MEDIA SANITIZATION OF USED ELECTRONICS

Federal Electronics Challenge Partner Call
Robin Billings, U.S. Environmental Protection Agency Region 4
August 2, 2012
DISCLAIMER

• The information in this presentation **does not** supersede any federal agency’s policies, procedures, guidance, or requirements with respect to media sanitization and data security

• Federal agencies and facilities should discuss these and other data security issues with their facility/property management, and information technology and security experts

• The information in this presentation **is not** exhaustive guidance on media sanitization and data security

• Federal agencies and facilities should reference the National Institute of Standards and Technology (NIST) Guidelines for Media Sanitization (NIST Special Publication 800-88) for comprehensive information on media sanitization options
Media sanitization is a method for ensuring data security of information stored on media.

**Media sanitization**
Actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

**Data security**
Preventing the unauthorized disclosure of information and ensuring confidentiality.
Media Sanitization and Electronics Stewardship

- Media store data
- Sanitization prevents unauthorized disclosure of information and ensures confidentiality
  - allows for reuse
  - secures for recycling
- Media sanitization practices may impact electronics stewardship activities, particularly reuse and recycling
- Executive Order 13423 and 13514 require reuse and donation of electronic equipment
- Select the least destructive media sanitization method, which still meets security and confidentiality needs
# Sources of Media

<table>
<thead>
<tr>
<th>Media:</th>
<th>Where you might find it:</th>
</tr>
</thead>
</table>
| Paper or microforms                             | • Imaging equipment, including printers, copiers, scanners, facsimile machines and multifunction devices (MFDs)  
|                                                  | • Microfiche readers and microfilming machines                                           |
| Hard drives                                      | • Computer desktops and laptops                                                         |
| Memory                                           | • Some imaging equipment                                                               |
| Removable electronic media (Floppies, CDs, DVDs, USB removable media, Zip disks, removable memory cards) | • As separate components  
|                                                  | • Within many electronics                                                              |
| Magnetic cassettes, cards, tapes and ribbon      | • Audio and visual (AV) equipment                                                      |
|                                                  | • Tape recorders and players                                                            |
Options for Media Sanitization

1. **Disposal**: discarding media with no further sanitization actions
2. **Clearing**: removing data from media so that the data can not be retrieved through a robust keyboard attack
   - *example*: overwriting
3. **Purging**: removing data from media so that the data can not be retrieved through a laboratory attack
   - *example*: degaussing
4. **Destroying**: rendering the media unable to be reused as originally intended; residual medium may need to be able to withstand a laboratory attack
   - *example*: shredding
Considerations for Media Sanitization

- Type of media (i.e., optical, magnetic, or paper/film)
- Size of media
- Confidentiality and necessary security of the data on the media
- Cost of sanitization tools and staff, and available budget
- Availability of sanitization tools and staff
- Training and certification of staff
- Length of time available for sanitization
NIST Flowchart

Security Categorization
- Low
  - Leaving Org Control? Yes: Purge
    - Clear
  - No: Document

- Moderate
  - Leaving Org Control? Yes: Purge
  - Reuse Media? Yes: Destroy
  - No: Document

- High
  - Leaving Org Control? Yes: Destroy
    - Reuse Media? No: Document
Options After Sanitization

- Consider the impact of your media sanitization methods.
- Media with low or moderate security classification may be sanitized and preserved for reuse.
- Recycling facilities may be able to recover plastics and metals from destroyed media.
  - Media that is sanitized through abrasive scraping, shredding, disintegrating or pulverizing may be able to be recycled.
  - Media sanitized through chemical destruction may not be able to be recycled and may require special handling for disposal.
- If media must be incinerated, look for a facility that practices energy recovery.
- Use of some contracting vehicles may require special media sanitization considerations.
Contact and Resources

- Robin Billings, U.S. EPA Region 4
  - Billings.Robin@epa.gov
  - 404-562-8515

- Federal Electronics Challenge: [http://www.epa.gov/fec/](http://www.epa.gov/fec/)
- Overview of Media Sanitization: [http://www.epa.gov/fec/resources/sanitization.pdf](http://www.epa.gov/fec/resources/sanitization.pdf)
Media Sanitization
Used Electronics Processing
SAND 2012-6049P
Where We're Coming From

- Sandia is a National Nuclear Security Administration (NNSA) laboratory for the Department of Energy (DOE)
  - More stringent data security requirements than other DOE sites
  - Geographically isolated – New Mexico, USA
    
    *(No passport required)*

- Only covering processes at Sandia’s New Mexico site
  - Other smaller Sandia sites self-manage or ship equipment and materials to us.
Used Electronics Triage

- Already vetted for internal reuse

- Donation occurs when possible
  - April 2012 “K-12 Computer Donation Event”
  - 25 Schools/Districts from around New Mexico
  - 1358 computers donated; along with monitors, parts, and office binders
  - No Hard Drives
End of Useful Life

▪ Shipped for basic domestic recycling
  ▪ Desktops and Laptops (without hard drives)
  ▪ CRT Monitors
  ▪ Broken LCD monitors
  ▪ Other mixed/broken electronics

▪ Shipped for refurbishment or constituent recovery
  ▪ ISDN telephones
  ▪ Whole circuit boards
  ▪ Standard server blades
  ▪ High performance “super” computers
Data Security in Processes

- Cell Phones / PDAs / Radios
  - Internally sanitized by computer support department
  - Hydraulically crushed to make “unattractive”
  - Added to circuit boards for final domestic destruction & recycling

- Removable Electronic Media (REM)
  - All unclassified film, magnetic, solid state and optical media
    - Witnessed Incineration

- Exception: Commercial Off The Shelf (COTS) CDs and DVDs
  - Recycled as polycarbonate
  - Good value per pound for plastic
Data Security in Processes

- Hard Drives
  1. Physically removed from computer/device
  2. Data is overwritten 7 times
     - Is this over-writing over-kill?
  3. Hard drive is dismantled
     - Scrap metal is recycled
     - Neodymium magnets are recovered
  4. Aluminum platter is degaussed
  5. Aluminum platter is shredded and recycled
Policy Drivers

- DOE Order  200.1A (2008) Info Tech Mgmt – points to:
  - DOE Order 205.1B (2011) – Cyber Security Mgmt
  - DOE Policy 470.1 – Integrated Safeguards and Security Mgmt

- DOE O 205.1B aims to be consistent with
  - National Institute of Standards and Technology (NIST)
  - Committee on National Security Systems (CNSS)

- Highly Conservative:
  We treat everything as if it might be “National Security Information”

- See NIST SP 800-88 – Guidelines for Media Sanitization
Guidelines for Media Sanitization

- 2.4 – “Studies have shown that most of today’s media can be effectively cleared by one overwrite.”
- Careful to note in its “Media Sanitization Decision Matrix” that the method must be “agency approved”.

Appendix A – Table A-1

- Addresses many specific types of media and hardware
  - Hard drives
  - Disks/discs
  - Microfilm
  - Network routers!

*When in doubt, burn it out...*
- Cancels “US Aid” referenced document from 1995
- Available at DoD Defense Security Service (www.dss.mil)
- Sanitize everything to the level determined by your Cognizant Security Agency (CSA)

The myth of the 3-pass DoD data destruction policy
- In 2006, the DoD “removed all verbiage on single vs. multiple pass.”
  - James Griffin, April 20, 2012
Lastly...

- A 5-page “Media Sanitization Considerations at Electronics End-of-Life” guide is available from the [FEC](http://p2.sandia.gov).

- Thanks!

Samuel A. McCord  
Solid Waste Recycling Planner  
Sandia National Laboratories  
Dept. of Regulated Waste & Pollution Prevention (P2)  
(o) 505-844-8916; (f) 505-844-2403  
[mailto:samccor@sandia.gov](mailto:samccor@sandia.gov)  