Standard Operating Procedure

Digital Media Sanitization

ITS-SOP-0035
Version Date: 20080915
Effective Date: 20080915
Expiration Date: 20110915
Responsible Office: Office of the Chief Information Officer

Document Change and Review History

Version Number	Summary of Changes	Changes Made/Reviewed By	Date

Table of Contents

1. Introduction

1.1 Purpose

The purpose of this Standard Operating Procedure (SOP) is to protect NASA information and to ensure that there is no accidental leakage; therefore, it institutes a procedure for sanitizing electronic storage devices.

The variety and capacity of electronic storage devices is increasing, and many of them are portable. As a result, there is an increased risk that NASA information could be used inappropriately. All NASA information has a low, moderate, or high security impact level. The approved method for sanitizing an electronic storage media device depends on the security impact level of the information stored on it.

1.2 Scope

Any electronic storage device that has ever contained NASA information, even for a brief period of time, must be sanitized before it can be reassigned, transferred, or discarded. This SOP applies to all information system owners, who are required to follow these procedures from the creation to the disposal of all information that is stored on information technology (IT) systems under their control.

This SOP does not cover classified information. Centers must contact the Office of Security and Program Protection (OSPP) for instructions on sanitizing or destroying classified information. In addition, this SOP does not cover destruction of hard-copy material.

1.3 Applicable Documents

This guidance was developed in accordance with the following regulatory mandates, directives, and federal publications:

- Federal Information Processing Standards (FIPS) Publication, *Standards for Security Categorization of Federal Information and Information Systems,* February 2004.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, (Revision 2) *Recommended Security Controls for Federal Information Systems,* December 2007
- NIST SP 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems*, July 2008
- NIST SP 800-88, *Guidelines for Media Sanitization*, September 2006
- National Security Agency (NSA) Storage Devices Destruction Guidance, http://www.nsa.gov/ia/government/mdg.cfm
- Department of Defense (DoD) 5520.22-M National Industrial Security Program Operating Manual (NISPOM)

1.4 Digital Media Sanitization

The need to sanitize a storage device generally falls into one of the following categories:

a. The storage device is being repurposed or reissued within NASA

b. The storage device is being repurposed, or reissued outside of NASA, or is otherwise temporarily or permanently leaving NASA's control

c. The storage device will no longer be used by NASA or any other party

Two factors combine to determine the proper method of sanitizing a storage device:

a. The mechanics of the method must correspond to the nature of the storage device. For example, a method that works on a hard disk might not work on a flash drive. (An example of the mechanics of this method is performing a three-pass DoD 5220.22M wipe)

b. The thoroughness of the method must correspond to the security category of the information on the storage device and to the storage device's future use

Sometimes there is more than one method of sanitizing a given device. In that case, rank them in order of effectiveness, and use the most effective method that is available.

1.5 Digital Media Sanitization Process

Sanitization is the process of removing data from storage devices so that it is impossible or nearly impossible to recover it. The sanitization method depends on the type of storage devices, and it can include removing labels, markings, and activity logs.

1.5.1 Methods

According to NIST SP 800-88, there are three primary methods for sanitizing storage devices:

a. Clearing the data

b. Purging the data

c. Destroying the data

In this publication, the terms "clear" and "purge" are interchangeable. It has been determined that, in the case of NASA information, "clearing" satisfies NIST's guidance for "purging."

Note: Using an approved mechanism for destroying storage devices, even when it is not required, is always an acceptable way to ensure the storage devices is properly sanitized.

1.5.2 Selection

Use the following two tables to select the sanitization method whose thoroughness corresponds to the security category of the information on the storage device and to the storage device's future use.

Table 9-1 applies to storage devices containing information with a low or moderate security impact level.

Security Impact Level: **Low or Moderate**		Acceptable Sanitization Methods	
		Clear	**Destroy**
Future Control of the Storage Device	Repurposed or Reissued **(under NASA control)**	YES	N/A
	Repurposed or Reissued **(not under NASA control)**	YES	N/A
	Discarded **(not under anyone's control)**	NO	YES

Table 9-1: Sanitization Method—Low or Moderate Impact Level

Table 9-2 applies to storage devices containing information with a high security impact level.

Security Impact Level: **High**		Acceptable Sanitization Methods	
		Clear	**Destroy**
Future Control of the Storage Device	Repurposed or Reissued **(under NASA control)**	YES	N/A
	Repurposed or Reissued **(not under NASA control)**	NO	YES
	Discarded **(not under anyone's control)**	NO	YES

Table 9-2: Sanitization Method—High Impact Level

After determining the method (clear or destroy) from Table 9-1 or 9-2 above, consult the following tables for the appropriate mechanisms for carrying out that method. If there is more than one mechanism in the list, select the one that can be done the easiest, as they are all sufficient. Tables 9-3 through 9-10 detail the various media types and their associated sanitization mechanisms.

Table 9-3 Hand-Held Devices – Sanitization Mechanisms
Table 9-4 Networking – Sanitization Mechanisms
Table 9-5 Magnetic Disks – Sanitization Mechanisms
Table 9-6 Magnetic Tape – Sanitization Mechanisms
Table 9-7 Optical Disks – Sanitization Mechanisms
Table 9-8 Memory – Sanitization Mechanisms
Table 9-9 Magnetic Cards – Sanitization Mechanisms
Table 9-10 Other Equipment – Sanitization Mechanisms

Sanitization Mechanisms for hand-held devices:

Type of Hand-Held Device	Clear mechanisms	Destroy mechanisms
Cell Phones	• Delete all information manually This includes the call history and all phone numbers • Perform a full reset Use the manufacturer's documentation or contact the manufacturer for the method of restoring the factory default settings.	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility
Personal Digital Assistants (PDAs)	• Delete all information manually • Perform a full reset Use the manufacturer's documentation or contact the manufacturer for the method of restoring the factory default settings.	• Incinerate it in a licensed facility • Shred • Pulverize

Table 9-3: Hand-Held Devices—Sanitization Mechanisms

Sanitization Mechanisms for networking devices:

Type of Networking Device	**Clear** *mechanisms*	**Destroy** *mechanisms*
Routers (any type)	• Perform a full reset Use the manufacturer's documentation or contact the manufacturer for the method of restoring the factory default settings.	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility

Table 9-4: Networking—Sanitization Mechanisms

Sanitization Mechanisms for magnetic disks:

Type of Magnetic Disk	**Clear** *mechanisms*	**Destroy** *mechanisms*
ATA Hard Drives	• Purge with Secure Erase. The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site. • Purge in an NSA/CSS-approved automatic degausser or disassemble the drive and purge the enclosed platters with an NSA/CSS-approved degaussing wand. • Purge with agency-approved and validated purge technologies or tools. Degaussing any current-generation hard disk renders it permanently unusable.	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility

Type of Magnetic Disk	**Clear** *mechanisms*	**Destroy** *mechanisms*
USB Removable Storage Pen drives, thumb drives, flash drives, memory sticks, or USB-powered hard drives	• Purge with Secure Erase. The Secure Erase software can be download from the University of California, San Diego (UCSD) CMRR site. • Purge in an NSA/CSS-approved automatic degausser or disassemble the drive and purge the enclosed platters with an NSA/CSS-approved degaussing wand. • Purge with agency-approved and validated purge technologies or tools. Degaussing any current-generation hard disk renders it permanently unusable.	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility
Zip Disks	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools.	• Shred • Incinerate it in a licensed facility
SCSI Drives	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools.	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility

Table 9-5: Magnetic Disks—Sanitization Mechanisms

Sanitization Mechanisms for magnetic tape:

Type of Magnetic Tape	**Clear** *mechanisms*	**Destroy** *mechanisms*
Reel and Cassette	• Overwrite or degauss the tape. Overwriting (also called re-recording) a tape is most often impractical, because it takes a very long time. Overwrite (re-record) the tape on a system that is similar to the one that originally recorded the data. For example, overwrite previously recorded sensitive VHS videos on a comparable VHS recorder. Overwrite the entire tape once with known non-sensitive signals.	• Incinerate the tapes in a licensed facility • Shred It is not necessary to prepare the tape for destruction, for example, by removing it from the reel or cassette. However, it may be necessary to do so for recycling or to comply with the destruction facility's requirements.

Table 9-6: Magnetic Tape—Sanitization Mechanisms

Sanitization Mechanisms for optical disks:

Type of Optical Disk	**Clear** *mechanisms*	**Destroy** *mechanisms*
CDs	Use the destroy mechanisms	• Use a commercial optical-disk grinding device to remove the information-bearing layers. • Incinerate the optical disk in a licensed facility. • Use an optical-disk shredder or disintegrator device to reduce the CD to particles that have a nominal edge dimension of five millimeters and surface area of twenty-five square millimeters, or smaller. This is the currently acceptable particle size. New disk shredders must reduce the disk to particles with a surface area of 0.25mm.

DVDs	Use the destroy mechanisms	• Use a commercial optical-disk grinding device to remove the information-bearing layers. • Incinerate the optical disk in a licensed facility. • Use an optical-disk shredder or disintegrator device to reduce the CD to particles that have a nominal edge dimension of five millimeters and surface area of twenty-five square millimeters, or smaller. This is the currently acceptable particle size. New disk shredders must reduce the disk to particles with a surface area of 0.25mm.

Table 9-7: Optical Disks—Sanitization Mechanisms

Sanitization Mechanisms for memory devices:

Type of Memory	**Clear** *mechanisms*	**Destroy** *mechanisms*
Compact Flash Drives, SD	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools. Table 11 below may provide appropriate tools to accomplish this task.	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility
Dynamic Random Access Memory (DRAM)	Purge the DRAM as follows: • Power it off • Remove the battery (if there is one)	• Shred • Disintegrate • Pulverize
Electronically Alterable PROM (EAPROM)	• Perform a full chip purge as described in the manufacturer's data sheets	• Shred • Disintegrate • Pulverize

Type of Memory	Clear *mechanisms*	Destroy *mechanisms*
Electronically Erasable PROM (EEPROM)	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools. • Remove all labels or markings that indicate the previous use or confidentiality.	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility
Erasable Programmable ROM (EPROM)	• Clear functioning EPROM by performing an ultraviolet purge following the manufacturer's recommendations, but for three times the recommended length of time. • Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools.	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility
Field Programmable Gate Array (FPGA) Devices (Non-Volatile)	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools	• Shred • Disintegrate • Pulverize
Field Programmable Gate Array (FPGA) Devices (Volatile)	Clear functioning FPGA as follows: • Power it off • Remove the battery (if there is one)	• Shred • Disintegrate • Pulverize
Flash Cards	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools. Table 11 below may provide appropriate tools to accomplish this task.	• Shred • Disintegrate • Pulverize

Type of Memory	Clear *mechanisms*	Destroy *mechanisms*
Flash EPROM (FEPROM)	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools • Perform a full chip purge as described in the manufacturer's data sheets.	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility
Magnetic Bubble Memory	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools	• Shred • Disintegrate • Pulverize When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance of the destruction device.
Magnetic Core Memory	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools • Degauss in an NSA/CSS-approved degausser	• Shred • Disintegrate • Pulverize When practical, the outer chassis and electronic circuit boards should be removed from the core memory unit to optimize the performance of the destruction device.
Non Volatile RAM (NOVRAM)	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools Each overwrite must remain in memory for a period longer than the data did. • Remove all power, including battery power.	• Shred • Disintegrate • Pulverize

Type of Memory	Clear *mechanisms*	Destroy *mechanisms*
PC Cards or Personal Computer Memory Card International Association (PCMCIA) Cards	Use the destroy mechanisms	Destroy by incinerating in a licensed facility or use (an NSA evaluated) a disintegrator to reduce the card's internal circuit board and components to particles that are nominally two (2) millimeters in size.
Programmable ROM (PROM)	Use the destroy mechanisms	
RAM	Purge the functioning DRAM as follows: • Power it off • Remove the battery (if there is one)	• Shred • Disintegrate • Pulverize
ROM	Use the destroy mechanisms	• Shred • Disintegrate • Pulverize
USB Storage Devices (Pen drives, thumb drives, flash drives, memory sticks) —not including hard drives	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools	• Shred • Disintegrate • Pulverize
Smart Cards	Use the destroy mechanisms	For smart card devices& data storage tokens that are in credit card form, cut or crush the smart card's internal memory chip using metals snips, a pair of scissors, or a strip cut shredder (nominal 2 mm wide cuts). Smart cards packaged into tokens (i.e. SIM chips, thumb drives and other physically robust plastic packages) that are not capable of being shredded should instead be destroyed via incineration or disintegration to 2 mm size particles.

Table 9-8: Memory—Sanitization Mechanisms

Sanitization Mechanisms for magnetic cards:

Type of Magnetic Card	**Clear** *mechanisms*	**Destroy** *mechanisms*
Magnetic Cards	• Overwrite the entire medium by using agency-approved and validated overwriting technologies, methods, and tools	• Shred • Incinerate by burning in a licensed facility

Table 9-9: Magnetic Cards—Sanitization Mechanisms

Sanitization Mechanisms for other equipment:

Type of Equipment	**Clear** *mechanisms*	**Destroy** *mechanisms*
Copy Machines	• Perform a full reset Use the manufacturer's documentation or contact the manufacturer for the method of restoring the factory default settings.	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility
Fax Machines	• Perform a full reset Use the manufacturer's documentation or contact the manufacturer for the method of restoring the factory default settings.	• Shred • Disintegrate • Pulverize • Incinerate it in a licensed facility

Table 9-10: Other Equipment—Sanitization Mechanisms

1.5.3 Approved Sanitization Tools

The National Security Agency (NSA) provides a list of evaluated products that are acceptable and approved for high-security disintegrators, optical storage devices destruction devices, punched tape destruction devices, and degaussers. This list can be found at http://www.nsa.gov/ia/government/mdg.cfm.

Additionally, for the electronic wiping of certain digital storage devices, NASA has approved the use of the following tools:

Product Name	Website
Secure Erase	http://cmrr.ucsd.edu/Hughes/SecureErase.html

Darik's Boot and Nuke (DBAN)	http://dban.sourceforge.net
WipeDrive/WipeDrive Pro	http://www.whitecanyon.com

Table 10-1: Approved Sanitization Tools

1.5.4 Recording and Verifying Sanitization

In order to ensure proper record keeping and fully meet NIST requirements, it is important that records are kept surrounding sanitization activities for media for systems with a HIGH security impact level. These records must be kept for systems with a security impact level of HIGH and are optional for systems with a security impact level of MODERATE or LOW. The form found in Appendix B has the information that should be recorded and tracked for these systems.

In addition to sanitization and record keeping activities, it is also necessary to periodically test the sanitization equipment and procedures to ensure they are performing as intended. Those involved with sanitization of media should periodically attempt to access and recover information that they have just sanitized after following their procedures. If information was successfully recovered, then the media should not be considered sanitized and the procedures and equipment should be thoroughly examined to determine where the failure occurred.

1.5.5 Special Considerations

The following should be taken into consideration when destroying digital storage devices:

a. Avoid the unauthorized destruction of records.

b. Do not sanitize electronic storage devices that contain federal records as defined in NASA Procedural Directive (NPD) 1440.6G.

c. If you are destroying records in compliance with their approved retention schedule, as in NPR 1441.1D, you can sanitize the storage device.

d. If there is any uncertainty, Centers should contact their local Records Manager for assistance.

1.6 Media Sanitization Roles and Responsibilities

The following roles and responsibilities are applicable to this SOP.

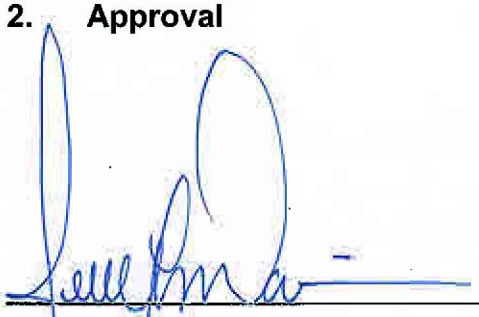
1.6.1 Information System Owner

The Information System Owner is responsible for ensuring that media associated with their systems are properly sanitized when appropriate.

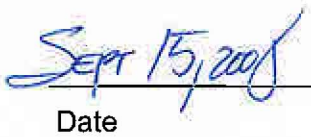
1.6.2 Media Sanitization Personnel

Media sanitization personnel are responsible for ensuring media is sanitized in an approved manner consistent with what is described in this SOP.

2. Approval



Jerry L. Davis
Deputy CIO IT Security
Senior Agency Information Security Officer



Date

Appendix A: Glossary

Acronym	Term	Explanation
CMRR	Center for Magnetic Recording Research	CMRR was founded in 1983 by a consortium of U.S. companies in the magnetic recording industry. It consists of faculty from various departments at the University of California, San Diego as well as additional researchers. Their mission is to excel in research, education, and the transfer of innovative ideas in the field of information storage technology and systems, particularly advanced data storage based upon magnetic recording.
DRAM	Dynamic Random Access Memory	Dynamic random access memory (DRAM) is the most common kind of random access memory (RAM) for personal computers and workstations. DRAM is dynamic in that, unlike static RAM (SRAM), it needs to have its storage cells refreshed or given a new electronic charge every few milliseconds.
PROM	Programmable Read-Only Memory	A non-volatile storage chip used in computers and other devices to store small amounts of volatile data, e.g. calibration tables or device configuration. It consists of an array of fuses and thus can only be programmed one-time, permanently. The key difference from a conventional ROM is that the programming is applied after the device is constructed. They are frequently seen in video game consoles or such products as electronic dictionaries, where PROMs for different languages can be substituted.
EPROM	Erasable Programmable Read-Only Memory	Similar to PROMs except once programmed, an EPROM can be erased only by exposing it to strong ultraviolet light. EPROMs are easily recognizable by the transparent fused quartz window in the top of the package, through which the silicon chip can be seen, and which permits UV light during erasing.
EEPROM	Electrically Erasable Programmable Read-Only Memory	Similar to EPROM, except the data can be erased by exposing it to an electrical charge instead of UV light source.
EAPROM	Electrically Alterable Programmable Read-Only Memory	Same as EEPROM.
FEPROM	Flash Erasable	Similar to EEPROM except that FEPROM is erased all at

Acronym	Term	Explanation
	Programmable Read-Only Memory	once while a regular EEPROM can erase one byte at a time.
FPGA (Non-Volatile)	Field Programmable Gate Array (FPGA) Devices (Non-Volatile)	A semiconductor device containing programmable logic components called "logic blocks", and programmable interconnects. Non-volatile FPGAs retain programming data when power is off.
FPGA (Volatile)	Field Programmable Gate Array (FPGA) Devices (Volatile)	A semiconductor device containing programmable logic components called "logic blocks", and programmable interconnects. Volatile FPGAs do not retain programming data when power is off. External memory is required to store the configuration which creates security risks.
NIST SP	National Institute of Standards and Technology Special Publication	Documents published by the Information Technology Lab (ITL) at NIST. Special Publications series include the 500 series (Information Technology), the 800 series (Computer Security), and the 881 series (Federal Electronic Data Interchange [EDI] Conventions). The NIST 800 Series is a set of documents that describe United States federal government computer security policies, procedures and guidelines.
NVRAM	Non Volatile Random Access Memory	The general name used to describe any type of random access memory which does not lose its information when power is turned off.
OSSP	Office of Security and Program Protection	The OSPP is responsible for all aspects of classified national security information matters, including establishing the certification and accreditation policies, procedures, and guidance for all classified IT systems operations. The OSPP responsibilities also include providing the OCIO with support in assessing and certifying unclassified IT systems and ensuring compliance with FISMA and Federal requirements.
PCMCIA Card	Personal Computer Memory Card International Association Card	The Personal Computer Memory Card International Association (PCMCIA) was organized in 1989 to promote standards for both memory and I/O integrated circuit cards. PCMCIA card is a credit card-size memory or I/O device that connects to a personal computer, usually a notebook or laptop computer. Probably the most common example of a PCMCIA card is the 28.8 Kbps modem for notebook computers.
PDA	Personal Digital Assistant	The term PDA can be used for any small mobile hand-held device that provides computing and information storage and retrieval capabilities for personal or business

Acronym	Term	Explanation
		use, often for keeping schedule calendars and address book information handy. The Blackberry and PalmPilot are examples of PDAs.

Appendix B: Media Sanitization Record Form

Responsible Organization(s)/Center(s):
Media Description:
Serial Number(s)/Property Number(s)/Media Identifier(s):
Backup Made of Information: ☐ Yes ☐ No **If Yes, Backup Location:**
Item Disposition: **Date Conducted:** _____ ☐ Clear **Conducted By (full name):** _____ ☐ Destroy **Phone Number:** _____ **Validated By (full name):** _____ **Phone Number:** _____
Sanitization Method Used:
Final Disposition of Media: ☐ Disposed ☐ Reused Internally ☐ Reused Externally ☐ Returned to Manufacturer ☐ Other: _____