# Guidelines for Media Sanitization

From the National Institute of Standards and Technology's

NNIST SP 800-88 Rev. 1

# Table of Contents

## Appendix A—Minimum Sanitization Recommendations

Once a decision is made based on factors such as those described in Section 4, and after applying relevant organizational environmental factors, then the tables in this Appendix can be used to determine recommended sanitization of specific media. That recommendation should reflect the FIPS 199 security categorization of the system confidentiality to reduce the impact of harm of unauthorized disclosure of information from the media.

Although use of the tables in this Appendix is recommended here, other methods exist to satisfy the intent of Clear, Purge, and Destroy. Methods not specified in this table may be suitable as long as they are verified and found satisfactory by the organization. Not all types of available media are specified in this table. If your media are not included in this guide, organizations are urged to identify and use processes that will fulfill the intent to Clear, Purge, or Destroy their media.

When an organization or agency has a sanitization technology, method and/or tool that they trust and have tested, they are strongly encouraged to share this information through public forums, such as the Federal Agency Security Practices (FASP) website[19]. The FASP effort was initiated as a result of the success of the Federal Chief Information Officer (CIO) Council's Federal Best Security Practices (BSP) pilot effort to identify, evaluate, and disseminate best practices for critical infrastructure protection (CIP) and security.

The proper initial configuration of each type of device helps ensure that the sanitization operation is as effective as possible. While called out for some specific items below, users are encouraged to check manufacturer recommendations and guides such as the DISA Security Technical Implementation Guides (STIGs)[20] for additional information about recommended settings for any other items in this list as well.

If a mobile device has nonvolatile removable memory, it may contain additional information that may or may not be addressed by the sanitization process identified in Table A-3. Contact the manufacturer and/or cellular provider to determine what types of data are stored on the removable memory and identify whether any additional sanitization is required for the removable memory. Additional details about such removable memory and associated data recovery capabilities are available in NIST SP 800-101 Revision 1[21]. If a mobile device does not have sufficient built-in sanitization appropriate for the sensitivity or impact level of the data it contains, then rather than destroy the device (to protect the information) consider contacting businesses providing sanitization services to determine if their services meet your needs.

Many internal storage devices (as opposed to removable media, such as an SD card) as well as storage subsystems that incorporate installed media, support dedicated sanitize commands. The

[19] http://csrc.nist.gov/groups/SMA/fasp/

[20] http://iase.disa.mil/stigs/

[21] NIST SP 800-101 Revision 1, *Guidelines on Mobile Device Forensics*, May 2014, 87 pp. http://dx.doi.org/10.6028/NIST.SP.800-101r1.

availability of these commands is impacted in some cases by system (i.e., BIOS/UEFI—Basic Input-Output System/Unified Extensible Firmware Interface) characteristics, such as how and when freeze lock commands are issued to a device. The use of a dedicated computer or equipment to perform sanitization that facilitates leveraging these commands (such as a PC or workstation, with an external drive bay that facilitates safely connecting a drive after the system has been powered on) can help address this issue. The behavior and methods to bypass freeze lock or other limitations on command availability vary between computers, so refer to the computer manufacturer for details about the behavior of specific models. Alternative approaches exist for addressing the issue, and will vary depending on the hardware, software, and firmware of the computer. University of California San Diego (UCSD)'s Center for Magnetic Recording Research (CMRR) has also developed some tools and documentation about work-arounds for this issue (see Appendix C for details).

Some sanitization procedures feature additional optional methods. The choice regarding whether to apply the optional components depends on the level of confidentiality of the data and assurance of correct implementation of the non-optional portion of the sanitization procedure. For example, an organization might decide that for PII, for example, that any method applied with an available optional component should execute that optional component. The choice may also be based on the time factor, as some procedures, including the optional method, can be executed in a total of a matter of minutes. In that case, the organization might decide to include the optional component even if the data is not in a higher confidentiality category.

**Table A-2: Networking Device Sanitization**

| Networking Devices | |
|---|---|
| **Routers and Switches (home, home office, enterprise)** | |
| **Clear:** | Perform a full manufacturer's reset to reset the router or switch back to its factory default settings. |
| **Purge:** | 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 the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | For both Clear and (if applicable) Purge, refer to the manufacturer for additional information on the proper Sanitization procedure.<br>Network Devices may contain removable storage. The removable media must be removed and sanitized using media-specific techniques. |

**Table A-3: Mobile Device Sanitization**

| **Mobile Devices**<br>**(If a device has removable storage – first check for encryption and unencrypt if so – then remove the removable storage prior to sanitization)** | |
|---|---|
| **Apple iPhone and iPad (current generation and future iPhones and iPads)** | |
| **Clear:** | Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu). (The sanitization operation should take only minutes as Cryptographic Erase is supported. This assumes that encryption is on and that all data has been encrypted.) Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results. |
| **Purge:** | Select the full sanitize option (typically in the 'Settings > General > Reset > Erase All Content and Settings' menu). (The sanitization operation should take only minutes with Cryptographic Erase being supported. This assumes that encryption is on and that all data has been encrypted.) |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Before sanitizing the device, ensure that the data is backed up to a safe place.<br>Current iPhones have hardware encryption – turned on by default. |
| **Blackberry** | **(back up data on device before sanitization)** |
| **Clear:** | BB OS 7.x/6.x - Select Options > Security Options > Security Wipe , making sure to select all subcategories of data types for sanitization. Then type "blackberry" in the text field, then click on "Wipe" ("Wipe Data" in BB OS 6.x) BB OS 10.x (Decrypt media card before continuing) Select Settings, Security and Privacy, Security Wipe . Type "blackberry" in the text field, then click on "Delete Data". The sanitization operation may take as long as several hours depending on the media size. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results. |
| **Purge:** | BB OS 7.x/6.x - Select Options > Security > Security Wipe, then make sure to select all subcategories of data types for sanitization. Then type "blackberry" in the text field, then click on "Wipe" ("Wipe Data" in BB OS 6.x). For BB OS 10.x Select Settings> Security and Privacy>Security Wipe. Type "blackberry" in the text field, then click on "Delete Data". The |

| | |
|---|---|
| | sanitization operation may take as long as several hours depending on the media size. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Centralized management (BES) allows for device encryption.<br>Refer to the manufacturer for additional information on the proper sanitization procedure, and for details about implementation differences between device versions and OS versions. Proper initial configuration using guides such as the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs) (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible. If the device contains removable storage media, ensure that the media is sanitized using appropriate media-dependent procedures. |
| **Devices running the Google Android OS** | **(connect to power before starting encryption)** |
| **Clear:** | Perform a factory reset through the device's settings menu. For example, on Samsung Galaxy S5 running Android 4.4.2, select settings, then, under User and Backup, select Backup and reset, then select Factory data reset. For other versions of Android and other mobile phone devices, 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. |
| **Purge:** | The capabilities of Android devices are determined by device manufacturers and service providers. As such, the level of assurance provided by the factory data reset option may depend on architectural and implementation details of a particular device. Devices seeking to use a factory data reset to purge media should use the eMMC Secure Erase or Secure Trim command, or some other equivalent method (which may depend on the device's storage media).<br>Some versions of Android support encryption, and may support Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a Purge capability that applies media-dependent sanitization techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | Proper initial configuration using guides such as the DISA STIGs (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible. Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. When in doubt, check device manual or call tech support.<br>For both Clear and Purge, refer to the manufacturer for additional information on the proper sanitization procedure. |
| **Windows Phone OS 7.1/8/8.x** | **(Centralized management may be needed for encryption)** |
| **Clear:** | Select the Settings option (little gear symbol) from the live tile or from the app list. On the "Settings" page, scroll to the bottom of the page and select the "About" button. In the about page, there will be a **reset your phone** button at the bottom of the page. Click on this button to continue. Choose Yes when you see the warning messages. Please note that after the process is completed, all your personal content will disappear. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results. |
| **Purge:** | The capabilities of Windows Phone devices are determined by device manufacturers and service providers. As such, the level of assurance provided by the factory data reset |

| | |
|---|---|
| | option may depend on architectural and implementation details of a particular device. Devices seeking to use a factory data reset to purge media should use the eMMC Secure Erase or Secure Trim command, or some other equivalent method (which may depend on the device's storage media).<br>In some environments, Windows Phone devices may support encryption, and may support Cryptographic Erase. Refer to the device manufacturer (or service provider, if applicable) to identify whether the device has a Purge capability that applies media-dependent sanitization techniques or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | Following the Clear/Purge operation, manually navigate to multiple areas of the device (such as browser history, files, photos, etc.) to verify that no personal information has been retained on the device. Before sanitizing your device, ensure that you back up your data to a safe location.<br>Refer to the manufacturer for proper sanitization procedure, and for details about implementation differences between device versions and OS versions. Proper initial configuration using guides such as the DISA STIGs (http://iase.disa.mil/stigs/) helps ensure that the level of data protection and sanitization assurance is as robust as possible. |
| **All other mobile devices** *This includes cell phones, smart phones, PDAs, tablets, and other devices not covered in the preceding mobile categories.* | |
| **Clear:** | Manually delete all information, then perform a full manufacturer's reset to reset the mobile device to factory state. Sanitization performed via a remote wipe should be treated as a Clear operation, and it is not possible to verify the sanitization results. |
| **Purge:** | See Destroy. Many mobile devices only offer capabilities to Clear (and not Purge) the data contents. A mobile device may offer Purge capabilities, but these capabilities are specific to the hardware and software of the device and should be applied with caution. The device manufacturer should be referred to in order to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | Following the Clear or (if applicable) Purge operation, manually navigate to multiple areas of the device (such as call history, browser history, files, photos, etc.) to verify that no personal information has been retained on the device.<br>For both Clear and (if applicable) Purge, refer to the manufacturer for proper sanitization procedure. |

**Table A-4: Equipment Sanitization**

| **Equipment** |
|---|
| **Office Equipment** *This includes copy, print, fax, and multifunction machines* |

| | |
|---|---|
| **Clear:** | Perform a full manufacturer's reset to reset the office equipment to its factory default settings. |
| **Purge:** | See Destroy. Most office equipment only offers capabilities to Clear (and not Purge) the data contents. Office equipment 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 the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting or block erasing) or Cryptographic Erase to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. Office equipment may have removable storage media, and if so, media-dependent sanitization techniques may be applied to the associated storage device. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | For both Clear and (if applicable) 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.<br>For both Clearing and (if applicable) Purge, the ink, toner, and associated supplies (drum, fuser, etc.) should be removed and destroyed or disposed of in accordance with applicable law, environmental, and health considerations. Some of these supplies may retain impressions of data printed by the machine and therefore could pose a risk of data exposure, and should be handled accordingly. If the device is functional, one way to reduce the associated risk is to print a blank page, then an all-black page, then another blank page. For devices with dedicated color components (such as cyan, magenta, and yellow toners and related supplies), one page of each color should also be printed between blank pages. The resulting sheets should be handled at the confidentiality of the Office Equipment (prior to sanitization). Note that these procedures do not apply to supplies such as ink/toner on a one-time use roll, as they are typically not used again and therefore will not be addressed by sending additional pages through the equipment. They will, however, still need to be removed and destroyed. Office Equipment supplies may also pose health risks, and should be handled using appropriate procedures to minimize exposure to the print components and toner.<br>For both Clear and (if applicable) Purge, refer to the manufacturer for additional information on the proper sanitization procedure. |

**Table A-5: Magnetic Media Sanitization**

| **Magnetic Media** | |
|---|---|
| **Floppies** | |
| **Clear:** | Overwrite media by using organizationally approved software and perform verification on the overwritten data. 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. |
| **Purge:** | Degauss in an organizationally approved degausser rated at a minimum for the media. |
| **Destroy:** | Incinerate floppy disks and diskettes by burning in a licensed incinerator or Shred. |
| **Magnetic Disks (flexible or fixed)** | |
| **Clear:** | Overwrite media by using organizationally approved software and perform verification on the overwritten data. 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. |

| | |
|---|---|
| **Purge:** | Degauss in an organizationally approved degausser rated at a minimum for the media. |
| **Destroy:** | Incinerate disks and diskettes by burning in a licensed incinerator or Shred. |
| **Notes:** | Degaussing magnetic disks typically renders the disk permanently unusable. |
| **Reel and Cassette Format Magnetic Tapes** | |
| **Clear:** | Re-record (overwrite) all data on the tape using an organizationally approved pattern, using a system with similar characteristics to the one that originally recorded the data. For example, overwrite previously recorded sensitive VHS format video signals on a comparable VHS format recorder. All portions of the magnetic tape should be overwritten one time with known non-sensitive signals. Clearing a magnetic tape by re-recording (overwriting) may be impractical for most applications since the process occupies the tape transport for excessive time periods. |
| **Purge:** | Degauss the magnetic tape in an organizationally approved degausser rated at a minimum for the media. |
| **Destroy:** | Incinerate by burning the tapes in a licensed incinerator or Shred. |
| **Notes:** | Preparatory steps for Destruction, such as removing the tape from the reel or cassette prior to Destruction, are unnecessary. However, segregation of components (tape and reels or cassettes) may be necessary to comply with the requirements of a Destruction facility or for recycling measures. |
| **ATA Hard Disk Drives** *This includes PATA, SATA, eSATA, etc* | |
| **Clear:** | 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. |
| **Purge:** | Four options are available:<br>1. Use one of the ATA Sanitize Device feature set commands, if supported, to perform a Sanitize operation. One or both of the following options may be available:<br>a. The overwrite EXT command. Apply one write pass of a fixed pattern across the media surface. Some examples of fixed patterns include all zeros or a pseudorandom pattern. A single write pass should suffice to Purge the media.<br>*Optionally:* Instead of one write pass, use three total write passes of a pseudorandom pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified.<br>b. If the device supports encryption and the technical specifications described in this document have been satisfied, the Cryptographic Erase (also known as CRYPTO SCRAMBLE EXT) command.<br>*Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase.<br>2. Use the ATA Security feature set's SECURE ERASE UNIT command, if support, in Enhanced Erase mode. The ATA Sanitize Device feature set commands are preferred over the over the ATA Security feature set SECURITY ERASE UNIT command when supported by the ATA device.<br>3. Cryptographic Erase through the Trusted Computing Group (TCG) Opal Security Subsystem Class (SSC) or Enterprise SSC interface by issuing commands as |

| | |
|---|---|
| | necessary to cause all MEKs to be changed (if the requirements described in this document have been satisfied). Refer to the TCG and device manufacturers for more information.<br>*Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Secure Erase or the Clear procedure could alternatively be applied following Cryptographic Erase.<br>4. Degauss in an organizationally approved automatic degausser or disassemble the hard disk drive and Purge the enclosed platters with an organizationally approved degaussing wand. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | 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.<br>When using the three pass ATA sanitize overwrite procedure with the invert option, the verification process would simply search for the original pattern (which would have been written again during the third pass).<br>The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media as defined in the ATA standard, such as a Host Protected Area (HPA), Device Configuration Overlay (DCO), or Accessible Max Address. Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. Recovery data, such as an OEM-provided restoration image may have been stored in this manner, and sanitization may therefore impact the ability to recover the system unless reinstallation media is also available.<br>When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in section 4.7 should also be performed after any additional techniques are applied following Cryptographic Erase.<br>Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D.<br>Given the variability in implementation of the ATA Security feature set SECURITY ERASE UNIT command, use of this command is not recommended without first consulting with the manufacturer to verify that the storage device's model-specific implementation meets the needs of the organization.<br>This guidance applies to Legacy Magnetic media only, and it is critical to verify the media type prior to sanitization. Note that emerging media types, such as HAMR media or hybrid drives may not be easily identifiable by the label. Refer to the manufacturer for details about the media type in a storage device.<br>Degaussing the media in a storage device typically renders the device unusable. |
| **SCSI Hard Disk Drives** *This includes Parallel SCSI,Serial Attached SCSI (SAS), Fibre Channel, USB Attached Storage (UAS), and SCSI Express Partial sanitization is not supported in this section.* | |
| **Clear:** | Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may optionally be used. |
| **Purge:** | Four 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 OVERWRITE service action. Apply one write pass of a fixed pattern across the media surface. Some examples of fixed patterns include all zeros or a pseudorandom pattern. A single write pass should suffice to Purge the media.<br>*Optionally:* Instead of one write pass, use three total write passes of a pseudorandom pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified.<br>b. If the device supports encryption, the CRYPTOGRAPHIC ERASE service action.<br>*Optionally:* After Cryptographic Erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite 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 overwrite command (if supported) to write one pass of zeros or a pseudorandom pattern across the media. If the overwrite command is not supported, the Clear procedure could alternatively be applied.<br>3. Degauss in an organizationally approved automatic degausser or disassemble the hard disk drive and Purge the enclosed platters with an organizationally approved degaussing wand. The degausser/wand should be rated sufficient for the media. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection, 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.<br>When using the three pass SCSI sanitize overwrite procedure with the invert (also known as complement) option, the verification process would simply search for the original pattern (which would have been written again during the third pass). While it is widely accepted that one pass of overwriting should be sufficient for Purging the data, the availability of a dedicated command that incorporates the ability to invert the data pattern allows an efficient and effective approach that mitigates any residual risk associated with variations in implementations of magnetic recording features across device manufacturers.<br>The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media, such as "SCSI mode parameter block descriptor's NUMBER OF LOGICAL BLOCKS field (accessible with the SCSI MODE SENSE and MODE SELECT commands". Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique.<br>When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase.<br>Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D.<br>This guidance applies to Legacy Magnetic media only, and it is critical to verify the media type prior to sanitization. Note that emerging media types, such as HAMR media or hybrid drives may not be easily identifiable by the label. Refer to the manufacturer for details about the media type in a storage device. |

| | |
|---|---|
| | Degaussing the media in a storage device typically renders the device unusable. |

**Table A-6: Peripherally Attached Storage Sanitization**

| **Peripherally Attached Storage** | |
|---|---|
| **External Locally Attached Hard Drives** *This includes, USB, Firewire, etc. (Treat eSATA as ATA Hard drive.)* | |
| **Clear:** | Overwrite media by using organizationally approved and tested 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:** | The implementation of External Locally Attached Hard Drives varies sufficiently across models and vendors that the issuance of any specific command to the device may not reasonably and consistently assure the desired sanitization result.<br>When the external drive bay contains an ATA or SCSI hard drive, if the commands can be delivered natively to the device, the device may be sanitized based on the associated media-specific guidance. However, the drive could be configured in a vendor-specific manner that precludes sanitization when removed from the enclosure. Additionally, if sanitization techniques are applied, the hard drive may not work as expected when reinstalled in the enclosure.<br>Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting, block erasing, Cryptographic Erase, etc.) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | Verification as described in the Verify Methods subsection must be performed for each technique within Clear and Purge.<br>Some external locally attached hard drives, especially those featuring security or encryption features, may also have hidden storage areas that might not be addressed even when the drive is removed from the enclosure. The device vendor may leverage proprietary commands to interact with the security subsystem. Please refer to the manufacturer to identify whether any reserved areas exist on the media and whether any tools are available to remove or sanitize them, if present. |

**Table A-7: Optical Media Sanitization**

| **Optical Media** | |
|---|---|
| **CD, DVD, BD** | |
| **Clear/ Purge:** | N/A |

| | |
|---|---|
| **Destroy:** | Destroy in order of recommendations:<br>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<br>2. Incinerate optical disk media (reduce to ash) using a licensed facility.<br>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 $\text{mm}^2$ or smaller. |

**Table A-8: Flash Memory-Based Storage Device Sanitization**

| **Flash Memory-Based Storage Devices** | |
|---|---|
| **ATA Solid State  Drives (SSDs)**  *This includes PATA, SATA, eSATA, etc.* | |
| **Clear:** | 1. Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools.  The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros.  Multiple passes or more complex values may alternatively be used.<br>Note: It is important to note that overwrite on flash-based media may significantly reduce the effective lifetime of the media and it may not sanitize the data in unmapped physical media (i.e., the old data may still remain on the media).<br>2. Use the ATA Security feature set's SECURITY ERASE UNIT command, if supported. |
| **Purge:** | Three options are available:<br>1. Apply the ATA sanitize command, if supported.  One or both of the following options may be available:<br>a. The block erase command.<br>*Optionally:*  After the block erase command is successfully applied to a device, write binary 1s across the user addressable area of the storage media and then perform a second block erase.<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, Secure Erase or 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, Secure Erase or the Clear procedure could alternatively be applied. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection.<br>When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully.  A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase. |

| | |
|---|---|
| | The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media as defined in the ATA standard, such as a Host Protected Area (HPA), Device Configuration Overlay (DCO), or Accessible Max Address. Even when a dedicated sanitization command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique. Recovery data, such as an OEM-provided restoration image may have been stored in this manner, and sanitization may therefore impact the ability to recover the system unless reinstallation media is also available.<br>Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D.<br>Given the variability in implementation of the Enhanced Secure Erase feature, use of this command is not recommended without first referring the manufacturer to identify that the storage device's model-specific implementation meets the needs of the organization.<br>Whereas ATA Secure Erase was a Purge mechanism for magnetic media, it is only a Clear mechanism for flash memory due to variability in implementation and the possibility that sensitive data may remain in areas such as spare cells that have been rotated out of use.<br>Degaussing must not be solely relied upon as a sanitization technique on flash memory-based storage devices or on hybrid devices that contain non-volatile flash memory storage media. Degaussing may be used when non-volatile flash memory media is present if the flash memory components are sanitized using media-dependent techniques. |
| **SCSI Solid State Drives (SSSDs)** *This includes Parallel SCSI, Serial Attached SCSI (SAS), Fibre Channel, USB Attached Storage (UAS), and SCSI Express.* | |
| **Clear:** | Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used.<br>Note: It is important to note that overwrite on flash-based media may significantly reduce the effective lifetime of the media and it may not sanitize the data in unmapped physical media (i.e., the old data may still remain on the media). |
| **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 service action.<br>b. If the device supports encryption, the CRYPTOGRAPHIC ERASE service action.<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. |
| **Notes:** | Verification must be performed for each technique within Clear and Purge as described in the Verify Methods subsection.<br>The storage device may support configuration capabilities that artificially restrict the ability to access portions of the media, such as SCSI mode select. Even when a dedicated sanitization |

| | |
|---|---|
| | command addresses these areas, their presence may affect the ability to reliably verify the effectiveness of the sanitization procedure if left in place. Any configuration options limiting the ability to access the entire addressable area of the storage media should be reset prior to applying the sanitization technique.<br>When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase.<br>Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance and in Appendix D.<br>Degaussing must not be performed as a sanitization technique on flash memory-based storage devices. |
| **NVM Express SSDs** | |
| **Clear:** | Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear procedure should consist of at least one pass of writes 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 NVM Express Format command, if supported. One or both of the following options may be available:<br>a. The User Data Erase command.<br>b. If the device supports encryption, the Cryptographic Erase command. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the User Data Erase command (if supported) to erase the media. If the User Data 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. *Optionally:* After Cryptographic Erase is successfully applied to a device, use the User Data Erase command (if supported) to erase the media. If the User Data 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. |
| **Notes:** | Verification must be performed for each technique within Clear and Purge.<br>When Cryptographic Erase is applied, verification must be performed prior to additional sanitization techniques (if applicable), such as a Clear or Purge technique applied following Cryptographic Erase, to ensure that the cryptographic operation completed successfully. A quick sampling verification as described in the Verify Methods subsection should also be performed after any additional techniques are applied following Cryptographic Erase.<br>Not all implementations of encryption are necessarily suitable for reliance upon Cryptographic Erase as a Purge mechanism. The decision regarding whether to use Cryptographic Erase depends upon verification of attributes previously identified in this guidance.<br>Degaussing must not be performed as a sanitization technique on flash memory-based storage devices. |
| **USB Removable Media** *This includes Pen Drives, Thumb Drives, Flash Memory Drives, Memory Sticks, etc.* | |
| **Clear:** | Overwrite media by using organizationally approved and tested overwriting |

| | |
|---|---|
| | technologies/methods/tools. The Clear pattern should be at least two passes, to include a pattern in the first pass and its complement in the second pass. Additional passes may be used. |
| **Purge:** | Most USB removable media does not support sanitize commands, or if supported, the interfaces are not supported in a standardized way across these devices. Refer to the manufacturer for details about the availability and functionality of any available sanitization features and commands. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | For most cases where Purging is desired, USB removable media should be Destroyed. |
| **Memory Cards** *This includes SD, SDHC, MMC, Compact Flash Memory, Microdrive, MemoryStick, etc.* | |
| **Clear:** | Overwrite media by using organizationally approved and tested overwriting technologies/methods/tools. The Clear pattern should be at least two passes, to include a pattern in the first pass and its complement in the second pass. Additional passes may be used. |
| **Purge:** | N/A |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | None. |
| **Embedded Flash Memory on Boards and Devices** *This includes motherboards and peripheral cards such as network adapters or any other adapter containing non-volatile flash memory.* | |
| **Clear:** | If supported by the device, reset the state to original factory settings. |
| **Purge:** | N/A If the flash memory can be easily identified and removed from the board, the flash memory may be Destroyed independently from the disposal of the board that contained the flash memory. Otherwise, the whole board should be Destroyed. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | While Embedded flash memory has traditionally not been specifically addressed in media sanitization guidelines, the increasing complexity of systems and associated use of flash memory has complementarily increased the likelihood that sensitive data may be present. For example, remote management capabilities integrated into a modern motherboard may necessitate storing IP addresses, hostnames, usernames and passwords, certificates, or other data that may be considered sensitive. As a result, for Clearing, it may be necessary to interact with multiple interfaces to fully reset the device state. When this concept is applied to the example, this might include the BIOS/UEFI interface as well as the remote management interface.<br>As with other types of media, the choice of sanitization technique is based on environment-specific considerations. While the choice might be made to neither Clear nor Purge embedded flash memory, it is important to recognize and accept the potential risk and continue to reevaluate the risk as the environment changes. |

**Table A-9: RAM- and ROM-Based Storage Device Sanitization**

| RAM and ROM-Based Storage Devices | |
|---|---|
| **Dynamic Random Access Memory (DRAM)** | |
| **Clear/ Purge:** | Power off device containing DRAM, remove from the power source, and remove the battery (if battery backed). Alternatively, remove the DRAM from the device. |
| **Destroy:** | Shred, Disintegrate, or Pulverize. |
| **Notes:** | In either case, the DRAM must remain without power for a period of at least five minutes. |
| **Electronically Alterable PROM (EAPROM)** | |
| **Clear/ Purge:** | Perform a full chip Purge as per manufacturer's data sheets. |
| **Destroy:** | Shred, Disintegrate, or Pulverize. |
| **Notes:** | None. |
| **Electronically Erasable PROM (EEPROM)** | |
| **Clear/ Purge:** | Overwrite media by using organizationally approved and validated overwriting technologies/methods/tools. |
| **Destroy:** | Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator. |
| **Notes:** | None. |