Media Sanitization Considerations for Federal Electronics at End-of-Life

Updated: 6/28/2012

PURPOSE

This resource provides an overview of media sanitization considerations for federal electronics at end-of-life.

DISCLAIMER

The guidance in this fact sheet **does not** supersede any federal agency's policies, procedures, guidance, or requirements with respect to media sanitization and data security. Federal organizations should discuss these and other data security issues with their facility/property management, and information technology (IT) and security experts.

This fact sheet 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.

INTRODUCTION

Data security is a critical consideration at the end-of-life for any piece of electronic equipment. Storage media must be handled and sanitized appropriately, prior to reuse, recycling or disposal, to prevent unauthorized disclosure of information and to ensure confidentiality. There are a number of options to ensure data security, each of which may allow for varying degrees of reuse for sanitized media.

The ability to reuse media is important, since federal agencies are encouraged to reuse and recycle their used electronics to the maximum extent possible. Selecting the least destructive media sanitization method, which still meets security and confidentiality needs, is necessary to facilitate the safe reuse of federal electronic equipment and media storage components.

Proper media sanitization may involve many different participants at your facility. Consider including IT staff, facility and property management, security officers, and affected environmental management system (EMS) team members when reviewing media sanitization procedures to maximize electronics reuse.

OVERVIEW OF MEDIA SANITIZATION

Electronic equipment and components may use, contain, or be various forms of storage media, such as:

Media:	Where you might find it:
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 • Some imaging equipment
Memory	• Most electronics
Removable electronic media (Floppies, CDs, DVDs, USB removable media, Zip or Jaz 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

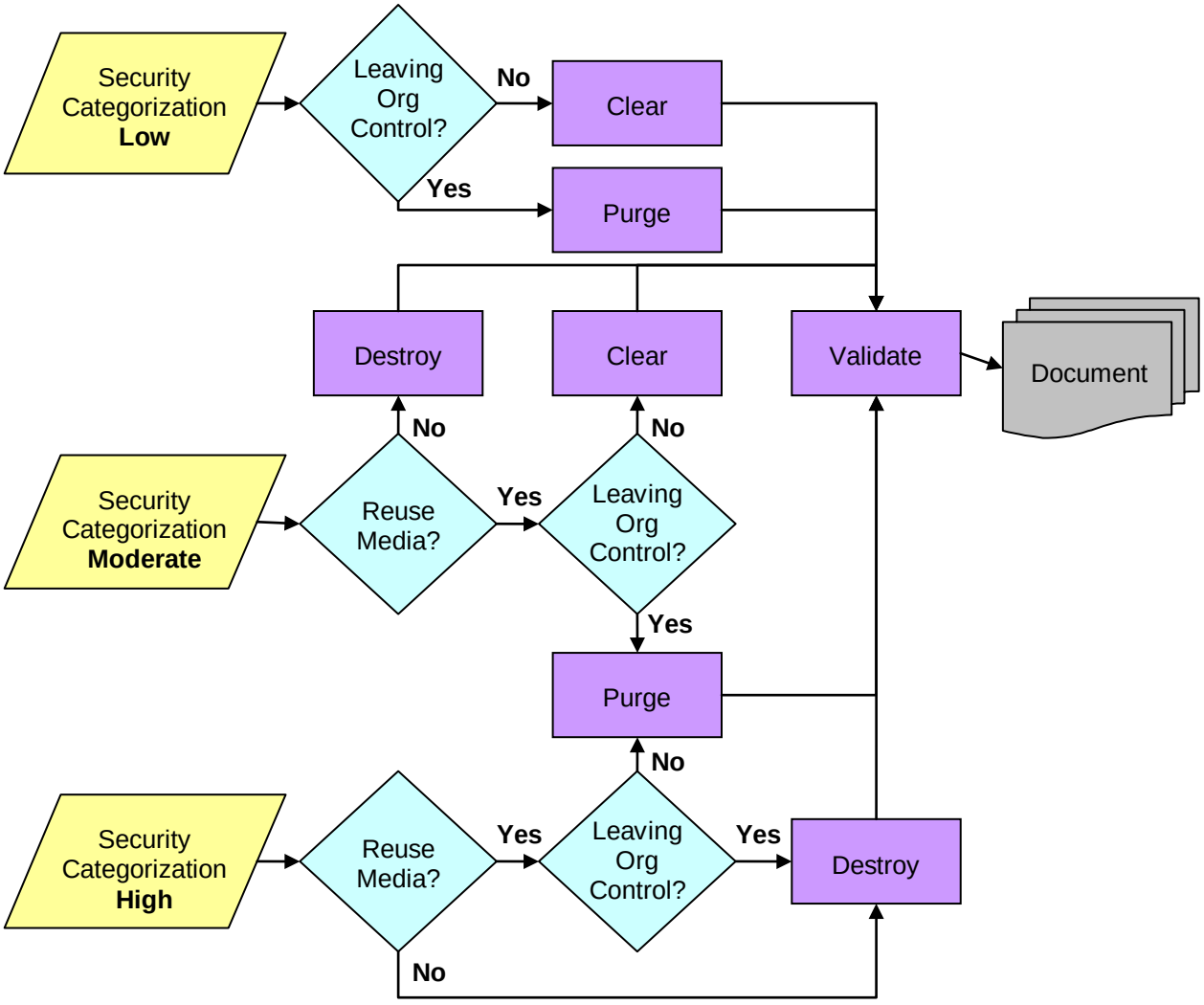
The table above is not all inclusive. Check product manuals to determine what hardware and removable media may be present in your equipment.

All of the above listed media may contain data which could be vulnerable to disclosure, if not properly sanitized.

There are four basic 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. Simple deletion of files does not suffice as clearing. *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.

NIST Special Publication 800-88 recommends the following steps for determining which media sanitization process to use, based on the security categorization and reuse options:



There are a number of additional factors to consider when selecting a media sanitization method, such as:

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

While many of these factors may influence the decision to use, or not use, a particular media sanitization process, usually the most pressing factor is the required level of security and confidentiality. Since federal organizations are required to reuse electronic assets to the maximum extent practicable, added to the security consideration is whether the media can be reused inside or outside the controlling organization.

Regardless of the chosen media sanitization process, your facility should record or receive relevant certification or documentation of data destruction, for a given medium at the desired security level.

OPTIONS FOR REUSE AND DONATION

If your organization intends to reuse media internally, or through transfer or donation to an outside organization, you must consider the impact of your media sanitization methods. As shown in the flowchart above, media with low or moderate security classification may be sanitized in a manner that preserves the ability to reuse the media. There are options for clearing and purging data from most media, which will allow the media to be used again without risk of disclosure of the old data. Table A-1 in NIST Special Publication 800-88 provides clearing and purging options for most media which allow it to be reused again.

OPTIONS FOR DESTROYED MEDIA

If physical destruction of the media is necessary, there may still be options for environmentally preferable disposal of the remaining media.

If media is rendered unusable by abrasive scraping, shredding, disintegrating or pulverizing, look for opportunities to recycle the resulting material. Some facilities may be able to separate, melt down, and resell the metals and plastics in destroyed media. Be aware that media rendered unusable through chemical destruction may not be able to be recycled and may require special disposal.

If media must be incinerated, look for an incinerator that practices energy recovery, which captures and uses the heat from incineration for water heating or electricity generation.

CONSIDERATIONS FOR SPECIAL CONTRACTS

Use of some contracting vehicles, such as seat management, leasing, exchange-sales, and manufacturer take-back services, require special considerations with regards to media sanitization. These contracting mechanisms may prohibit removal of media, or physical destruction or purging that renders media unusable (e.g., degaussing). Be sure to include media sanitization clauses in these contracts that allow your agency or facility to meet its data security requirements, either through internal sanitization or sanitization by your vendor. If your organization opts to use vendor-provided media sanitization services, be sure that the vendor's practices meet your agency's data security requirements.

REFERENCES

The NIST Guidelines for Media Sanitization are available at: http://csrc.nist.gov/publications/PubsSPs.html (See "SP 800-88").

CONTACT INFORMATION

If you have questions related to this resource or need other assistance with the Federal Electronics Challenge, please contact your Regional Champion: http://www2.epa.gov/fec/technical-assistance.

Visit the FEC online: http://www2.epa.gov/fec/

E-mail the FEC: fec@epa.gov