



Green Computing, Data Security, and Media Sanitization

August 2008 Federal Electronics
Challenge Partner Teleconference



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



Definitions

- 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 is a *method* for ensuring data security of information stored on media



Why Media Sanitization?

- Media store data
- Sanitization prevents unauthorized disclosure of information and ensures confidentiality
 - Allows for reuse
 - Secures for recycling



Media Sanitization and Electronics Stewardship

- Media sanitization practices may impact electronics stewardship activities, particularly reuse and recycling
- Executive Order 13423 requires reuse and donation of electronic equipment
- ★ Select the least destructive media sanitization method, which still meets security and confidentiality needs

Media is Everywhere!

Media:	Where you might find it:
Paper or microforms	<ul style="list-style-type: none">• Imaging equipment, including printers, copiers, scanners, facsimile machines and multifunction devices (MFDs)• Microfiche readers and microfilming machines
Hard drives	<ul style="list-style-type: none">• Computer desktops and laptops• Some imaging equipment
Memory	<ul style="list-style-type: none">• Most electronics
Removable electronic media (Floppies, CDs, DVDs, USB removable media, Zip disks, removable memory cards)	<ul style="list-style-type: none">• As separate components• Within many electronics
Magnetic cassettes, cards, tapes and ribbon	<ul style="list-style-type: none">• Audio and visual (AV) equipment• Tape recorders and players



Options for Media Sanitization

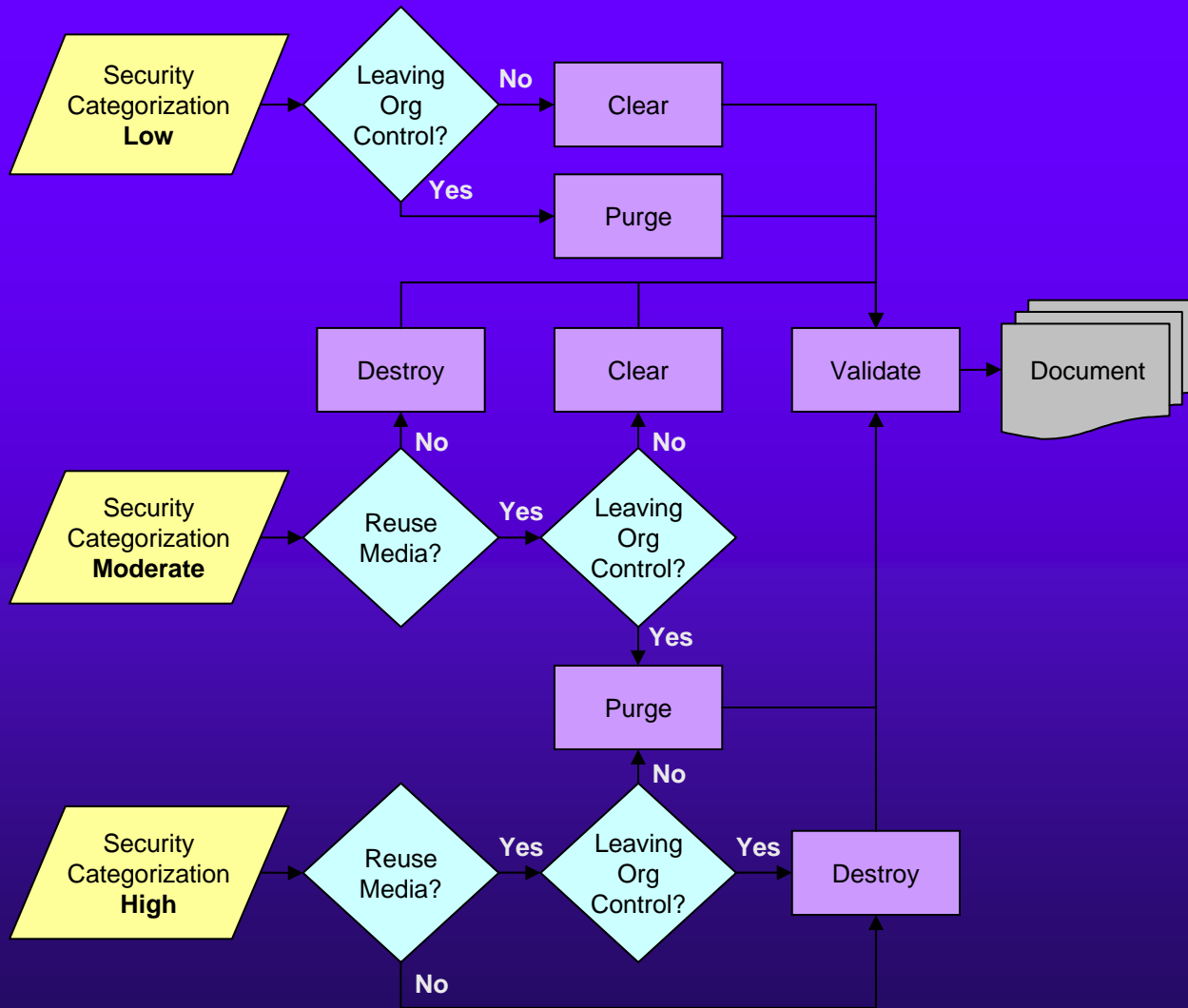
1. **Disposal:** Discarding media with no further sanitization actions
2. **Clearing:** Removing data from media so that the data can not be retrieved through a robust keyboard attack
 - *Example:* overwriting
3. **Purging:** Removing data from media so that the data can not be retrieved through a laboratory 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





Options for Reuse and Donation

- Consider the impact of your media sanitization methods
- Media with low or moderate security classification may be sanitized and preserved for reuse
- Some options for clearing or purging allow reuse without risk of disclosure
 - Check Table A-1 in NIST Special Publication 800-88



Options for Destroyed Media

- 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



Considerations for Special Contracts

- Use of some contracting vehicles may require special media sanitization considerations
 - Seat management, leasing, exchange-sales, and manufacturer take-back services
- These contracts may prohibit removal or destruction of media
- Include agency and facility media sanitization requirements in these contracts
- For take-back, ensure the manufacturer can meet agency and facility media sanitization requirements



Data Security and Electronics Stewardship

- Other electronics stewardship activities may require consideration of impacts to data security
 - Power management and shut-down implementation
 - Switching from desktops to laptops
 - Use of alternative contracts, such as seat management or leasing



References

- FEC's Media Sanitization Considerations at Electronics End-of-Life
 - <http://www.federalelectronicschallenge.net/resources/docs/sanitization.pdf>
- NIST Guidelines for Media Sanitization (See "SP 800-88")
 - <http://csrc.nist.gov/publications/PubsSPs.html>
- UNICOR's FES presentation with an overview of media considerations
 - http://www.fedcenter.gov/_kd/go.cfm?destination=ShowItem&Item_ID=9501



Contact Information

- Cate Berard
- U.S. Environmental Protection Agency
- Phone: 202-564-8847
- E-mail: berard.cate@epa.gov



Federal Electronics Challenge

- Web site:
 - <http://www.federalelectronicschallenge.net/>
- E-mail:
 - info@electronicschallenge.net (for general inquiries)
 - partner@electronicschallenge.net (for Partners only)