Technical Reference Document

Summary of NIST Special Publication 800-88:

Guidelines for Media Sanitization

• Recommendations of the National Institute of Standards and Technology

DESTRUCTDATA, INC. 12 Rogers Rd. Unit 8 Haverhill, MA 01835 Toll Free: 800-781-4799 www.destructdata.com

Summary of NIST Special Publication 800-88

Guidelines for Media Sanitization

Recommendations of the National Institute of Standards and Technology

INTRO REVISION 1:

Issued in 2006, NIST Special Publication 800-88 has become the defacto guideline for electronic media sanitization. The original 43 page publication has been expanded to 57 pages in Revision 1; while the structure of the document is essentially the same, three areas have key additions or expansions:

Section 2.3 Trends In Storage Methods and *Section 2.4 Trends in Sanitization:* notes the revolutionary effect of flash storage technology (SSD) and the increasing complexity of determining sanitization methods.

Section 4.7 Verification Methods / 4.8 Documentation: in general, the need to implement independent verification of sanitized media, including the deployment of a validation too different from that used for the data wipe. Summary reviews possible approaches (see page 4).

Appendix A Minimum Sanitization Recommendations: expanded to 9 tables and includes media not considered relevant in 2006, especially SSDs, iPhones, Android powered devices and other mobile devices.

BEGIN SUMMARY

Sanitization is the process of removing data from a hard drive, CD-ROM or other electronic media, generally at the end of the data's life cycle. Special Publication 800-88 provides guidelines for establishing a program for the sanitization of hard drives and other electronic media. It recommends a number of methods for sanitizing various storage media and verifying the process. The life cycle of a physical HDD or other media storage device is a separate topic, but one often directly related to and affected by the data disposal policy.

The data disposal methods cited include *physical destruction*, *degaussing* (magnetic) and *non-destructive (erasing)* solutions (explained below). The NIST document also provides guidance for how to match destruction technologies with specific security, business and environmental requirements. The key to the guidelines is not that they identify the most secure technologies, but that they offer a range of possibilities that can be matched with data confidentiality, risk, cost, scale etc. They should be regarded as sound recommendations based on scientific testing and not as rigid industry standards. While a typical audience might be a CIO or privacy officer seeking to establish a data protection program, the material is relatively easy to understand for non-professionals. It can therefore provide guidance to anyone seeking to sanitize electronic data.

Special Publication 800-88 is also an excellent resource for organizations and system owners in the process of developing overall privacy protection programs, as mandated in most recent privacy legislation. It has become the de facto reference for privacy professionals undertaking to comply with federal and state regulations regarding the disposal of end-of-life (non-classified) electronic data.

This DestructData, Inc. summary of original NIST publication report provides a "thumbnail" version of the essential information found in the revised 57 page document. Appendix A, *Minimum Sanitization Recommendation for Media Containing Data*, encapsulates the core concepts of the original NIST publication and is reproduced in part at the end of this document. The matrix provides a context for the practical product and policy choices a complete program will require.

Sidebar 1: Background

What is NIST and the Information Technology Laboratory?

The National Institute for Standards and Technology (NIST) is responsible for developing best practices and guidelines, including minimum requirements, for implementing adequate information security in all federal agency operations and assets. However, these standards do not apply to national security systems. The Information Technology Lab's (ITL) functions include developing technical, physical, administrative, and management standards and guidelines for cost effective security and privacy of sensitive unclassified information in Federal computer systems.

Section 1: Introduction

Sanitization refers to the general process of removing data from hard drives, CD-ROMS or other storage media so that data may not be easily retrieved and reconstructed. When storage media is transferred, becomes obsolete, or is no longer usable or required by an information system, it is important to ensure that residual magnetic, optical, or electrical data is not easily recoverable. The increased use of encryption within IT infrastructures may actually make electronic storage media more attractive to data thieves.

All data disposal practices should first determine that information is captured and maintained as required by business and regulatory needs. Furthermore, this process should be ongoing, as controls need to be adjusted when conditions change.

Section 2: Background

Critical factors affecting information disposition and media sanitization should be determined at the start of a system's development. While disposal of data is most likely to occur at the end of the data life cycle, it may be required any time a storage device leaves the control of the organization. This may be for maintenance reasons, system upgrades, or during a tech refresh.

First categorize the information and consider the level of confidentiality, then assess the media on which it is stored. Any security plan for the lifespan of data should be developed in a manner that is appropriate to its security level.

Increases in track density and the corresponding changes in the storage medium have resulted in a situation where clearing and purging the media have converged.

Best practices are changing rapidly due to new types of storage media, especially flash storage as found in Solid State Drives (SSD). Degaussing, a fundamental way to sanitize magnetic media, no longer applies in most cases for flash-based devices. This change is so profound that a "reinvestigation" is in order.

Additionally, when shredders or other physical destruction devices are used to destroy SSD drives, the particle size is reduced according to increases in storage density. This presents a serious challenge to equipment manufacturers.

NIST divides sanitization types for each type of media into three categories: *Clearing, Purging* and ***Destroying***.

The category descriptions that follow here are summations of those Table 5.1 (page 23 of original document) in the NIST original.

Clearing: Protects information against a robust keyboard attack. Deletion does not. Clearing means information can't be retrieved by data, disk or file recovery utilities, and must be resistant to keystroke recovery attempts executed from standard input devices or data scavenging tools. Overwriting is an acceptable clearing method. The goal is to replace written data with random data in logical storage locations and all other addressable locations. Clearing can't be used for media that is damaged or not writable. Media type and size should also be considered. Most modern media can be effectively cleared by one overwrite pass.

Purging: Identified as a higher security level than clearing because it protects information against a laboratory attack. A laboratory attack is more sophisticated than a keyboard attack and uses non-standard methods and tools to steal data outside of its operating environment. Although not sufficient for some media, for ATA drives manufactured after 2001, purging and clearing are now regarded as essentially the same.

Sidebar 2: Sanitization Decision Making Factors

1. What types of media storage does the organization need to be sanitized?
2. What is the confidentiality level of data stored on the media?
3. Will the media be processed in a controlled area?
4. Should the sanitization process be conducted within the organization or outsourced?
5. What is the anticipated volume of media to be sanitized by type of media?
6. What is the availability of sanitization equipment and tools?
7. What level of personnel training is required for equipment/tools?
8. How long will each sanitization process take?
9. What is the relative cost of any process when tools, training, validation, and reentering media into the supply stream is considered?

Some methods of purging (which vary by media and must be applied with considerations described further throughout this document) include overwriting, block erase, Cryptographic Erase, through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the abstraction inherent in typical read and write commands.

Degaussing is also recognized as a purge level sanitization method. Degaussing exposes a hard drive to a strong magnetic drive, which destroys the firmware that manages the drive. It renders the drive unusable. Degaussers are rated according to the type of media they can sanitize and are especially useful for purging damaged media. They are good for destroying media with exceptionally large storage capacities or for purging diskettes quickly. Not recommended for CD-ROMs and other optical media or flash memory drives such as SSD.

If purging media is not a reasonable sanitization method for organizations, this guide recommends that the media be destroyed.

Destroying: The most secure form of sanitization. Once destroyed, however, drives cannot be reused as originally intended. Physical destruction methods include disintegration, incineration, pulverizing, shredding, and melting. If a high security categorization requires destruction, the residual hard drive (or other storage media) component must be able to withstand a laboratory attack.

Disintegration, Incineration, Pulverization, and Melting: These sanitization methods are designed to completely destroy the media. They may be outsourced to qualified metal destruction or incineration facilities, or performed on-site by service providers specifically certified for this activity.

Shredding: 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 match the confidentiality level of the data.

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.

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.

Other factors in Sanitization decisions:

The cost versus benefit aspects and environmental factors related to implementation of a media sanitization process should be analyzed prior to finalizing a solution. See Sidebar 2 for additional factors.

Section 3: Roles and Responsibilities

This section lists the various personnel that should be included in the decision making and implementation of a data security program. (See Sidebar 3 for an abridged listing of specific titles and functions).

Section 4. Information Sanitization and Disposition Decision Making

The core of this section is a flow chart that visually summarizes how to think about choosing sanitization methods. The chart is based on security categorizations and guides the reader through a decision matrix that can help focus the selection process.

Sidebar 3: Roles and Responsibilities

Program Managers/Agency Heads:
Ultimate responsibility for information security governance and providing adequate resources and their deployment.

Chief Information Officer (CIO):
The "information custodian" is charged with promulgating information security policy.

Information System Owner:
Should ensure that maintenance or contractual agreements are in place and sufficient for protecting system media confidentiality.

Information Owner:
Ensures appropriate supervision of onsite media when maintenance by service providers occurs. Also responsible for making users aware of data sensitivity levels.

Senior Agency Information Security Officer (SAISO):
Responsible for ensuring information disposition policy is implemented throughout the organization.

System Security Manager/Officer:
Assists system management officials in coordinating the security efforts of a particular system.

Property Management Officer:
Responsible for ensuring that sanitized media and devices are properly accounted for.

Records Management Officer:
Responsible for advising the data owner of record retention requirements.

Privacy Officer:
Responsible for providing advice on the privacy issues.

Users:
Must understand confidentiality levels in order to assure proper handling of information.

Choosing storage media is a key decision when determining sanitization policy. Primarily an IT business decision, sanitization throughout the life cycle should be considered when selecting storage media. Many storage devices contain multiple forms of media that may require different methods of sanitization. For example, a PC may contain a hard drive, RAM, and ROM.

In order to control data and conduct timely sanitization, organizations must know which media are capturing data and when. These decisions can be as simple as ensuring placement of paper shredders in work areas or address destroying electronic equipment at the end of its life cycle.

A key decision on sanitization is whether the media will be reused or recycled. If media are not intended for reuse either within or outside an organization due to damage or other reason, the simplest and most cost-effective method of control may be destruction.

Control of Media:
A factor influencing an organizational sanitization decision is who has control and access to the media. This aspect must be considered when media leaves organizational control. Media control may be transferred when media are returned from a leasing agreement or are being donated or resold to be reused outside the organization.

Document the decision making process upon completion and ensure that a strategy and proper resources are in place to support these decisions. This process is often the most difficult aspect of media sanitization because it includes validation as an additional component. It requires documenting decisions and actions, identifying resources, and having critical interfaces with key officials.

Verification of Sanitization Results (Revision 1):
Verifying sanitization is essential. A full reading of all accessible areas to verify that the expected sanitized value is in all addressable locations should be performed if time and external factors permit.

Since full verification is almost never practical, representative sampling is advised: Three objectives should be considered:

1. When using an analysis tool, select pseudorandom locations on the media each time it is applied. This reduces the likelihood that sanitization has only worked on a subset of the media.

2. Break up the media across the addressable space and select a large enough number of subsections so that the media is well-covered. The suggested minimum number of subsections for hard drives leveraging LBA addressing is one thousand. Select at least two non-overlapping pseudorandom locations from within each subsection. Include the first and last addressable location on the storage device.

3. Each consecutive sample location (should cover at least 5% of the subsection and not overlap the other sample in the subsection. Given two non-overlapping samples, the resulting verification should cover at least 10% of the media once all subsections have had two samples taken.

Secondary Verification: A subset of storage media should be selected at random for secondary verification using a separate validation tool from a different developer. For the secondary verification, a full validation should be performed on least 20% of sanitized media. The secondary validation provides assurance that the primary operation is working as expected.

Sidebar 4: Tools and Resources

NIST APPROVAL: NIST does not conduct an evaluation of any specific product for the purpose of validating its ability to clear, purge, or destroy information contained on any specific medium. If an organization has validated a product, they are strongly encouraged to share this information through public forums, such as the Federal Agency Security Practices (FASP) website. FASP can be found at http://csrc.nist.gov/fasp/.

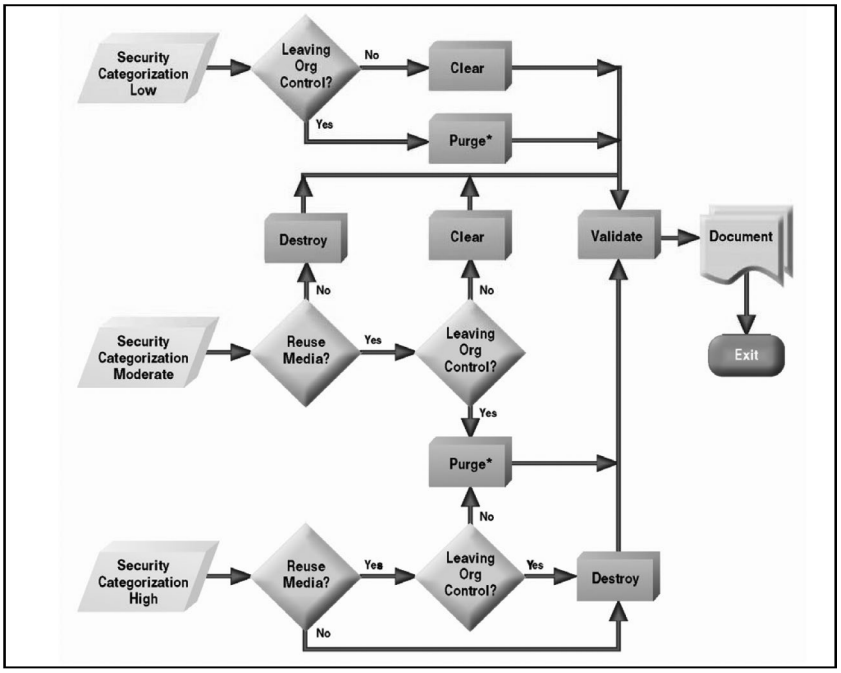
FIRMWARE PURGING: For hard drive devices or devices where firmware purge commands (Secure Erase) can be accessed and utilized, this option may be the best solution. ***Firmware purge commands can provide strong assurance of data protection while allowing the device to be reused.***

Documentation:
Inadequate record keeping can have negative consequences in the real world. Document what, when and how media are sanitized, as well as the final disposition.

Following sanitization, a certificate of media disposition -electronic or hard copy - should be completed for each piece of electronic media that has been sanitized.
Ideally, the certificate should record at least the following details:
• Manufacturer • Model • Serial Number • Organizationally Assigned Media or Property Number • Media Type (ie magnetic, flash, hybrid, etc.) • Media Source • Pre-Sanitization Confidentiality Level • Sanitization Description (ie. Clear, Purge, Damage, Destruct) • Method Used (ie. degauss, overwrite, block erase, crypto erase, etc.) • Tool Used (including version) • Verification Method (ie. full, quick sampling, etc.) • Post-Sanitization Confidentiality Level • Post-sanitization destination

All documentation should include:
• Name of Person
• Position/Title of Person
• Date
• Location
• Phone or Other Contact Information
• Signature

Appendix G provides a useful sample form (see original document).



Sidebar 4: Tools and Resources (Continued)

DONATIONS AND DISPOSAL: Organizations and individuals wishing to donate used electronic equipment or seeking guidance on disposal of residual materials after sanitization should consult the Environmental Protection Agencies (EPA) electronic recycling and electronic waste information website at http://www.epa.gov/e-Cycling/. This site offers advice, regulations, and standard publications related to sanitization, disposal, and donations. It also provides external links to other sanitization tool resources.

Minimum Sanitization Recommendations for Media Containing Data

Appendix A: Media Sanitization Decision Matrix.
Media types are listed in the left column. The "decision" columns correspond to the destruction methods described on page 2.

This matrix closely follows a fundamental principle expressed throughout the NIST 800-88 document: sanitization methods should be based on confidentiality or security levels first. While this chart primarily covers hard drives, SSDs and optical media, the matrix in the original document covers a wider range of hard copy, data storage and telecommunication devices.

Appendix A. Minimim Sanitization Recommendations from Media Containing Data

(*Abridged* - Complete Tables on page 26 NIST Special Publication 800-88

Media Type	Clear	Purge	Physical Destruction
ATA Hard Drives	Overwrite media by using agency-approved and validated overwriting technologies/ methods/tools.	1. Purge using Secure Erase. The Secure Erase software can be downloaded from the University of California, San Diego (UCSD) CMRR site. 2. Purge hard disk drives by either purging the hard disk drive in an NSA/CSS-approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand**. 3. Purge media by using agency-approved and validated purge technologies/tools. ***Degaussing any current generation hard disk will render the drive permanently unusable.*	• Disintegrate. • Shred. • Pulverize. • Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.

Sidebar 4: Tools and Resources (Continued)

OUTSOURCING: Organizations can outsource media sanitization and destruction if business and security management decide that this option will maintain confidentiality while optimizing available resources. When exercising this option, organizations must exercise "due diligence" when entering into a contract with another party engaged in media sanitization.

Due diligence for this case is accepted as outlined in the FTC's Disposal of Consumer Report Information and Records Document 16 CFR Part 682. This document states *due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule , obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.*

Appendix A. Media Sanitization Decision Matrix (Continued)
(*Abridged* - Original on page 17 NIST Special Publication 800-88

Media Type	Clear	Purge	Physical Destruction
SCSI Drives	Overwrite media by using agency-approved and validated overwriting technologies/ methods/tools.	Purge hard disk drives by either purging the hard disk drive in an NSA/ CSS approved automatic degausser or by disassembling the hard disk drive and purging the enclosed platters with an NSA/CSS-approved degaussing wand.	• Disintegrate. • Shred. • Pulverize. • Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator.
TABLE A-8 Flash Memory ATA Solid State Drives (SSDs) includes PATA, SATA, eSATA, etc.	Overwrite media by using organizationally approved and validated overwriting technologies/ methods/tools. The Clear pattern should be at least a single pass with a fixed data value, such as all zeros. Multiple passes or more complex values may alternatively be used. 2. Leverage (the non-enhanced) ATA Secure Erase, if supported by the device.	1. Apply the ATA sanitize command, 2. Apply the ATA Secure Erase command. The sanitize command is preferred to Secure Erase when the sanitize command is supported by the device. 3. Cryptographic Erase through the TCG Opal SSC or Enterprise SSC interface by issuing commands as necessary to cause all MEKs to be changed.	• Disintegrate. • Shred. • Pulverize. • Incinerate. Incinerate hard disk drives by burning the hard disk drives in a licensed incinerator. *Applying destructive techniques to non-magnetic storage media such as flash is also becoming more challenging, as the necessary particle size for commonly applied grinding techniques goes down proportionally to any increases in flash storage density. Flash chips already present challenges with occasional damage to grinders due to the hardness of the component materials, and this problem will get worse as grinders attempt to grind the chips into even smaller pieces.*
CDs / DVDs	See Physical Destruction	See Physical Destruction	Destroy in order of recommendations: • Removing the Information bearing layers of optical media using a commercial optical disk grinding device. • Incinerate optical disk media (reduce to ash) using a licensed facility. • Use optical disk media shredders or disintegrator devices to reduce to particles that have a nominal edge dimension of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm2)**. ***This is a current acceptable particle size. Any future disk media shredders obtained should reduce DVD to surface area of .25mm.*

ABOUT DESTRUCTDATA, INC.
DestructData is the largest independent provider of End of Life data destruction/ security solutions. Our specialty is integrating the best data erasure solutions available with purpose built hardware to accommodate any volume and application. To compliment and certify the data erasure process, we provide independent QC tools that satisfy world wide certifications requirements and standards. If physically destroying the media is required, we provide all methods of physical destruction for any type of electronic media including smartphones and tablets. As a pioneer in the specialized field of end of life cycle data destruction, DestructData implements the nuts and

Please feel free to submit comments or questions to:

DESTRUCTDATA, INC.
12 Rogers Rd. Unit 8
Haverhill, MA 01835
www.destructdata.com
Toll Free: 800-781-4799
seanoleary@destructdata.com

For inquiries on DestructData products, please e-mail info@destructdata.com