

# Guidelines for Media Sanitization

*Recommendations of the National  
Institute of Standards and Technology*  
NIST Special Publication 800-88

Method	Description
Clear	<p>One method to sanitize media is to use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not rewriteable. The media type and size may also influence whether overwriting is a suitable sanitization method [SP 800-36].</p>
Purge	<p>Degaussing and executing the firmware Secure Erase command (for ATA drives only) are acceptable methods for purging.</p> <p>Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged or inoperative media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. [SP 800-36]</p>
Destroy	<p>There are many different types, techniques, and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, then after the destruction, the media should be able to withstand a laboratory attack.</p> <p><i>Disintegration, Pulverization, Melting, and Incineration.</i> These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.</p> <p><i>Shredding.</i> Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed.</p> <p>Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and MO disks, must be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues must be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm<sup>2</sup>).</p>

Once a decision is made (see section 4) and after applying relevant organizational environmental factors, then Table A-1 can be used to determine recommended sanitization of specific media. This recommendation should reflect the Federal Information Processing Standard (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 Table A-1 is recommended here, other methods exist to satisfy the intent of clear, purge (still relevant in some cases), and destroy, and methods not specified in this table may be suitable as long as they are vetted 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 validated, they are strongly encouraged to share this information through public forums, such as the Federal Agency Security Practices (FASP) website. 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. FASP can be found at <http://csrc.nist.gov/fasp/>.

**Table A-1. Media Sanitization Decision Matrix**

Media Type	Clear	Purge	Physical Destruction
<b>Hard Copy Storages</b>			
Paper and microforms	See Physical Destruction.	See Physical Destruction.	<p>Destroy paper using cross cut shredders which produce particles that are 1 x 5 millimeters in size (reference devices on the NSA paper Shredder EPL), or to pulverize/disintegrate paper materials using disintegrator devices equipped with 3/32 inch security screen (reference NSA Disintegrator EPL.).</p> <p>Destroy microforms (microfilm, microfiche, or other reduced image photo negatives) by burning. When material is burned, residue must be reduced to white ash.</p>
<b>Hand-Held Devices</b>			

Cell Phones	Manually delete all information, such as calls made, phone numbers, then perform a full manufacturer's reset to reset the cell phone back to its factory default settings.  ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	Shred.  Disintegrate.  Pulverize.  Incinerate by burning cell phones in a licensed incinerator.
Personal Digital Assistant (PDA) (Palm, PocketPC, other)	Manually delete all information, then perform a manufacturer's hard reset to reset the PDA to factory state.  ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	Incinerate PDAs by burning the PDAs in a licensed incinerator.  Shred.  Pulverize.

#### Networking Devices

Routers (home, home office, enterprise)	Perform a full manufacturer's reset to reset the router back to its factory default settings.  ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	Shred.  Disintegrate.  Pulverize.  Incinerate. Incinerate routers by burning the routers in a licensed incinerator.
---	--	----------------	--

#### Equipment

Copy Machines	Perform a full manufacturer's reset to reset the copy machine to its factory default settings.  ** Please contact the manufacturer for proper sanitization procedure.	Same as Clear.	Shred.  Disintegrate.  Pulverize.  Incinerate. Incinerate copy machines by burning the copy machines in a licensed incinerator.
Fax Machines	Perform a full manufacturer's reset to reset the fax machine to its factory default settings.  ** Please contact the manufacturer for proper sanitization procedures.	Same as Clear.	Shred.  Disintegrate.  Pulverize.  Incinerate. Incinerate fax machines by burning the fax machines in a licensed

			incinerator.
<b>Magnetic Disks</b>			
Floppies	Overwrite media by using agency-approved software and validate the overwritten data.	Degauss in a NSA/CSS-approved degausser.	<p>Incinerate floppy disks and diskettes by burning the floppy disks and diskettes in a licensed incinerator.</p> <p>Shred.</p>
ATA Hard Drives	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	<ol style="list-style-type: none"> <li>1. Purge using Secure Erase. The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site.</li> <li>2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.**</li> <li>3. Purge media by using agency-approved and validated purge technologies/tools.</li> </ol> <p>**Degaussing any current generation hard disk will render the drive permanently unusable.</p>	<p>Disintegrate.</p> <p>Shred.</p> <p>Pulverize.</p> <p>Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.</p>

<p>USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) with Hard Drives</p>	<p>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</p>	<ol style="list-style-type: none"> <li>1. Purge using Secure Erase The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site.</li> <li>2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.**</li> <li>3. Purge media by using agency-approved and validated purge technologies/tools.</li> </ol> <p>**Degaussing any current generation hard disk will render the drive permanently unusable.</p>	<p>Disintegrate.</p> <p>Shred.</p> <p>Pulverize.</p> <p>Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.</p>
<p>Zip Disks</p>	<p>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</p>	<p>Degauss using a NSA/CSS-approved degausser.</p> <p>**Degaussing any current generation zip disks will render the disk permanently unusable.</p>	<p>Incinerate disks and diskettes by burning the zip disks in a licensed incinerator.</p> <p>Shred.</p>

SCSI Drives	<p>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</p>	<p>Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.</p> <p>***Degaussing any current generation hard disk will render the drive permanently unusable.</p>	<p>Disintegrate.</p> <p>Shred.</p> <p>Pulverize.</p> <p>Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.</p>
-------------	---	--	--

**Magnetic Tapes**

<p>Reel and Cassette Format Magnetic Tapes</p>	<p>Clear magnetic tapes by either re-recording (overwriting) or degaussing. 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.</p> <p>Clearing by Overwriting: Overwriting should be performed on a system similar to the one that originally recorded the data. For example, overwrite previously recorded classified or 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.</p>	<p>Degauss using an NSA/CSS-approved degausser.</p> <p>Purging by Degaussing: Purge the magnetic tape in any degausser that can purge the signal enough to prohibit playback of the previous known signal. Purging by degaussing can be accomplished easier by using an NSA/CSS-approved degausser for the magnetic tape.</p>	<p>Incinerate by burning the tapes in a licensed incinerator.</p> <p>Shred.</p> <p>Preparatory steps, 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.</p>
--	---	---	---

**Optical Disks**

CDs	See Physical Destruction.	See Physical Destruction.	<p>Destroy in order of recommendations:</p> <p>Removing the Information bearing layers of CD media using a commercial optical disk grinding device.</p> <p>Incinerate optical disk media (reduce to ash) using a licensed facility.</p> <p>Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm<sup>2</sup>). **</p> <p>** This is a current acceptable particle size. Any future disk media shredders obtained should reduce CD to surface area of .25mm<sup>2</sup>.</p>
-----	---------------------------	---------------------------	---

DVDs	See Physical Destruction.	See Physical Destruction.	<p>Destroy in order of recommendations:</p> <p>Removing the Information bearing layers of DVD media using a commercial optical disk grinding device.</p> <p>Incinerate optical disk media (reduce to ash) using a licensed facility.</p> <p>Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm<sup>2</sup>). **</p> <p>** This is a current acceptable particle size. Any future disk media shredders obtained should reduce DVD to surface area of .25mm.</p>
------	---------------------------	---------------------------	---

**Memory**

Compact Flash Drives, SD	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	See Physical Destruction.	<p>Destroy media in order of recommendations.</p> <p>Shred.</p> <p>Disintegrate.</p> <p>Pulverize.</p> <p>Incinerate by burning in a licensed incinerator.</p>
Dynamic Random Access Memory (DRAM)	Purge DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	<p>Shred.</p> <p>Disintegrate.</p> <p>Pulverize.</p>
Electronically Alterable PROM (EAPROM)	Perform a full chip purge as per manufacturer's data sheets.	Same as Clear.	<p>Shred</p> <p>Disintegrate</p> <p>Pulverize</p>

Electronically Erasable PROM (EEPROM)	<p>Overwrite media by using agency approved and validated overwriting technologies/methods/tools.</p> <p>Remove all labels or markings that indicate previous use or confidentiality.</p>	Same as Clear.	<p>Shred.</p> <p>Disintegrate.</p> <p>Pulverize.</p> <p>Incinerate by burning in a licensed incinerator.</p>
---------------------------------------	---	----------------	--

Media Type	Clear	Purge	Destroy
Erasable Programmable ROM (EPROM)	<p>Clear media in order of recommendations.</p> <ol style="list-style-type: none"> <li>Clear functioning EPROM by performing an ultraviolet purge according to the manufacturer's recommendations, but increase the time requirement by a factor of 3.</li> <li>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</li> </ol>	Same as Clear.	<p>Shred.</p> <p>Disintegrate.</p> <p>Pulverize.</p> <p>Incinerate by burning in a licensed incinerator.</p>
Field Programmable Gate Array (FPGA) Devices (Non-Volatile)	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	Same as Clear.	<p>Shred.</p> <p>Disintegrate.</p> <p>Pulverize.</p>
Field Programmable Gate Array (FPGA) Devices (Volatile)	Clear functioning FPGA by powering off and removing the battery (if battery backed).	Same as Clear.	<p>Shred.</p> <p>Disintegrate.</p> <p>Pulverize.</p>
Flash Cards	Overwrite media by using agency approved and validated overwriting technologies/methods/tools.	Same as Clear.	<p>Shred.</p> <p>Disintegrate.</p> <p>Pulverize.</p>

Flash EPROM (FEPROM)	Perform a full chip purge as per manufacturer's data sheets.	Purge media in order of recommendations. 1. Overwrite media by using agency approved and validated overwriting technologies/methods/tools. 2. Perform a full chip purge as per manufacturer's data sheets.	Shred. Disintegrate. Pulverize. Incinerate by burning in a licensed incinerator.
----------------------	--	--	---

<p>Magnetic Bubble Memory</p>	<p>Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</p>	<p>Purge by Collapsing the Magnetic Bubbles:</p> <ol style="list-style-type: none"><li>1. Degaussing: Degauss in an NSA/CSS-approved degausser. However, care must be taken to insure that the full field (at least 1500 gauss) of the degausser is applied to the actual bubble array. All shielding materials must be removed from the circuit card and/or bubble memory device before degaussing.</li><li>2. Raising the Magnetic Bias Field: Magnetic bubble memory with built-in magnetic bias field controls may be purged by raising the bias voltage to levels sufficient to collapse the magnetic bubbles. Recommend that specific technical guidance be obtained from the bubble memory manufacturer before attempting this procedure.</li></ol>	<p>Shred.</p> <p>Disintegrate.</p> <p>Pulverize.</p> <p>When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance of the destruction device.</p>
---------------------------------------	---	--	--

Magnetic Core Memory	<p>Clear media in order of recommendations.</p> <ol style="list-style-type: none"> <li>1. Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.</li> <li>2. Degauss in an NSA/CSS-approved degausser.</li> </ol>	<p>Purge core memory devices either by overwriting or degaussing.</p> <p style="padding-left: 40px;">Overwrite media by using agency approved and validated overwriting technologies/methods/ tools</p> <p style="padding-left: 40px;">Degauss in an NSA/CSS-approved degausser. Remove all labels or markings that indicate previous use or confidentiality. NOTE - Attenuation of the magnetic field due to chassis shielding and separation distance are factors that affect erasure performance and should be considered. All steel shielding materials (e.g., chassis, case, or mounting brackets) should be removed before degaussing.</p>	<p style="text-align: center;">Shred.</p> <p>Disintegrate.</p> <p>Pulverize.</p> <p>When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance.</p>
Non Volatile RAM (NOVRAM)	<ol style="list-style-type: none"> <li>1. Overwrite media by using agency approved and validated overwriting technologies/methods/tools.</li> <li>2. Each overwrite must reside in memory for a period longer than the data resided.</li> <li>3. Remove all power to include battery power.</li> </ol>	Same as Clear.	<p style="text-align: center;">Shred.</p> <p>Disintegrate.</p> <p>Pulverize.</p>
PC Cards or Personal Computer Memory Card International Association (PCMCIA) Cards	See Physical Destruction.	See Physical Destruction.	Destroy by incinerating in a licensed incinerator or use (an NSA evaluated) a disintegrator to reduce the card's internal circuit board and components to particles that are nominally two (2) millimeters in size.
Programmable ROM (PROM)	See Physical Destruction.	See Physical Destruction.	Destroy by incinerating in a licensed incinerator.

RAM	Purge functioning DRAM by powering off and removing the battery (if battery backed).	Same as Clear.	Shred. Disintegrate. Pulverize.
ROM	See Physical Destruction.	See Physical Destruction.	Shred. Disintegrate. Pulverize.
USB Removable Media (Pen Drives, Thumb Drives, Flash Drives, Memory Sticks) without Hard Drives	Overwrite media by using agency approved and validated overwriting technologies/methods/tools	Same as Clear.	Shred. Disintegrate. Pulverize.
Smart Cards	See Physical Destruction.	See Physical Destruction.	For smart card devices& data storage tokens that are in credit card form, cut or crush the smart card's internal memory chip using metals snips, a pair of scissors, or a strip cut shredder (nominal 2 mm wide cuts). Smart cards packaged into tokens (i.e. SIM chips, thumb drives and other physically robust plastic packages) that are not capable of being shredded should instead be destroyed via incineration licensed incinerator or disintegration to 2 mm size particles.

<b>Magnetic Cards</b>			
Magnetic Cards	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools	Degauss in an NSA/CSS-approved degausser.	Shred.  Incinerate. Incineration of magnetic cards shall be accomplished by burning the magnetic cards in a licensed incinerator.

<b>Glossary Term</b>	<b>Definition</b>
Clear	To use software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. See comments on clear/purge convergence.
CD	Compact Disc: a class of media on which data are recorded by optical means.
CD-RW	Compact Disc Read/Write: A CD that can be purged and rewritten multiple times.
CD-R	Compact Disc Recordable: A CD that can be written on only once but read many times. Also known as WORM.
CMRR	The Center for Magnetic Recording Research (CMRR) advances the state-of-the-art in magnetic storage, and trains graduate students and postdoctoral professionals. The Center is located at the University of California, San Diego.
Data	Pieces of information from which “understandable information” is derived.

Degauss	To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing. Degaussing any current generation hard disk (including but not limited to IDE, EIDE, ATA, SCSI and Jaz) will render the drive permanently unusable since these drives store track location information on the hard drive in dedicated regions of the drive in between the data sectors.
Destruction	The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive.
Digital	The binary coding scheme generally used in computer technology to represent data as binary bits (1s and 0s).
Disintegration	A physically destructive method of sanitizing media; the act of separating into component parts.
Disposal	Disposal is the act of discarding media with no other sanitization considerations. This is most often done by paper recycling containing non-confidential information but may also include other media.
DVD	Digital Video Disc – a disc the same shape and size as a CD; but the DVD has a higher density and gives the option for data to be double-sided or double-layered.
DVD-RW	A rewritable (re-recordable) DVD disk for both movies and data from the DVD Forum.
DVD+RW	A rewritable (re-recordable) DVD disk for both movies and data from the DVD+RW Alliance.
DVD+R	A write-once (read only) version of the DVD+RW optical disk from the DVD+RW Alliance.
DVD-R	A write-once (read only) DVD disk for both movies and data endorsed by the DVD Forum.
Electronic Media	General term that refers to media on which data are recorded via an electrically based process.
Erase	Process intended to render magnetically stored information irretrievable by normal means.
FIPS	Federal Information Processing Standard.
Format	Pre-established layout for data.
Hard Disk	A rigid magnetic disk fixed permanently within a drive unit and used for storing data.
Incineration	A physically destructive method of sanitizing media; the act of burning completely to ashes.
Information	Meaningful interpretation or expression of data.
Media	Plural of medium.
Media Sanitization	A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.
Medium	Material on which data are or may be recorded, such as paper, punched cards, magnetic tape, magnetic disks, solid state devices, or optical discs.
Melting	A physically destructive method of sanitizing media; to be changed from a solid to a liquid state generally by the application

	of heat.
Optical Disks	A plastic disk that is “written” (encoded) and “read” using an optical laser device. The disc contains a highly reflective metal and uses bits to represent data by containing areas that reduce the effect of reflection when illuminated with a narrow-beam source, such as a laser diode.
Overwrite	Writing patterns of data on top of the data stored on a magnetic medium. NSA has researched that one overwrite is good enough to sanitize most drives. See comments on clear/purge convergence.
Physical Destruction	A sanitization method for optical media, such as CDs.
Pulverization	A physically destructive method of sanitizing media; the act of grinding to a powder or dust.
Purge	Rendering sanitized data unrecoverable by laboratory attack methods. See comments on clear/purge convergence.
Read	Fundamental process in an information system that results only in the flow of information from an object to a subject.
Record	To write data on a medium, such as a magnetic tape, magnetic disk, or optical disc.
Recovery Procedures (recoverable)	Action necessary to store data files of an information system and computational capability after a system failure.
Remanence	Residual information remaining on storage media after clearing.
Residue	Data left in storage after information processing operations are complete, but before degaussing or overwriting has taken place.
ROM	Read Only Memory. Generally a commercially available disc or solid state device on which the content was recorded during the manufacturing process.
Sanitize	Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
Secure Erase	<p>An overwrite technology using firmware based process to overwrite a hard drive. Is a drive command defined in the ANSI ATA and SCSI disk drive interface specifications, which runs inside drive hardware. It completes in about 1/8 the time of 5220 block erasure. It</p> <p>Was added to the ATA specification in part at CMRR request. For ATA drives manufactured after 2001 (Over 15 GB) have the Secure Erase command and successfully pass secure erase validation testing at CMRR. A standardized internal secure erase command also exists for SCSI drives, but it is optional and not currently implemented in SCSI drives tested by CMRR. SCSI drives are a small percentage of the world’s hard disk drives, and the command will be implemented when users demand it.</p>
Shred	A method of sanitizing media; the act of cutting or tearing into small particles.
Storage	Retrievable retention of data. Electronic, electrostatic, or electrical hardware or other elements (media) into which data

	may be entered, and from which data may be retrieved.
WORM	Write-Once Read Many.
Write	Fundamental operations of an information system that results only in the flow of information from a subject to an object.

**This Page Intentionally Left Blank**

Many different government, U.S. military, and academic institutions have conducted extensive research in sanitization tools, techniques, and procedures in order to validate them to a certain level of assurance. The National Institute of Standards and Technology (NIST) does not conduct an evaluation of any tool set to validate its ability to clear, purge, or destroy information contained on any specific medium.

Organizations are encouraged to seek products that they can evaluate on their own. They can use a trusted service or other federal organizations' evaluation of tools and products and they are expected to continually monitor and validate the effectiveness of their selected sanitization tools as they are used.

If an organization has a product that they trust and have validated, then they are strongly encouraged to share this information through public forums, such as the Federal Agency Security Practices (FASP) website. 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. FASP can be found at <http://csrc.nist.gov/fasp/>.

This guide also recommends that the user consider the NSA devices posted on the public NSA website. NSA states "The products on these lists have met NSA specific performance requirements; however, inclusion on the list does not constitute an endorsement by NSA or the U.S. government.

[NSA/CSS-EPL-02-01-M](#) - NSA/CSS Evaluated Products List (EPL) for High Security Crosscut Paper Shredders, Annex A to NSA/CSS 02-01, version M, dated: April 2005 [NSA/CSS-EPL-02-02-F](#) - NSA Evaluated High-Security Disintegrators, Annex A to NSA/CSS 02-02, version F, dated: April 2005 [NSA/CSS EPL 04-02-B](#) - Optical Media Destruction Devices, Annex A to NSA/CSS 04-02, version B, Date: 30 September 2005

[NSA/CSS-EPL-9-12A-B](#) - Degausser Approved Products List - Annex A to NSA/CSS Manual 130-2, version B, dated: May 2005"

In addition to the NSA device listing, the Defense Security Service (DSS) publishes an Assessed Product List (APL), which is a listing of products assessed against the vendors claims of sanitation. The DSS APL states, "The APL does not endorse any company's

product, nor does it constitute certification or accreditation for the product's use in a classified environment. The intent is to give security personnel information on the capability of the product, whereby, they can determine the possible application of the product to meet their security requirement.”<sup>5</sup>

This listing can be found at [http://www.dss.mil/infoas/assessed\\_products\\_list.doc](http://www.dss.mil/infoas/assessed_products_list.doc) .

For hard drive devices or devices where firmware purge commands can be accessed and utilized, this may be the best option for an organization. Firmware purge commands can provide strong assurance of data protection while allowing the device to be reused. More information on firmware secure erasure for ATA hard drives can be found at <http://cmrr.ucsd.edu/hughes/subpgset.htm> .

Organizations and individuals wishing to donate used electronic equipment or seeking guidance on disposal of residual materials after sanitization should consult the Environmental Protection Agencies (EPA) electronic recycling and electronic waste information website at <http://www.epa.gov/e-Cycling/> . This site offers advice, regulations, and standard publications related to sanitization, disposal, and donations. It also provides external links to other sanitization tool resources.

Organizations can outsource media sanitization and destruction if business and security management decide that this would be the most reasonable option for them to maintain confidentiality while optimizing available resources. When exercising this option, this guide recommends that organizations exercise “due diligence” when entering into a contract with another party engaged in media sanitization. Due diligence for this case is accepted as outlined in 16 CFR 682 which states “due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule [guide], obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.”<sup>6</sup>

For home users and telecommuters needing to sanitize media, media sanitization methods developed for organizations might be impractical or unsafe. Telecommuters should check their organizational policies before attempting any type of sanitization. Here are a few guidelines that home users and telecommuters could follow:

If you are a telecommuter, ensure that you follow your organizations sanitization policies and instructions first. Organization policies and procedures take precedent over these instructions.

Check your provided instruction manual. If guidance for information sanitization for the system is provided, follow those instructions. Instruction manual sanitization guidance takes precedent over these instructions.

If you are unsure, unclear or cannot conduct sanitization in a safe manner with suitable assurance that your information has been sanitized, take the system to a professional either through your organization or with an outside vendor.

Be sure you are ready to dispose of your media. **Have backup copies made of all your information to keep in a secure place in case you ever need to refer to your data.**

When you are ready to dispose of the system, ensure you follow all disposal instructions. Many media contain hazardous material.

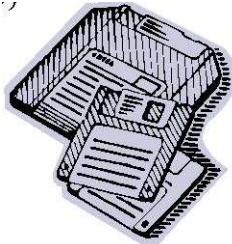
**Decide:** If you require sanitization for the media under consideration. Is this just a cell phone with public numbers stored in the phone book or is it your home PC with tax preparations, bank account information, and investment records?

**First:** Ensure that all power sources are disconnected, unplugged, or removed.

**If:** You have a cell phone, PDA, or other form of mobile computing device,

**Then:** Manually delete all information. Then see your instruction manual for how to conduct a factory hard reset. Ensure that any removable storage media are removed from the device.

**If:** You have removable mass storage media, including (but not limited to) compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), Compact Flash, Memory Sticks, Secure Digital, Jump Drives and magneto-optic disks (MO),



**Then:** These media should be destroyed by shredding, physically breaking, or rendering the media physically unable to be reinserted into the device to read the media.

**If:** You have a PC,

**Then:** You can conduct sanitization through the following two methods.

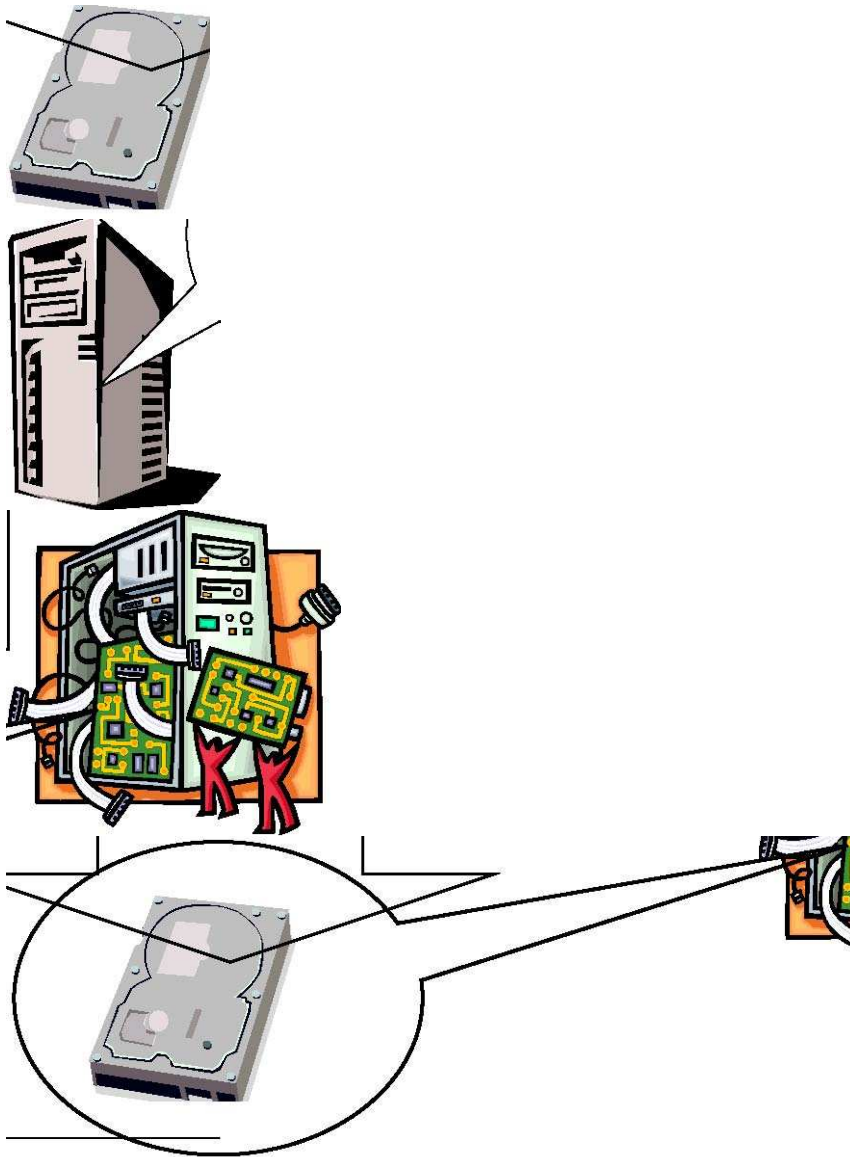
1. Use software to conduct sanitization. Check with your PC maker for a recommended tool and check testimonies of sanitization tools in industry and computing magazines. These resources can be found in hard copy in your local library and online. Conducting online searches for 'Sanitization Tools' and 'Disk Drive Sanitization' will yield multiple sources for research into tools for sanitization. Users can also check the NIST Federal Agency Security Practices (FASP) website at <http://csrc.nist.gov/fasp/> to see what tools and procedures some federal agencies are using for sanitization.
2. Physically impair your disk drive to prevent information recovery from a keyboard attack. In order to conduct this, ensure all power sources are disconnected. Locate computer hard drive. Use your provided instruction manual and/or provided schematic to locate. Remove hard drive from PC.

Remove any steel shielding materials, mounting brackets, and cut any electrical connection to the hard drive unit.

The hard drive should then be subjected, in a suitable facility with individuals wearing appropriate safety equipment, to physical force... (e.g., pounding with a

hammer...) that will disfigure, bend, mangle, or otherwise mutilate the hard drive so that it cannot be reinserted into a functioning computer. Sufficient force should be used directly on top of the hard drive unit to cause shock/damage to the disk surfaces. In addition, any connectors that interface into the computer must be mangled, bent, or otherwise damaged to the point that the hard drive could not be reconnected without significant rework. [7]

Some schematics located on inside of chassis.



All About Degausser and Erasure of Magnetic Media. Athana International. 20 June 2005

Anastasi, Joe. The New Forensics: Investigating Corporate Fraud and the Theft of Intellectual Property. N.p.: John Wiley and Sons, 2003. 1-288.

Army Regulation 25-2. U.S Army. ELECTRONIC PUBLISHING SYSTEM, 17 Nov 2003.

D.Millar, "Clean Out Old Computers Before Selling/Donating," June 1997;

Davis, Harvey A. National Security Agency. NSA/CSS POLICY MANUAL 9-12. N.p.: n.p., 2000.

"Degaussing Described." Weircliffe International Ltd in the interests of magnetic media users and others who are affected by the phenomena of Ferro-magnetism (2005).

Dictionary definition of **EPROM** The American Heritage® Dictionary of the English Language, Fourth Edition Copyright © 2004, 2000 by [Houghton Mifflin Company](#) . Published by Houghton Mifflin Company.

"Future of Computing (Optical & Biological Possibilities)." Future of Computing. 04 June 1997. Dept. of Engineering, Imperial College London. 10 Nov. 2005

Garfinkel, Simson L., and Abhi Shelat. "Remembrance of Data Passed: A Study of Disk Sanitization Practices." IEEE Security & Privacy 1st ser. 1 (2003). 09 June 2005

Gutmann, Peter, ed. Secure Deletion of Data from Magnetic and Solid-State Memory. San Jose: Sixth USENIX Security Symposium Proceedings, 1996.

Gutmann, Peter, ed. Data Remanence in Semiconductor Devices. Washington, D.C: 10th USENIX SECURITY SYMPOSIUM, 2001.

J.Hasson, "V.A. Toughens Security after PC Disposal Blunders," *Federal Computer Week*, 26 Aug. 2002;

LeaseForum. "Understanding Data Storage, Data Liability and Current Data Removal Methodologies." Addressing Data at Asset Retirement. N.p.: n.p. 2002. 1-8.

Magnetoresistive Random Access Memory (MRAM). Comp. James Daughton. 4 Feb. 2000. NVE. 17 June 2005

Microsoft, "Microsoft Extensible Firmware Initiative FAT32 File System Specification," 6 Dec. 2000;

National Computer Security Center, "A Guide to Understanding Data Remanence in Automated Information Systems,"

Understand Degaussing. Peripheral Manufacturing Inc. 18 June 2005.

US Department of Defense, "Cleaning and Sanitization Matrix," DOS 5220.22-M, Washington, D.C., 1995.

**Organization:** \_\_\_\_\_

**Item Description:** \_\_\_\_\_

**Make/Model:** \_\_\_\_\_

**Serial Number(s)/Property Number(s):** \_\_\_\_\_

\_\_\_\_\_

**Backup Made of Information:** Yes

No

**If Yes, Backup Location:** \_\_\_\_\_

**Item Disposition:** Clear **Date Conducted:** \_\_\_\_\_

Purge **Conducted By:** \_\_\_\_\_

Destroy **Phone #:** \_\_\_\_\_

**Validated By:** \_\_\_\_\_

**Phone #:** \_\_\_\_\_

**Sanitization Method Used:** \_\_\_\_\_

**Final Disposition of Media:** Disposed

Reused Internally

Reused Externally

Returned to Manufacturer

Other: \_\_\_\_\_