

  
Approved for Release

Mary C. Pleffner

Departmental Property Management Officer

3/21/2011  
Date

DEPARTMENT OF COMMERCE (DOC)  
CHIEF FINANCIAL OFFICER AND ASSISTANT SECRETARY FOR  
ADMINISTRATION  
OFFICE OF ADMINISTRATIVE SERVICES

PROPERTY BULLETIN #5, FY11

**SUBJECT:** DOC Media Sanitization

**EFFECTIVE DATE:** March 11, 2011

**EXPIRATION DATE:** Effective until canceled or superseded

**SUPERSEDES:** Not Applicable

**BACKGROUND:** In accordance with the DOC Information Technology Security Program Policy and Minimum Implementation Standards, dated June 2005, it is a requirement that "units sanitize or destroy information system digital media before its disposal or release for reuse outside the organization, to prevent unauthorized individuals from gaining access to and using the information contained on the media." Additionally, in accordance with NIST Special Publication 800-88, *Guidelines for Media Sanitization*, dated September 2006, Property Management Officers are "responsible for ensuring that sanitized media and devices that are redistributed within the organization, donated to external entities, or destroyed are properly accounted for." Media sanitization is crucial in preventing the unauthorized disclosure of information.

**PURPOSE:** The purpose of this property bulletin is to ensure all Property Officials (POs) are familiar with the requirements regarding media sanitization for personal property.

**PROCEDURES/APPLICABILITY:** Sanitization is the process of removing data from storage media with the reasonable assurance that the data may not be easily retrieved and reconstructed. Many types of personal property that we use to store data is sensitive and confidential in nature. If the property is not properly sanitized, the release of an unauthorized disclosure of information could result. Examples of personal property that require sanitization before its disposal or release for reuse outside the organization include desktop computers, laptop/portable/notebook computers, Blackberry/Palm Pilot/personal digital assistant devices, mobile/cellular phones, color/laser/multi-function printers, copiers, fax machines, scanners, servers, and removable storage media. There are several different methods to sanitize media. These methods include:

- Clear – Overwrite storage space on the media with non-sensitive data.

- Purge – Expose media to a strong magnetic field in order to disrupt the recorded magnetic domains.
- Destroy – Various methods designed to completely destroy the media, typically carried out at an outsourced destruction facility.

All POs should consult with their respective CIO office to obtain guidance and assistance in conducting proper media sanitization of personal property. Below are guidelines, per NIST Special Publication 800-88, for common types of personal property (leased or owned) that require sanitization and corresponding examples of recommended sanitization action.

Property Type	Clear	Purge	Physical Destruction
Copy machines/Fax machines	Perform a full manufacturer's reset to return the router back to its factory default settings. Contact the manufacturer for proper sanitization procedure.	Same as Clear.	<ul style="list-style-type: none"> <li>• Shred.</li> <li>• Disintegrate.</li> <li>• Pulverize.</li> <li>• Incinerate. (Incinerate copy machines by burning them in a licensed incinerator.)</li> </ul>
Hard Drives/USB Removable Media	Overwrite media by using agency-approved and validated overwriting technologies/methods/tools.	<ul style="list-style-type: none"> <li>• Purge using Secure Erase. The Secure Erase software can be downloaded from the University of California, San Diego (UCSD) CMRR site.</li> <li>• Purge hard disk drives either 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>• Purge media by using agency-approved and validated purge technologies/tools.</li> </ul> <p>**Degaussing any current generation hard disk will render the drive permanently unusable.</p>	<ul style="list-style-type: none"> <li>• Disintegrate.</li> <li>• Shred.</li> <li>• Pulverize.</li> <li>• Incinerate. (Incinerate hard disk drives by burning them in a licensed incinerator.)</li> </ul>

It is understood that POs generally do not sanitize media. However, it is important that they are familiar with media sanitization requirements to ensure that personal property, as applicable, is properly sanitized and clearly annotated as sanitized before removal or

disposal. All operating units should have documented procedures that detail the process for properly sanitizing media from personal property. Please refer to DOC Information Technology Security Program Policy, dated January 2009, and NIST Special Publication 800-88, *Guidelines for Media Sanitization*, dated September 2006 for additional guidance.

**REFERENCES:**

- DOC Information Technology Security Program Policy, January 2009
- DOC Personal Property Management Manual, October 2007
- Deputy Secretary of Commerce Memorandum, November 6, 2006, Subject: Safeguarding Personally Identifiable Information
- NIST Publication 800-88, *Guidelines for Media Sanitization*, September 2006.

**PROGRAM MANAGER CONTACT INFORMATION:** William Garrett, Chief, Personal Property Management Division, [wgarrett@doc.gov](mailto:wgarrett@doc.gov), (202) 482-6122.