

Guideline for Media Sanitization
NIST DRAFT SPECIAL PUBLICATION
800-88

Computer Security Division
Information Technology Laboratory

Presentation Overview

- Why do sanitization?
- What is sanitization?
- How to do sanitization?

FISMA Legislation

Overview

“Each federal agency shall develop, document, and implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source...”

-- **Federal Information Security Management Act of 2002**

Minimum Security Requirements

FISMA Requirement

- Develop minimum information security requirements for information and information systems in each security category defined in FIPS 199
- Publication status:
 - ✓ Federal Information Processing Standards (FIPS) Publication 200, “Minimum Security Requirements for Federal Information and Information Systems”
 - ✓ Final Publication: **December 2005**

Categorization Standards

FISMA Requirement

- Develop standards to be used by federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels
- Publication status:
 - ✓ Federal Information Processing Standards (FIPS) Publication 199, “Standards for Security Categorization of Federal Information and Information Systems”
 - ✓ Final Publication: **February 2004**

FIPS 199

- Evaluate a system based on the impact of loss of the following:
 - Availability
 - Integrity
 - Confidentiality

Minimum Security Controls

- Develop minimum security controls (management, operational, and technical) to meet the minimum security requirements in FIPS 200
- Publication status:
 - ✓ NIST Special Publication 800-53, “Recommended Security Controls for Federal Information Systems”
 - ✓ Final Publication: **February 2005**

Sources of Information

- Department of Defense
- National Security Agency
- University Centers for Magnetic Recording Research
- Vendors

What is sanitization?

- **Dispose:** (not really sanitized) Just tossed away.
- **Clear:** Resistant to keyboard attacks.
- **Purge:** Resistant to laboratory attacks.
- **Destroy:** Resistant to recreation of media

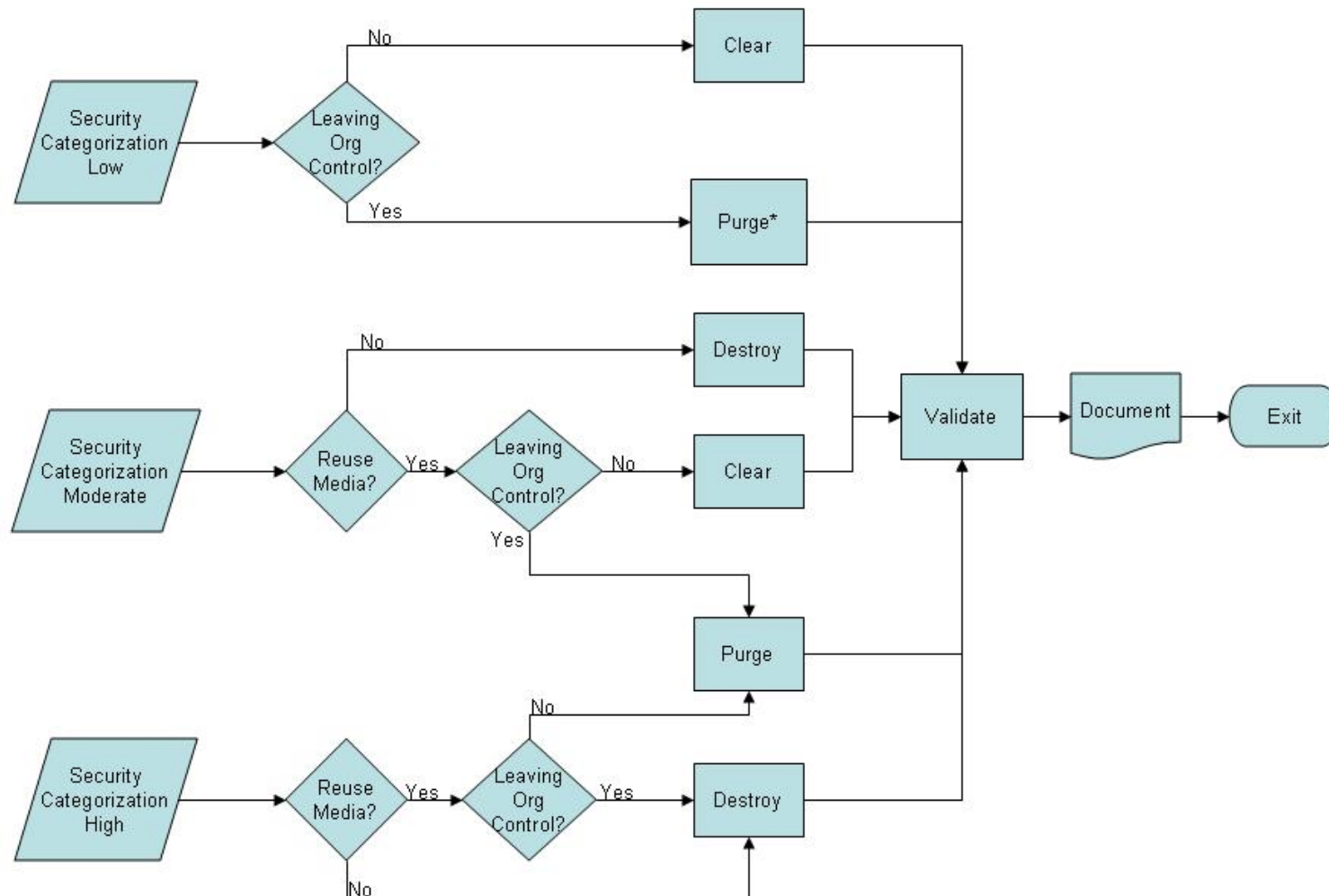
Don't re-do if working

- Guidance is not intended to replace a sanitization program that is:
 - Effective
 - Operational
 - Compliant with FIPS 200 and satisfies SP 800-53 and 800-53A.

How to do it?

- **Identify your media and know your information.**
- **Decide on a sanitization method.**
- **Find supportive tools.**
- **Validate your tools/policies/procedures.**
- **Share your findings.**

Take a graduated approach



What is reasonable?

- Don't degauss the paper or spend \$5K to sanitize a \$50 hard drive.
- Scale it up for ease, risk, resources.
- Make cost effective risk based decisions weighing environmental factors that may be unique to your agency.

Know What Information Is Where

- What media are you using across your agency. Is there non agency media on your systems?
- What information is on that media.
- What information is not on media.
- Loose control of your information locations, loose control of your sanitization.

Not all information is categorized

- Many other forms of information exists that is not associated with a categorized system. This information may be just as important for sanitization.

Assign labels to your information

- The ‘other than system’ related information needs to be categorized in accordance with local policy.
- “For public release”
- “For internal use only”
- “For HR only”

Make a decision regarding how to sanitize your media.

- Low
- Moderate
- High
- Internal Label
- Dispose
- Clear
- Purge
- Destroy

Share your discoveries

Address  <http://csrc.nist.gov/fasp/>

Information Technology Laboratory
Computer Security Division (CSD) &

Computer Security
Resource Center
(CSRC)

NIST
National Institute of
Standards and Technology

Federal Agency Security Practices

Federal Computer Security Program Manager's Forum

[Search FASP site](#)

[HOME](#)

[FASP Areas](#)

[Pilot BSPs](#)

[FAQ](#)

[Submit FASP](#)

[Public/Private
Security Practices](#)

[Checklists /
Implementation
Guides](#)

[Federal Computer
Security Program
Managers' Forum](#)

[Points of Contacts](#)

Disclaimer Notice &
Privacy Policy /
Security Notice
Send comments or
suggestions to
[webmaster-
csrc@nist.gov](mailto:webmaster-csrc@nist.gov)
NIST is an Agency of
the U.S. Commerce

WELCOME to the Federal Agency Security Practices (FASP) web site. The FASP effort was initiated as a result of the success of the Federal CIO Council's Federal Best Security Practices (BSP) pilot effort to identify, evaluate, and disseminate best practices for CIP and security. NIST's Computer Security Division was asked to undertake the transition of this pilot effort to an operational program. As a result, NIST developed this web site. The FASP site contains agency policies, procedures and practices; the CIO pilot BSPs; and, a Frequently-Asked-Questions (FAQ) section. The FASP site differs from the BSP pilot in material provided and in complexity.

The FASP area contains a list of categories found in many of the NIST Special Publications. Based on these categories, agencies are encouraged to share their information technology (IT) security information and IT security practices and submit them for posting on the FASP site. Any information on position descriptions for security positions and statements of work for contracting security-related activities are also encouraged. Procedures for submission of FASPs can be found on the "Submit FASP" web page.

The Pilot BSPs are listed separately and appear in their original format. They have also been incorporated into the FASP areas listing.

The FAQ section is comprised of exchanges and questions on computer security related issues between the members of the Federal Computer Security Program Managers' Forum.



With the support of the Federal Computer Security Program Managers' Forum, NIST offer this information sharing and collaborative endeavor as an educational resource for Federal security professionals. We solicit your participation and welcome your comments and suggestions.

DISCLAIMER

NIST has designed this web site primarily as an educational resource for Federal security professionals. NIST makes no claim that use of the security practices will assure a successful outcome. Each Federal security professional should apply his or her own professional judgment when using a security practice.

Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

Share your thoughts.

Address  http://csrc.nist.gov/publications/drafts.html 

Computer Security Division :
Computer Security Resource Center (CSRC)

Information Technology Laboratory

NIST
National Institute of Standards and Technology

Focus Areas | **Publications** | **Advisories** | **Events** | **Site Map**

[CSRC Homepage](#)
[CSRC Site Map](#)

Search CSRC:

CSD Publications:
- [Draft Publications](#)
- [Special Publications](#)
- [FIPS Pubs](#)
- [ITL Security Bulletins](#)
- [NIST IRs](#)

Draft Publications

Computer Security Resource Center - CSD

Having trouble viewing a .pdf document on this page? [Click link for details.](#)

Would you like to receive e-mail notification(s) when NIST releases new security publications? [Click here to learn more about it and how to subscribe to this list.](#)

- **December 16, 2005: Draft Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators**
[Adobe PDF](#) (1,342 KB)

A draft NIST Special Publication (Draft SP 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators) is available for comment. Comments should be submitted to [Elaine Barker](#) by Wednesday, February 1, 2006. Please place "Comments on SP 800-90" in the subject line.

Don't forget the following:

- Property management
- Privacy Officers
- FOIA Office
- Management Continuity
- Back ups

Why, What, How

- Do it because:
 - Its required
 - It reduces risk of unauthorized disclosure
- Clear it, purge it, destroy it = control it.
- Identify your media, your information, your tolerance for risk. Make a decision.

Contact Information

**100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930**

Matthew Scholl

(301) 975 2941

mscholl@nist.gov