



# Federal Electronics Challenge

## Sanitization of Computers and Electronic Storage Media A.K.A. - Disk Sanitization

Mike Caltabiano  
Environmental Protection Agency,  
Office of Environmental Information,  
Office of Technology Operations and Planning,  
Desktop and Collaborations Solutions Branch



*Office of Technology Operations and Planning*

# Sanitization of Computers

- A large volume of electronic information is stored on computer hard disk and electronic media throughout the Environmental Protection Agency (EPA). Much of this information is sensitive to disclosure due to its confidentiality.
- Most of the software at EPA is licensed under special agreements which prohibit the transfer of this software outside of the Agency.
- All information and licensed software must be properly removed when disposing of computer systems with a hard drive.
- This is also applicable to all other electronic storage media including, Personal Digital Assistance (PDAs), Blackberries, removable media such as CDs, DVDs, Universal Serial Bus (USB drives), Zip drive media, Jaz drives, backup disks, diskettes and tapes.



# Purpose for Sanitization?

- Unauthorized disclosure of certain information may subject the Agency to legal liability, negative publicity, monetary penalties, and the possible loss of funding. This procedure is designed to ensure that IT resources do not contain information of a confidential nature before being transferred outside of any US Environmental Protection Agency facility or region, for surplus or destruction. IT resources and electronic storage media will be cleaned of all information.



# Background for Sanitization.

- Studies of disk sanitization indicate that simply deleting files from the media or formatting a hard drive is not sufficient to completely erase data so that it cannot be recovered.
- When you delete files in Windows by moving them into the Recycle Bin all data remains on the hard disk.
- Read more about disk sanitization practices in an article written by Simson L. Garfinkel and Abhi Shelat from the Massachusetts Institute of Technology.  
[http://www.hddrecovery.com.au/HDD\\_Press\\_2.htm](http://www.hddrecovery.com.au/HDD_Press_2.htm)



# Procedures

- Overwriting hard drives and electronic storage media utilizing Department of Defense (DOD) accepted software. Overwriting of data means replacing previously stored data on a drive or disk with a predetermined pattern of meaningless information, effectively rendering the data unrecoverable. ***After overwriting, the hard drive is still physically functional and can accept formatting.***

There are several algorithms of overwriting:

- **Single Pass** – data area is overwritten once with “1” or “0”.
- **DoD Method** – the data area is overwritten with 0’s, then 1’s and then once with pseudo random data.
- **NSA erasure algorithm** – data is overwritten seven times with “0” pattern then with “1” and so on. It is the best method for quick and secure deletion.
- **Guttman Method** – the data area is overwritten 35 times. This method overwrites the drive taking into account the different encoding algorithms used by various hard drive manufacturers.



# Procedures continued

- Physically destroying (See Definitions) the storage media, rendering it unusable. Hard drives should be destroyed when protection can't be reliably ensured; the technology is old or can not be handled by the available tools. ***Physical destruction must be accomplished to an extent that precludes any possible further use of the hard drive or storage media.*** We recommend physical destruction be performed by a “Hard Drive Destruction Service”.

**Performed by a shredding service.**



# Procedures continued

- Degaussing (See Definitions) a hard drive or storage media to randomize the magnetic domains – most likely rendering the drive or media unusable in the process. If they are defective or cannot be economically repaired or sanitized for reuse by the available tools, then the media will be degaussed and discarded. **This option should not be used for any system containing a hard drive or electronic storage media that has information with concern for confidentiality.**
- For destruction of a CD/DVD, the most economical form of destruction is a ***CD/DVD shredder***.
- Zip drive media, flash/USB drives should be physically destroyed if these devices cannot be sanitized via the DOD accepted overwriting software.
- If necessary, destruction of electronic storage media can include CELL Phones, PDA's and Blackberries. Depending of the level of information that was stored on the device.
- ***Note: Drives with Classified or higher security data should be destroyed.***



# Overwriting for Sanitization

## Wipe Tools:

- **WipeDrive 3.0** [www.whitecanyon.com](http://www.whitecanyon.com)
  - Windows Platform – DOD approved. Erases files, folders, cookies, or an entire drive.
- **CyberScrub** [www.cyberscrub.com](http://www.cyberscrub.com)
  - Windows Platform – DOD approved. Erases files, folders, cookies, or an entire drive. Implements Gutmann patterns.
- **DataScrubber** [www.datadev.com/ds100.html](http://www.datadev.com/ds100.html)
  - Windows, Unix Platforms – DOD Approved. Handles SCSI remapping and swap area. Claims to be developed in collaboration with the US Air Force Information Welfare Center.
- **Eraser** [www.heidi.ie/eraser](http://www.heidi.ie/eraser)
  - Windows Platform – Freeware- erases entire drive Unknown if DOD approved.

A more comprehensive list of sanitation tools is available at [www.SDEAN12.org](http://www.SDEAN12.org).



# Sanitization Equipment

EPA recommends but does not endorse the following products:

## Degaussing Tools:

- HD-1 All Media Degausser  
The HD-1 erases virtually all formats of tape, diskettes and hard-disks up to 160 GB. Please note; hard drives are not reusable once degaussed.
- Model 8000 Hard Drive/Media Degausser  
The Model 8000 Table Top unit is a low noise, compact unit with “industrial strength” flux fields and features a foot-control for hands-free operation.

## Tools used for CD/DVD shredding:

- PRIMERA Disc Shredder – DS360
- Aleratec DVD/CD Shredder Plus XC
- Kobra 240 SS4
- HSM Model 125.2 Shredder
- Intimus 502CD CD Shredder
- Olympia 1500 CD Shredder



# Definitions

**Sanitization, sanitized** – is the end result after all data is obliterated. Including all associated file system structures, operating system formatting and information from fixed disk or electronic storage media.

**Physical destruction** – destroying the item by physical force. For example, removing the hard drive from a computer and strike it with a large device to break it and the platters to small pieces. The best process is Disk Drive Shredding.

**Degaussing** is a process whereby the magnetic media are erased, (i.e., returned to a zero state). Degaussing (demagnetizing) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable by keyboard or laboratory attack. A degausser is an electro-magnetic device used for this purpose.

**Sensitive data** – includes; Confidential Business Information (CBI), research information, procurement information, contract information, contract awards, incentive awards, personnel data, OIG related information, human resource information (SSN, etc), privacy act information and any other information that should not be released to the public.



# Waivers for Sanitization

**Waivers**

**will**

**not**

**be**

**considered!**





# Sanitization of Computers and Electronic Storage Media

## Practices at EPA

- Sanitization Policy in development
  - Recommend the DOD approved overwrite method for all non-classified PC hard drives
  - OEI/Office of the CIO uses Wipe Drive prior to reuse or recycling the PC.

**NOTE: Anything categorized as National Security Information Systems is not covered by this procedure.**

