National Reconnaissance Office

Business Function 100, Security and Counterintelligence
Directive 100-29, NRO Information Systems Media and Component Sanitization Policy

Instruction 100-29-1, NRO Information Systems Media 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.

TABLE OF CONTENTS

NI 100-29-1 CHANGE LOG.................................... 3

SECTION I - INTRODUCTION.................................... 4

SECTION II - NRO INFORMATION SYSTEM MEDIA SANITIZATION DOCUMENTATION.................................... 4

Governing NBF.................................... 4

Description.................................... 4

Instruction Point of Contact.................................... 6

Support Systems.................................... 6

Process Narrative for Media Sanitization.................................... 7

Process Flow Diagram for Media Sanitization.................................... 9

Table 1: Risk & Internal Control Table.................................... 10

SECTION III - CONFIGURATION CONTROL.................................... 11

APPROVING SIGNATURE.................................... 11

APPENDIX A - PROCESS FLOW DIAGRAM LEGEND.................................... 12

APPENDIX B - GLOSSARY and ACRONYM LIST.................................... 13

APPENDIX C - REFERENCES/AUTHORITIES.................................... 16

NI 100-29-1 CHANGE LOG

Revision	Date	Revised By	Pages Affected	Remarks

SECTION I - INTRODUCTION

In accordance with the National Reconnaissance Office (NRO) Governance Plan, the NRO Business Function (NBF) 100, Security and Counterintelligence and NRO Directive (ND) 100-29, NRO Information Systems Media and Component Sanitization, this instruction sets forth the procedural implementation guidance and provides applicable information to perform the NRO information system media sanitization process. All NRO personnel who perform tasks or have duties specific to media sanitization will comply with this NRO Instruction (NI). When the work to be performed under an NRO contract must comply with this instruction, the program office shall list this instruction as a reference document in the contract statement of work and related documentation.

This NI supersedes and rescinds the following:

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

SECTION II - NRO INFORMATION SYSTEM MEDIA SANITIZATION DOCUMENTATION

The sub-sections that follow detail the Media Sanitization processes.

Governing NBF

NBF 100, Security and Counterintelligence, 3 April 2012.

Description

The NRO captures, processes, and stores information using a wide variety of data storage media. This information must be protected from creation-to-disposal in a manner that is appropriate to the sensitivity and highest classification level of the information contained on the media. When organizations and individuals discard storage media and devices, proper techniques shall be used to remove the data, or destroy the media, to protect the confidentiality of NRO information.

Media sanitization is the process of removing data from storage media, with reasonable assurance that the data cannot be retrieved and/or reconstructed. Data that has been improperly or unsuccessfully removed (i.e., data remanence) from media could be recreated by unauthorized individuals. All of the residual physical, magnetic, optical, or electrical representation of data that has been deleted from the media shall be highly improbable, if not impossible, to recover.

NRO activities will comply with Security Agency (NSA) Central Security Service (CSS) Storage Device Declassification Manual and guidance from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, *Guidelines for Media Sanitization*, together with local Standard Operating Procedures (SOPs), to enable security professionals to make effective, risk-based decisions for the proper sanitization of the information recorded on the media and for its disposal.

All questions regarding proper sanitization or release procedures may be directed to the Office of Security and Counterintelligence (OS&CI), [redacted] (b)(3)

Two Primary Types of Media

1. Hard copy media: Physical representations of information, such as paper printouts, printers and facsimile ribbons, drums, and platens.

2. Electronic media: The bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices (volatile and non-volatile), phones, mobile computing devices, networking equipment, and many other types of electronic equipment.

Media types will change as technology changes. However, the process for media sanitization should always focus on protecting the information that is recorded on the media.

NSA/CSS 9-12 and NIST SP 800-88 outline available sanitization methods for the different types of media, and provides information on the minimum recommended sanitization techniques for removing data and disposing of media.

Methods for Media Sanitization

An important criterion to consider when deciding on the best method of sanitization is the overall risk categorization of the data on the information system (IS) (e.g., LOW, MODERATE, or HIGH). This system data categorization can be found in NRO Information Enterprise Management Online (NIEMO).

After the IS categorization has been determined by referencing NIEMO, determine the nature of the medium on which the information is recorded (i.e., magnetic, optical, electronic), determine the disposition of the media (i.e., reuse, destroy, transfer out of NRO control), and decide on the appropriate process for sanitization.

Sanitization Resources

Equipment used for NRO media destruction must be evaluated to measure effectiveness if not previously evaluated by an NRO-recognized entity. The NSA maintains an unclassified (UMIS-accessible) webpage for media destruction evaluated product listings. The following is a list of resources available:

a. http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml, Media Destruction Guidance

b. http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS-EPL-02-01-AC.pdf, NSA/CSS Evaluated Products List for High Security Crosscut Shredders, 1 September 2011

c. http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS-EPL-04-01.pdf, NSA/CSS Evaluated Product List for Punched Tape Destruction Devices, Version C, 29 July 2005

d. http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_EPL_04-02-K.pdf, NSA/CSS Evaluated Product List for Optical Media Destruction Devices, 1 September 2011

e. http://www.nsa.gov/ia/_files/government/MDG/EPL-Degausser25February2010.pdf, NSA/CSS Evaluated Products List - Degausser, 25 February 2010

f. http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf, NSA/CSS Storage Device Declassification Manual (SDDM), December 2007

g. http://www.nsa.gov/ia/_files/Government/MDG/NSA_CSS_EPL_02_02_P.pdf, NSA/CSS Evaluated Products List (EPL) for High-Security Disintegrators, Version P, 31 January 2012

Instruction Point of Contact

OS&CI [redacted] (b)(3)

Support Systems

All NRO Information Systems.

Process Narrative for Media Sanitization

1.0 Assess the sensitivity category of the stored data per NIEMO.

1.1 The Program Security Officer (PSO) and/or Information System Security Officer (ISSO) can assist with assessing the data categorization based on data present, data once stored, or data processed based on the categorization level of the system (i.e., LOW, MODERATE, or HIGH).

2.0 Determine whether the media will be reused or destroyed.

3.0 Determine if media will leave organizational control.

NOTE: Complex systems such as servers, server systems, robust storage systems, and scientific instruments pose significant challenges for sanitization. Provision for these types of systems must be made for equipment returned to manufacturers or sent for repair and included in the local SOP.

NOTE: ISSOs with servers, server systems and more complex storage assets such as RAID arrays and computer-based scientific instruments (e.g., test equipment) should be familiar with the vendor Letters of Volatility (LoVs) and follow NSA and NIST recommendations and procedures for effective media sanitization and disposition.

NOTE: Storage media assets returned to a vendor for warranty service, replacement, or sent to an external party for repair should be fully sanitized to prevent data reconstruction, unless an agreement covering data handling responsibilities is in place in accordance with ND 100-31, *Media Protection Controls for NRO Information Systems*. If sanitization is necessary, but impossible, without physically destroying the storage media, arrangements should be made to conduct repairs on-site if possible, otherwise an agreement for data handling and secure transport is required.

4.0 Determine the appropriate sanitization method per local equipment availability and capability as documented in the SOP.

NOTE: The sanitization process is critical to ensuring the protection of NRO data. Proper techniques, whether clearing (e.g., overwriting), purging (e.g., degaussing), or destroying (e.g., shredding) afford the NRO with the assurance that data is removed from the media and the risk of compromise is mitigated.

4.1 Clear the media by deleting information using methods that prevent retrieval of data by disk or file recovery utilities, and that resist keystroke recovery attempts. Overwriting is an acceptable method for clearing media and protecting the confidentiality of the information which allows the media to be reused within the NRO (e.g., an equivalent or higher security environment). Clearing **does not** allow reuse of media at a lower classification level, from SCI handling to collateral levels, or the release out of NRO control without ISSO approval. The logical storage location of data, such as the file allocation table, as well as all addressable locations shall be overwritten, replacing the original data with random data. Overwriting cannot be used for media that are damaged (hard disks with bad or inaccessible tracks) or that are not suitable for overwriting (e.g., optical media).

4.2 Purging the media protects the confidentiality of information against laboratory attack, such as the use of signal processing equipment. Degaussing is a purging method that exposes magnetic media to a strong magnetic field to disrupt the recorded magnetic domains. Degaussing can be an effective method for purging damaged media, media with exceptionally large storage capacities, or for quickly purging diskettes. Degaussing cannot be used to purge nonmagnetic media, such as CDs and DVDs, or semi-conductor data storage and memory devices. Additionally, degaussing may damage internal magnetic hard disk mechanisms beyond repair.

NOTE: Purging is not a substitute for terminal destruction. Media must be purged prior to terminal destruction.

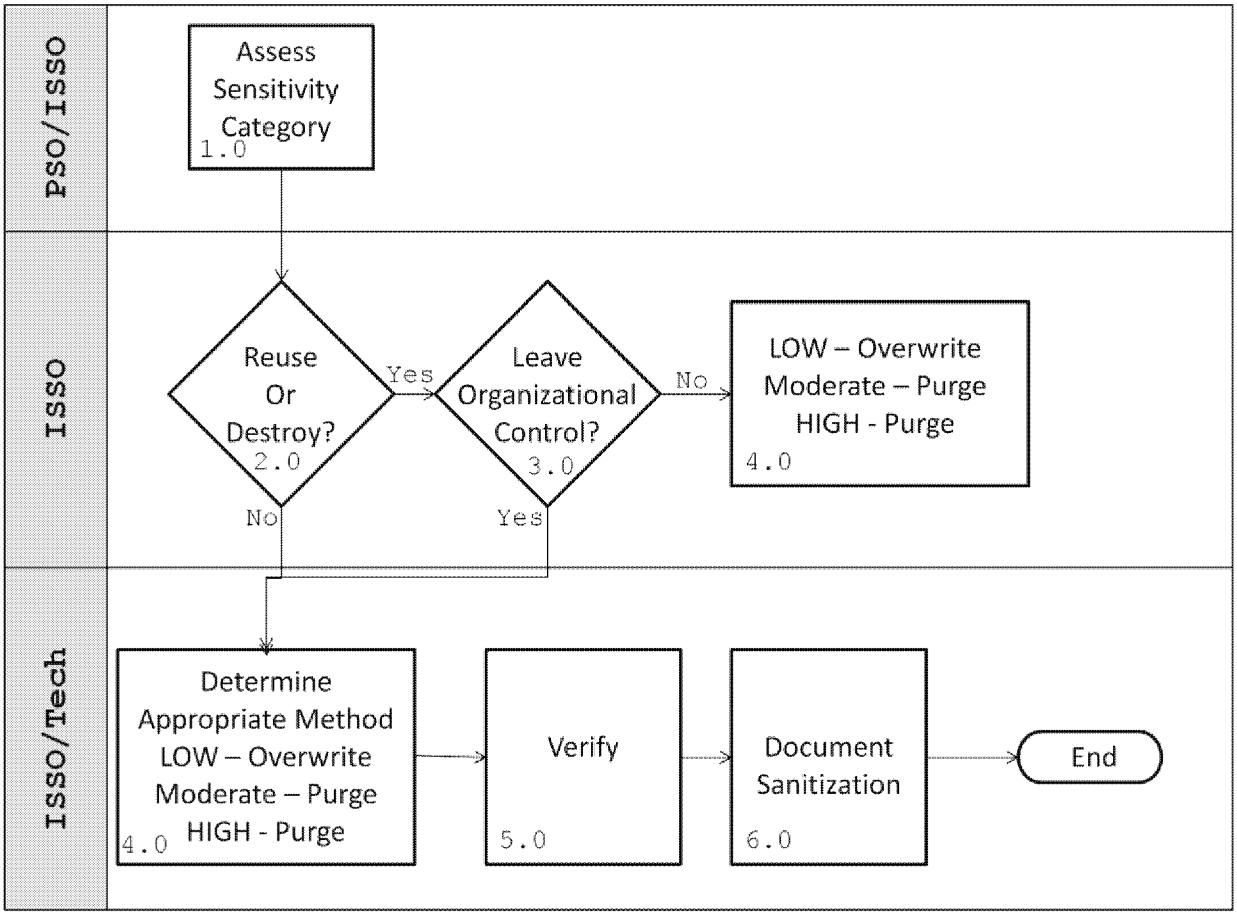
4.3 Destroying media prevents its reuse. Destruction techniques include disintegration, incineration, pulverization, and melting of the media. Paper and flexible diskettes that have been removed from their outer containers can be shredded to an appropriate shred size (refer to NIST SP 800-88) so that the information cannot be reconstructed. Sanding the media by applying an abrasive tool or treating the surface with chemicals can also be used to completely remove the media recording surface. Optical mass storage media, including CDs and DVDs, must be destroyed by burning, pulverizing, crosscut shredding or grinding (CDs only) the information-bearing surface. These processes should be carried out by trained and authorized personnel with appropriate equipment at an appropriate facility. All magnetic and non-magnetic media shall be purged prior to destruction - degaussed or overwritten, respectfully.

NOTE: All formerly classified media must be destroyed prior to release to unclassified environment unless explicitly approved by the ISSO.

5.0 Verification of sanitization by cognizant security official via NRO Form NP 4-05, *Property Turn-In Request*.

6.0 A record of what media were sanitized, when and how they were sanitized, and the final disposition of the media shall be maintained for a minimum of two (2) years in accordance with the NRO *Records Control Schedule*.

Process Flow Diagram for Media Sanitization



Anti-Compromise Emergency Destruction

Emergency situations present a very different condition in which to safeguard IS and data from compromise. In such cases, the primary objective is the safety of the personnel and then the destruction of or denial of access to sensitive or classified information. [redacted]

(b)(3)

For additional information, the NSA has compiled a set of video instructions outlining acceptable methods for emergency destruction. On NMIS, these can be viewed at: [redacted]

(b)(3) 50 USC 3605
(b)(3) 10 USC 424

Table 1: Risk & Internal Control Table

Risk	Internal Control
IS storage medium containing sensitive/classified information must be sanitized before it is disposed of, reused, recycled, or returned to the owner or manufacturer to prevent compromise.	The organization sanitizes information system media using approved equipment, techniques, and procedures.
Records of the sanitization and disposition of IS storage media must be maintained for administrative purposes.	The organization tracks, documents, and verifies media sanitization actions.

Periodic testing of degaussing/destruction equipment will verify it is functioning properly.	The organization ensures periodic testing of sanitization equipment/procedures to ensure proper performance.

SECTION III - CONFIGURATION CONTROL

All changes to NI 100-29-1, NRO Information Systems Media Sanitization Instruction require the NBF owner approval.

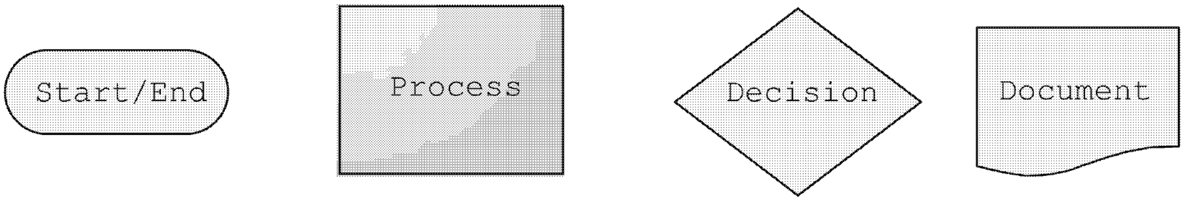
APPROVING SIGNATURE

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

A. Jamieson Burnett
Security and Counterintelligence,
NBF Owner

3 APR 2013
Date

APPENDIX A - PROCESS FLOW DIAGRAM LEGEND



APPENDIX B - GLOSSARY and ACRONYM LIST

Term and Acronym	Definition
CSS	Central Security Service
Clearing	The process of removing any data stored on storage media prior to the media's reuse at the same classification level.
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.
Degausser	An electrical device or hand-held permanent magnet assembly which generates a coercive magnetic force for the purpose of degaussing magnetic storage media or other magnetic material.
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.

Term and Acronym	Definition
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.
NSA	National Security Agency
NBF	NRO Business Function
ND	NRO Directive
NIE	NRO Information Enterprise
NIEMO	NRO Information Enterprise Management Online
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.

Term and Acronym	**Definition**
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.
Volatile Memory	Devices that do not retain stored information when power is removed. Examples include DRAMs and SRAMs.

APPENDIX C - REFERENCES/AUTHORITIES

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

b. National Security Agency/Central Security Service Storage Device Declassification Manual, December 2007

c. NRO Governance Plan, 25 October 2011

d. NBF 100, Security and Counterintelligence, 3 April 2012

e. ND 100-29, NRO Information Systems Media and Component Sanitization, 3 April 2013