

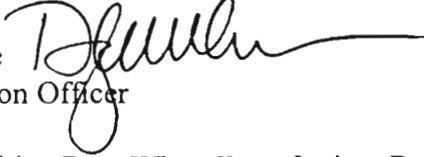


# United States Department of the Interior

OFFICE OF THE SECRETARY  
Washington, D.C. 20240

## IRM Bulletin 2001-0004

To: Solicitor  
Heads of Bureaus and Offices  
Bureau/Office Chief Information Officers  
Director, National Business Center  
Bureau/Office Personal Property Officers

From: Daryl W. White   
Chief Information Officer

Subject: Protecting Sensitive Data When Transferring, Donating, or Disposing of Computer Equipment

This bulletin is effective immediately.

Interior computer systems are routinely transferred, donated, or disposed of to organizations that are outside of Interior's control through replacements, equipment maintenance, and excess/surplus actions. While these actions are beneficial and necessary, bureaus/offices have a requirement to ensure that sensitive information is not exposed to the risk of unauthorized disclosure. Bureaus/Offices must also ensure that in transferring, donating, or disposing of computer equipment, they do not violate software copyright laws.

The normal deletion of computer files and data only obscures that information from immediate view. These files and data can usually be recovered with minimal expertise using commercially available software utilities. Effective deletion of data requires a more deliberate procedure, usually entailing an overwriting process called wiping. Also, by failing to remove commercial software applications from the hard drives, there is the potential for a bureau/office to place itself in the position of violating software copyrights and end-user licensing agreements.

This bulletin specifies a risk management approach to safe re-use or disposal of this type of equipment and applies to all Interior computer systems.

### **Risk Management Approach**

In Interior, virtually all computers should be considered to potentially contain sensitive information. Bureaus/Offices will use one of the two following approaches to remove sensitive data, depending on the level of sensitivity, when transferring, donating, or disposing computer equipment.

National Security Information System (NSIS) - That is, any system processing information classified as Top Secret, Secret, or Confidential. Storage media for these systems will be dismantled and destroyed, or degaussed by a National Security Agency approved degaussing device. Storage media used in NSIS systems will not be released outside of United States Government classified information control without the express written permission of the Department's Chief Information Officer and the Director of Managing Risk and Public Safety. Managers also have the responsibility of assessing risk of internal equipment transfers, however, even internal transfers of this security level of equipment should be destroyed or properly sanitized (degaussed).

Unclassified Information - That is, any information system not processing National Security Information. Storage media for these systems will be sanitized by using disk "wiping" software, a low-level reformat (with data verification), or dismantled and destroyed. The selection of the particular method is to be made based on the individual needs and capabilities of the implementing organization or entity. Managers have the responsibility of ensuring the equipment is sanitized before computer equipment is transferred (internal transfers included), donated or destroyed.

No equipment should be excessed or transferred until the appropriate method of data protection has been applied to all storage media contained within that equipment. In some cases, non-volatile memory, such as removable flash cards, exist and may contain sensitive information. These forms of memory should also be erased or removed from the device. Also, ensure that all removable storage media (floppies, ZIP disks, backup tapes, CD-ROMs, etc.) are removed or destroyed before the equipment is transferred, disposed of, or donated.

Software may only be transferred, donated or disposed of in accordance with the authorities listed in the software license agreement.

IRM certification must be provided to the property officers to ensure degaussing and/or forms of memory have been erased or removed from the device. No property may be transferred, donated, recycled, sold or scrapped without the approval of the servicing property office.

### **Waivers and Exceptions**

Waivers and exceptions to these requirements require formal Departmental approval prior to implementation. The Department of the Interior Chief Information Officer will coordinate all requests for waivers and exceptions.

**Authorities**

375 DM Chapter 19  
IPMD 114-60

**Contact**

Questions concerning this bulletin should be directed to the Departmental IT Security Manager, Steve Schmidt on (202) 208-5438 or email at [steve\\_schmidt@ios.doi.gov](mailto:steve_schmidt@ios.doi.gov).