





# Instructions to Complete NOAA Computer/Hard Drive/Scanners/Printers/Monitors/Any Assets Retaining Information Sanitization Validation Form

## SUMMARY:

The drive owner or local IT specialist must sanitize hard drive data to ensure it is unrecoverable or must completely destroy the drive. Directives on accomplishing this are published by the NOAA OCIO and must be complied.

Final event documentation submitted to PPMB, as well as locally maintained records, should include a “**NOAA Computer/Hard Drive Sanitization Validation Form**”. This form should be completed by both the individual responsible for cleaning the hard drive and the property custodian. This policy applies to all NOAA offices.

*\*NOAA National Disposal Plan for Personal Property Management –10.1.2. Cleaning Hard Drives*

Below are instructions to complete the form for the computer/hard drive to be sanitized. Reference the Inventory Assets (Global Information) report for the identified property, as necessary.

- 1) **Organization** – Select the owning NOAA organization from the drop down menu, which corresponds to the custodial area.
- 2) **Property Custodian Name and Property Custodian Code (Custodial Area)** – Enter the Property Custodian name and the unique, alpha-numeric Property Custodian Code, assigned to the Property Custodial, for which custodial responsibility of the identified barcode(s) fall under.
- 3) **Barcode Number** – Enter the barcode number for the property to be sanitized.
- 4) **Model Number** – Enter the related model number for the identified barcode.
- 5) **Serial Number** – Enter the related serial number for the identified barcode.
- 6) **Description** – Enter the related description for the identified barcode.

### Reference Document: Inventory Assets (Global Information) Report

Sunflower Enterprise  
ASMSG03
**Inventory Assets (Global Information)**
Page 3 of  
02/24/2011 09:..

Barcode #	Barc ode Type	Flags	Description	Manufacturer	Model Number	Serial Number	Asset Value	Eff Date
CD0001678407		E O	SATELLITE	BOEING SATELLITE SYSTEMS, INC.	GOES-15	SN_CD0001678407	\$ 422,325,711.53	02/17/20

Unique Name :  
Cust Area : 54015N327  
Property Contact : BLOWE TERRANCE / 540035  
Current User : CARTER WILLIAM 42740  
Fed. Supply Group : SPACE VEHICLES  
Asset Condition : 4 USED - MAJOR REPAIRS NOT REQUIRED  
Expected Return Date :  
Utilization Code : IN SERVICE

Stock Number :  
Location : SUITLAND, MD  
BUILDING : NSOF ROOM : IN EARTH'S ORBIT

Vendor :  
Old Serial Number : New Serial Number: SN\_CD0001678407

Property Custodian Name	Property Custodian Code	Description
ACQUISITION COST	\$100,000	Bureau:14**Fiscal Year:2010**Fund Code:28**Organization:54-40-02-0001-00-00-00**User Code:000000**Adjust depreciation from:
ACQUISITION COST	\$9,068,441.29	Bureau:14**Fiscal Year:2010**Fund Code:28**Organization:54-40-02-0001-00-00-00**User Code:000000**Adjust depreciation from:
ACQUISITION COST	\$10,346,986.97	Bureau:14**Fiscal Year:2010**Fund Code:32**Organization:54-40-02-0001-00-00-00**User Code:000000**Adjust depreciation from:
ACQUISITION COST	\$3,116,679.35	Bureau:14**Fiscal Year:2010**Fund Code:36**Organization:54-40-02-0001-00-00-00**User Code:000000**Adjust depreciation from:
ACQUISITION COST	\$6,883,000	Bureau:14**Fiscal Year:2010**Fund Code:36**Organization:54-40-02-0001-00-00-00**User Code:000000**Adjust depreciation from:
ACQUISITION COST	\$4,192,873.4	Bureau:14**Fiscal Year:2010**Fund Code:36**Organization:54-40-02-0001-00-00-00**User Code:000000**Adjust depreciation from:
ACQUISITION COST	\$7,090,828.17	Bureau:14**Fiscal Year:2010**Fund Code:36**Organization:54-40-02-0001-00-00-00**User Code:000000**Adjust depreciation from:
ACQUISITION COST	\$93,630,034.25	Bureau:14**Fiscal Year:2010**Fund Code:36**Organization:54-40-02-0001-00-00-00**User Code:000000**Adjust depreciation from:
ACQUISITION COST	\$3,493,459.26	Bureau:14**Fiscal Year:2010**Fund Code:1002**Organization:54-40-02-0001-00-00-00**User Code:000000**Adjust depreciation from:
ACQUISITION COST	\$61,474,983.98	Bureau:14**Fiscal Year:2010**Fund Code:36**Organization:54-40-02-0001-00-00-00**User Code:000000**Adjust depreciation from:

**\*The information identified above should match the detail provide on this spreadsheet.**

7) **Sanitization Method Used** – Select the sanitization method from the drop down menu that was utilized to remove the secure data from the computer/hard drive. Reference the table below as necessary.

TYPE:	DESCRIPTION:
<b>Clearing</b>	<p>Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Simple deletion of items would not suffice for clearing. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. It must be resistant to keystroke recovery attempts executed from standard input devices and from data scavenging tools. For example, overwriting is an acceptable method for clearing media.</p> <p>There are overwriting software or hardware products to overwrite storage space on the media with non-sensitive data. This process may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table) but also may include all addressable locations. The security goal of the overwriting process is to replace written data with random data. Overwriting cannot be used for media that are damaged or not writeable. The media type and size may also influence whether overwriting is a suitable sanitization method.</p>
<b>Purging</b>	<p>Purging information is a media sanitization process that protects the confidentiality of information against a laboratory attack. For some media, clearing media would not suffice for purging. However, for ATA disk drives manufactured after 2001 (over 15 GB) the terms clearing and purging have converged.</p> <p>A laboratory attack would involve a threat with the resources and knowledge to use nonstandard systems to conduct data recovery attempts on media outside their normal operating environment. This type of attack involves using signal processing equipment and specially trained personnel.</p> <p>Executing the firmware Secure Erase command (for ATA drives only) and degaussing are examples of acceptable methods for purging. Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.</p> <p>Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains. A degausser is a device that generates a magnetic field used to sanitize magnetic media. Degaussers are rated based on the type (i.e., low energy or high energy) of magnetic media they can purge. Degaussers operate using either a strong permanent magnet or an electromagnetic coil. Degaussing can be an effective method for purging damaged media, for purging media with exceptionally large storage capacities, or for quickly purging diskettes. Degaussing is not effective for purging nonmagnetic media, such as optical media [compact discs (CD), digital versatile discs (DVD), etc.).</p>
<b>Destroying</b>	<p>Destruction of media is the ultimate form of sanitization. After media are destroyed, they cannot be reused as originally intended. Physical destruction can be accomplished using a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting.</p> <p>If destruction is decided upon due to the high security categorization of the information or due to environmental factors, any residual medium should be able to withstand a laboratory attack.</p> <p><i>Disintegration, Incineration, Pulverization, and Melting.</i> These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or incineration facility with the specific capabilities to perform these activities effectively, securely, and safely.</p> <p><i>Shredding.</i> Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality level that the information cannot be reconstructed.</p> <p>Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD), and magneto-optic (MO) disks must be destroyed by pulverizing, crosscut shredding or burning.</p> <p>Destruction of media should be conducted only by trained and authorized personnel. Safety, hazmat, and special disposition needs should be identified and addressed prior to conducting any media destruction.</p>
<b>Removed</b>	Removal is only used for monitors, scanners, printers, or any assets that cannot be sanitized.

*NIST Special Publication 800-88 (Guidelines for Media Sanitization) - Table 2-1. Sanitization Types*

8) **Final Disposition of Media** – Enter the applicable status for the data removed as a result of sanitation.

a) **Disposed** – The device will be destroyed.

b) **Other** – All other future use or action to be taken regarding the identified device.

9) **IT Security Official** - This item should be completed by your ISSO (Information System Security Officer).

**REFERENCES:**

**NOAA National Disposal Plan for Personal Property Management:**  
[http://www.pps.noaa.gov/060111\\_noaa\\_national\\_disposal\\_plan.pdf](http://www.pps.noaa.gov/060111_noaa_national_disposal_plan.pdf)

**NIST Special Publication 800-88 (Guidelines for Media Sanitization):**  
[http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88\\_rev1.pdf](http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf)