge:</td>
<td></td>
</tr>
<tr>
<td>Destroy:</td>
<td>Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.</td>
</tr>
</tbody>
</table>
## Optical Media

<table>
<thead>
<tr>
<th>Optical Media</th>
<th>CD, DVD, BD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clear:</td>
<td>N/A</td>
</tr>
<tr>
<td>Purge:</td>
<td>N/A</td>
</tr>
</tbody>
</table>
| Destroy:      | Destroy in order of recommendations:  
                1. Removing the information-bearing layers of CD media using a commercial optical disk grinding device. Note that this applies only to CD and not to DVD or BD media.  
                2. Incinerate optical disk media (reduce to ash) using a licensed facility.  
                3. Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of 0.5 mm and surface area of 0.25 mm or smaller. |