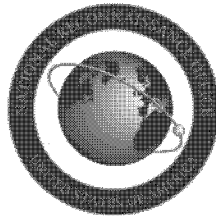


UNCLASSIFIED

National Reconnaissance Office
Business Function 100, Security and Counterintelligence
**Directive 100-29, NRO Information Systems Media and
Component Sanitization**



3 APRIL 2013

Unless otherwise noted at the redaction site, (b) (3) denials in this document are made pursuant to 10 U.S.C. § 424.

UNCLASSIFIED

UNCLASSIFIED

ND 100-29, NRO Information Systems Media and Component Sanitization
FY 2013

TABLE OF CONTENTS

ND 100-29 CHANGE LOG 3

SECTION I - INTRODUCTION..... 4

SECTION II - APPLICATION..... 4

SECTION III - REFERENCES/AUTHORITIES..... 5

SECTION IV - POLICY..... 5

SECTION V - ROLES AND RESPONSIBILITIES..... 8

SECTION VI - DIRECTIVE POINT OF CONTACT..... 9

APPROVING SIGNATURE..... 10

APPENDIX - GLOSSARY and ACRONYM LIST..... 11

UNCLASSIFIED

ND 100-29, NRO Information Systems Media and Component Sanitization
FY 2013

ND 100-29 CHANGE LOG

Revision	Date	Revised By	Pages Affected	Remarks

UNCLASSIFIED

UNCLASSIFIED

ND 100-29, NRO Information Systems Media and Component Sanitization
FY 2013

SECTION I - INTRODUCTION

In accordance with the National Reconnaissance Office (NRO) Governance Plan this NRO Directive (ND) defines the scope, authorities, and responsibilities specific to NRO Business Function (NBF) 100, Security and Counterintelligence. The ND is coordinated with appropriate stakeholders, and is approved by the NBF owner, with administrative approval of the Director, Office of Policy and Strategy (OP&S). Official record copies are archived by OP&S.

SECTION II - APPLICATION

All NRO personnel who perform tasks or have duties specific to NBF 50, Information Technology, Information Assurance, Information Management (IT-IA-IM) and NBF 100, will comply with this ND and its corresponding instructions. When the work performed under an NRO contract must comply with this directive and corresponding instructions, the program office shall list these as reference documents in the contract statement of work and related documentation.

This Directive provides guidance for the sanitization and destruction of NRO information systems (IS) storage media¹ and components processing sensitive or classified information. Information processed on these devices may range from UNCLASSIFIED to TOP SECRET, and may include compartmented, sensitive, personally identifiable, and limited-distribution material.

Data remanence is the residual physical representation of data that remains after attempts have been made to remove or erase the data. This residue may result from data being left intact by a nominal file deletion operation, by reformatting of storage media that does not remove data previously written to the media, or through physical properties that allow previously written data to be recovered. Data remanence may make disclosure of sensitive information possible should the storage media or device be released into an uncontrolled environment (e.g., thrown in the trash, or released to a third party).

This ND supersedes and rescinds the following:

¹Storage media is considered to be any component of a system or media that, by design, is capable of retaining information.

UNCLASSIFIED

UNCLASSIFIED

**ND 100-29, NRO Information Systems Media and Component Sanitization
FY 2013**

NRO Instruction 50-10a, Clearing, Sanitization, and Destruction of Information System Components, 5 March 2004

SECTION III - REFERENCES/AUTHORITIES

The following documents, or their successors, are referred to completely or in part within this ND.

a. Memorandum of Agreement Between the Secretary of Defense and the Director of National Intelligence Concerning the National Reconnaissance Office, 21 September 2010

b. Intelligence Community Directive 503, *"IC IT Systems Security Risk Management, Certification and Accreditation,"* 15 September 2008

c. National Security Agency/Central Security Service Policy Manual 9-12, *"NSA/CSS Storage Device Declassification Manual,"* December 2007

d. National Institute of Standards and Technology Special Publication 800-88, *"Guidelines for Media Sanitization,"* 11 September 2006

e. NRO Business Function 50, IT-IA-IM, 3 April 2012

f. NRO Business Function 100, Security and Counterintelligence, 3 April 2012

g. NRO Directive 100-31, Media Protection Controls for NRO Information Systems, 3 April 2013

SECTION IV - POLICY

It is imperative that all persons responsible for the secure handling of sensitive or classified IS storage media and devices be aware of the retentive properties, the known risks in attempting to erase the information, and the security procedures that will help prevent unauthorized or inadvertent disclosure of sensitive or classified data.

Storage media and devices shall be safeguarded in the manner prescribed for the highest classification of the information ever processed by the IS until they are subjected to an approved sanitization² procedure. Methods to counter data remanence include overwriting, degaussing and physical

² The removal of sensitive data to ensure it may not be reconstructed.

UNCLASSIFIED

UNCLASSIFIED

**ND 100-29, NRO Information Systems Media and Component Sanitization
FY 2013**

destruction. The method required depends upon the intended subsequent use of the media or device as described in NRO Instruction (NI) 100-29-1, *NRO Information Systems Media Sanitization* or NI 100-29-2, *NRO Information Systems Component Excess and Sanitization*.

Media containing NRO sensitive or classified information shall be sanitized in a manner that will prevent (data) reconstruction/reutilization. Persons (e.g., Information System Security Officers (ISSOs)) appropriately trained to verify data categorization and sanitization shall conduct or oversee the sanitization procedures and administratively verify and account for each item.

There are three methods of sanitization, the choice of which depends upon the intended subsequent use of the media or device as described in NI 100-29-1 or NI 100-29-2:

1. Clearing: Removing data from media so that the data cannot be retrieved through a robust keyboard attack. Simple deletion of files does not suffice as clearing. *Example: overwriting.*

2. Purging: Removing data from media so that the data cannot be retrieved through a laboratory attack. *Example: degaussing.*

3. Destroying: Rendering the media unable to be reused as originally intended. *Example: shredding.*

To protect classified or sensitive information from unauthorized disclosure, media and devices containing such information shall be sanitized prior to reuse or disposition (e.g., disposal or recycling, return of leased media to the owner, or return of defective or inoperable media for repair or replacement).

NOTE: Magnetic media (e.g., Hard Disk Drive (HDD)) may only be reused at the same or higher classification level within the NRO. Electronic media may be reused with ISSO approval after proper sanitization and verification. Optical media shall never be reused.

Sanitization also requires the removal of all labels and classification/control markings.

UNCLASSIFIED

UNCLASSIFIED

**ND 100-29, NRO Information Systems Media and Component Sanitization
FY 2013**

National Security Agency (NSA) Central Security Service (CSS) Storage Device Declassification Manual (reference d) and Institute of Standards and Technology (NIST) Special Publication 800-88, *Guidelines for Media Sanitization* (reference e), apply to NRO media and devices containing classified or sensitive information and provides guidelines for the sanitizing media, including:

- a. Magnetic disks (e.g., floppies, hard drives, memory sticks with hard disks, and zip drives).
- b. Magnetic tapes (e.g., reel and cassette format).
- c. Magnetic cards (e.g., swipe cards).
- d. Optical disks (e.g., CDs, DVDs, Blu-Ray).
- e. Memory (e.g., flash drives, thumb drives, solid-state drives (SSD), DRAM, PROM).
- f. Hard copy (e.g., paper and microfilm).
- g. Networking devices such as routers.
- h. Handheld devices such as cell phones, smart phones, and personal digital assistants (PDA).
- i. Equipment (e.g., copiers, printers, monitors, and fax machines).

NRO components shall develop local standard operating procedures (SOPs) for sanitization based upon this Directive and local availability of equipment and capabilities. The SOPs shall address:

- a. Verification of the impact categorization (i.e., LOW, MODERATE, or HIGH) for the overall IS confidentiality and information processed on the media or device in accordance with NRO Information Enterprise Management Online (NIEMO).
- b. A determination of disposition of the media or device (e.g., will be disposed of, reused within the organization, or sent outside the organization).
- c. Sanitization options (refer to Table A-1 in NIST SP 800-88 and specific vendor Letters of Volatility (LoVs)).

UNCLASSIFIED

UNCLASSIFIED

**ND 100-29, NRO Information Systems Media and Component Sanitization
FY 2013**

d. Verification and documentation of the sanitization using NP Form 4-05, *Property Turn-In Request*.

Any request for deviation from the guidelines prescribed in NSA/CSS 9-12 or NIST 800-88 shall be directed to the Office of Security and Counterintelligence (OS&CI) [redacted]

(b)(3)

If required, sensitive media may also be securely shipped to non-NRO facilities for sanitization. For example, the NSA may accept classified and/or sensitive media for destruction. For more information and requirements for the NSA facility, contact NSA Classified Material Conversion Customer Service at [redacted]

(b)(3) 50
USC + 3605

SECTION V - ROLES AND RESPONSIBILITIES

OS&CI shall:

a. Provide oversight of the NIE information system media and device sanitization policy.

b. Publish and maintain policy guidelines for the safeguarding of NRO information to prevent disclosure (inadvertently or through insider actions) associated with media and device sanitization.

Information System Security Managers (ISSMs) shall:

a. Maintain the responsibility for the security of all information systems and media assigned to the organization under his/her purview.

b. Develop and implement media sanitization SOPs for storage media and devices to be disposed of, reused, recycled, returned to owner, or returned for repair or replacement.

c. Establish verification and review procedures for sanitized media and devices having processed NRO classified or sensitive information.

d. Maintain a record of equipment release (NP Form 4-05) indicating the procedure used for sanitization and date of release to the equipment custodian. The record shall be retained for two (2) years.

Information System Security Officers (ISSOs) shall:

UNCLASSIFIED

**ND 100-29, NRO Information Systems Media and Component Sanitization
FY 2013**

- a. Ensure sanitization requirements are addressed in System Security Plans (SSPs) and Standard Operating Procedures (SOPs).
- b. Verify that media and devices are properly sanitized before release.
- c. Verify that leased storage media and devices are properly sanitized before they are returned to the owner.
- d. Verify that defective or inoperable storage media and devices are properly sanitized before they are returned to the vendor or manufacturer for repair or replacement.
- e. Verify that defective or inoperable storage media and devices, not being returned to vendors or manufacturers that cannot be sanitized, are physically destroyed.
- f. Ensure periodic testing of sanitization equipment (e.g., degaussers, shredders, etc.) to ensure proper operation.

Program Security Officers (PSOs) shall resolve any classification issues prior to media/device sanitization.

Users shall:

- a. Ensure the proper safeguarding of classified and sensitive storage media in accordance with NRO Directive 100-31, *Media Protection Controls for NRO Information Systems*.
- b. Notify ISSO and PSO when media or devices processing classified or sensitive information are no longer required.

SECTION VI - DIRECTIVE POINT OF CONTACT

OS&CI,


(b)(3)

UNCLASSIFIED

ND 100-29, NRO Information Systems Media and Component Sanitization
FY 2013


APPROVING SIGNATURE

As the NBF owner for NBF 100, Security and Counterintelligence, I confirm that this document provides a complete representation of the ND 100-29, NRO Information Systems Media and Component Sanitization and the document has been coordinated with stakeholders in this process.



A. Jamieson Burnett
Security and Counterintelligence,
NBF Owner

3 APR 2013
Date



Damon R. Wells
Director, Office of
Policy and Strategy

3 APR 2013
Date

UNCLASSIFIED

UNCLASSIFIED

ND 100-29, NRO Information Systems Media and Component Sanitization
FY 2013

APPENDIX - GLOSSARY and ACRONYM LIST

Term and Acronym	Definition
CSS	Central Security Service
Degauss	In the context of information systems security, used to denote one of two meanings: Reduce the magnetization of a storage device to zero by applying a reverse (coercive) magnetizing force, commonly referred to as demagnetizing, or reduce the correlation between previous and present data to a point that there is no known technique for recovery of the previous data.
Destruction (Media)	The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible to recover or prohibitively expensive.
High Impact	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
IS	Information System
ISSO	Information System Security Officer
LoV	Vendor Letter of Volatility. A specialized letter issued by manufacturers of electronic devices that states the capabilities of the on-board memory devices of an individual product. It is primarily used with concern to the security requirements of companies working with very sensitive information. The purpose is to state what the capabilities of the on-board memory devices are. Letters of Volatility can usually be obtained by contacting the manufacturer of the product.
Low Impact	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
Moderate Impact	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
NBF	NRO Business Function
ND	NRO Directive
NI	NRO Instruction
NIE	NRO Information Enterprise

UNCLASSIFIED

UNCLASSIFIED

ND 100-29, NRO Information Systems Media and Component Sanitization
FY 2013

Term and Acronym	Definition
NIST	National Institute of Standards and Technology
Non-Volatile Memory	Devices that retain stored information when power is removed. Examples include magnetic media, optical disks, and certain solid state media.
NRO	National Reconnaissance Office
NSA	National Security Agency
OP&S	Office of Policy and Strategy
OS&CI	Office of Security and Counterintelligence
Overwriting	A software process that replaces data previously stored on storage media with a predetermined set of meaningless data.
PSO	Program Security Officer
Purging	The removal of sensitive data from an information system, its storage devices, and other peripheral devices by erasure, overwriting of storage, or resetting of registers to ensure that data may not be reconstructed.
Sanitization	The removal of information from the media or equipment such that data recovery using any known technique or analysis is prevented. Sanitizing shall include the removal of data from the media, as well as the removal of all classified labels, markings, and activity logs.
Sensitive Information	Information which if lost, misused, modified or allowed unauthorized access can adversely affect the privacy or welfare of an individual, proprietary information of a business or even the security, internal and foreign affairs of a nation depending on the level of sensitivity and nature of the information.
SOPs	Standard Operating Procedures. Written procedures created to provide specific documentation for various, usually highly technical, processes.
SSP	System Security Plan
Storage Media	Referring to computer components and recording media that retain analogue or digital data. Data storage is a core function and fundamental component of computers. Storage media includes memory devices in computers (hard drives) and any removable/transportable memory medium, such as magnetic tape or disk, optical disk, or digital memory card.

UNCLASSIFIED