Compliance Resources

Simplifying Privacy Law and Data Sanitization Compliance

- Thumbnails of Federal Legislation
- Working Summary of NIST Special Publication 800-88

Sean O'Leary
Communications Director
DestructData, Inc.
February 15, 2011

DESTRUCTDATA
MEDIA SANITIZATION SOLUTIONS

Simplifying Privacy Law and Data Sanitization Compliance

Sean O'Leary
Communications Director, DestructData, Inc.

Introduction and Overview

In addition to older Federal legislation such as Sarbanes-Oxley, FACTA and HIPAA, there are now forty six state and territorial laws that regulate the management of private electronic data. Two more major federal acts are making their way through Congress, one in the House and another in the Senate*. In spite of the shifting political landscape, they have a high probability of enactment.

Within this expanding body of legislation, there is significant variation in terms of purpose and scope. The individual laws differ with regard to the classes of entities covered, definitions of personal information, identification of agencies selected for rulemaking, enforcement and other considerations. Some are intended to promote transparency within a specific industry segment, others are written for the purpose of expanding the use of electronic records. Civil penalties for failure to secure private data also differ from law to law, the common feature being a markedly upward trend in recent years. Criminal penalties now augment civil fines.

In the first half of this document, we have provided summaries of existing federal laws affecting privacy and data breaches, as well as those making their way through Congress.

Regardless of other variations, recent privacy legislation consistently includes two common requirements: 1) establishment of formal data security programs and 2) notification of individuals in the case of a data breaches. As a key component of these mandatory data security programs, virtually every new law also includes a provision that covered entities must securely destroy end of life cycle electronic private data. This is because - despite the focus on protecting data-in-motion - a significant percentage of data theft involves retired storage media.

For the electronic data disposal segment of IT security, we believe there is a compelling argument that "real world" compliance is simpler than it appears. Consider that specific technical nuts and bolts of data erasure and destruction are not referenced in most actual legislation language, so it isn't strictly accurate to describe a company or procedure as "FACTA compliant" or "HITECH approved". Instead the various legislative Acts describe the intent of the law, then direct a government agency to develop practical "guidance" that determines rules governing practical execution.

In almost every case, these guidelines are expressly meant to be flexible and to be consistent with similar laws. As a result, most federal guidance is notably non-specific, tending toward "examples" than requirements. This self-referencing rulemaking process increasingly creates de facto adaptation of the recommendations published in the National Institute of Standards and Technology's (NIST) Special Publication 800-88: Guidelines for Media Sanitization. Issued in 2006, this analysis identifies multiple methods for destroying data on electronic storage media and ranks them according to security level.

Table of Contents

* HR2221, the Data Accountability and Trust Act (DATA), is intended to establish a uniform set of regulations governing the collection and protection of consumer's Personally Identifiable Information (PII). S.1490 is the Senate version of HR2221 (DATA) bill.

A number of legal experts have indicated that the language found in government data disposal rules in most cases establishes a Safe Harbor scenario for covered entities that have applied technologies and methods referenced in the guidance. However, this is a forty one page document that includes an extensive amount of material that is not relevant to most data disposal scenarios.

The second section of this document is an easy to digest summarization of the more comprehensive NIST Special Publication 80-88. Intended as a more manageable reference resource, it covers all of the key core material more briefly than the original.

The NIST 800-88 guidelines don't eliminate the need to take relevant technical, cost/benefit, environmental and custody/control factors into consideration, rather, they provide an outline for evaluating these parameters. In terms of specific technologies, the NIST guidelines deal with a manageable range of possibilities , ranked according to security level. The methodologies are split between physical (or mechanical) destruction and non-destructive. Physical destruction ranks the highest in terms of security, but renders the storage media unusable. The non-destructive methods are described as purging and over-writing; they securely erase data without destroying the functionality of the hard drive or other electronic media.

"The NIST 800-88 guidelines don't eliminate the need to take relevant technical, cost/benefit, environmental and custody/ control factors into consideration, rather, they provide an outline for evaluating these parameters. "

Within any particular media storage scenario, IT managers should be able to choose one or more methodology consistent with business objectives, scale of operations, environmental considerations, security requirements and insurance-based factors. As the discipline matures, more companies are seeking data disposal solutions within a greater business or mission context, such as the ability to maximize asset value through re-sale or recycling, or social and tax benefits through charity donation.

DestructData, Inc. is a media sanitization system integrator and service provider. As a pioneer in the specialized field of end of life cycle data destruction, the company implements the nuts and bolts solutions that assure compliance with complex data disposal legislation. Professional data security consultants provide guidance that matches solutions to specific scenarios. DestructData sells, rents and custom integrated hardware/software systems for any level of media storage operation. In addition, the on-site services division is able to cost-effectively deliver high volume drive sanitization without removing drives from client premise.

DESCRIPTION: The Act (along with the similar S1490) is intended to create a nationwide set of regulations for Data Brokers, enforced by a new set of federal crimes and penalties for violations. It would establish a uniform set of regulations to govern the collection of and protection of consumer's Personally Identifiable Information (PII), as well as regulations governing notification of security breaches involving PII. Specific to our interests, it directs the FTC to **specify processes for disposing of obsolete electronic and non-electronic data** containing PII.

Personal information is defined as an individual's first name or initial and last name, or address, or phone number, in combination with any one or more key elements such as Social Security number, driver's license number or other State identification number, financial account number, or credit or debit card number, and any required security code, access code, or password that is necessary to permit access to an individual's financial account.

This bill is purposely consistent in intent and language to forty-six existing state data breach notification laws and also to pending Senate bill S.1490. One of the intentions of HR1666 is to **pre-empt state laws already passed, theoretically establishing a uniform regulatory climate**. Both H.R.2221 and S.1490 would create a regulatory standard to regulate the collection, storage and disposal of consumer PII.

DATA SECURITY FACTORS: The Federal Trade Commission (FTC) is emerging as the principle enforcement agency responsible for defining proper technical procedures for protecting data. Among the requirements set forth by the Act, organizations holding private data must **establish a data security policy,** identify an information security officer and set up a process for identifying vulnerabilities. This is the key component in virtually all recent data privacy protection legislation. Organizations must also monitor for breaches and **establish processes for securely destroying end-of-service data on hard drives and other electronic media**.

The Act deems an information broker to be in compliance with the relevant provisions of this Act if the broker is in compliance with any other federal information security statutes that specify similar or greater protections than those required under this H.R. 2221.

ENFORCEMENT / PENALTIES: DATA H.R. 2221 specifies civil penalties for violations of requirements for information security. Organizations can be fined for not establishing data security policies or naming a data security officer. The law provides for penalties up to **$11,000 a day** for each day the organization is out of compliance. Specific penalties for data breaches are calculated as follows: multiplying the number of violations of each section by an amount not greater than $11,000. Each failure can be treated as a separate violation. The maximum civil penalty calculated under this clause **shall not exceed $5,000,000**.

States Attorneys for individual states may initiate enforcement following data breaches, with additional enforcement or intervention by the FTC possible.

DATA (HR2221)

FULL NAME:
Data Trust & Accountability Act
(HR 2221)

STATUS:
Passed by U.S. House of Representatives December 2009 /

Dec 9, 2009: Received in the Senate and Read twice / referred to the Committee on Commerce, Science, and Transportation.

EFFECTIVE DATE:
Pending passage of S.1490

TARGET:
Data brokers, defined by the Act as entities primarily engaged in the collection of personal data for more than 5,000 individuals for a fee and transmission of that data through interstate commerce to third parties. However, if the FTC remains the primary agency, organizations not under FTC jurisdiction (banks, savings and loans airlines and railroads) will be exempt.

AGENCIES:
Federal Trade Commission (FTC)

DESCRIPTION: This Act is the Senate version of DATA (HR 2221) S.1490 seeks to prevent and mitigate identity theft, to ensure privacy, to provide notice of security breaches, and to enhance criminal penalties, law enforcement assistance, and other protections against security breaches, fraudulent access, and misuse of personally identifiable information.

DATA SECURITY FACTORS: The Federal Trade Commission (FTC) is the primary enforcement agency responsible for defining proper technical procedures for protecting data. Among the requirements set forth by the Act, organizations holding private data must establish a data security policy, identify an information security officer and set up a process for identifying vulnerabilities. Written security programs are key components in virtually all recent privacy protection data. Organizations must also monitor for breaches and establish processes for securely destroying end-of-service data on hard drives and other electronic media. The Act deems an information broker to be in compliance with this Act if they are in compliance with any other federal information security statutes that provide similar or greater protections.

ENFORCEMENT / PENALTIES: Although this Act is unlikely to change the guidelines or standards for secure data disposal compliance, it does break new ground in terms of penalties. Among the tough new regulations is an amendment of the federal criminal code to add intentionally accessing a computer without authorization to the definition of racketeering activity.

In addition, Section 102 imposes a fine and/or prison term of up to five years for intentionally and willfully concealing a security breach involving sensitive personally identifiable information that causes economic damage to one or more persons. The Act also instructs the Department of Justice to designate a department-wide Chief Privacy Officer and the U.S. Sentencing Commission to review and amend, if appropriate, federal sentencing guidelines for persons convicted of using fraud to access, or to misuse, digitized or electronic personally identifiable information, including sentencing guidelines for identity theft. Finally, it allows state attorneys general to bring a civil action in a U.S. district court to enforce security breach notification requirements and authorizes the Attorney General to stay, or intervene in, any state action.

PDPSA (S 1490)

FULL NAME:
Personal Data Privacy and Security Act of 2009
(S1490)

STATUS:
This Act is essentially the Senate version of DATA (HR 2221)

Dec 9, 2009: Received in the Senate and Read twice and referred to the Committee on Commerce, Science, and Transportation.

FUNDING:
$1,000,000 for each of fiscal years 2010 through 2015 to carry out this Act.

TARGET:
Data brokers, defined by the Act as entities primarily engaged in the collection of personal data for more than 5,000 individuals and transmission of that data through interstate commerce to third parties. However, if the FTC remains the primary agency, organizations not under FTC jurisdiction (banks, savings and loans airlines and railroads) will be exempt.

AGENCIES:
Federal Trade Commission (FTC)

DESCRIPTION: Section 216 directs the FTC and other agencies to adopt consistent and comparable rules regarding the proper disposal of consumer report information and records. These rules must also be consistent with the requirements of the Gramm-Leach-Bliley Act. The Rule covers information in both electronic and hard copy form.

DATA SECURITY FACTORS: According to the FTC, the standard for the proper disposal of information derived from a consumer report is flexible, and allows the organizations and individuals covered by the Rule to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of different disposal methods, and changes in technology. Although the Disposal Rule applies to consumer reports and the information derived from consumer reports, the FTC recommends that anyone who disposes of any type of records containing a consumer's personal or financial information to take similar protective measures.

The final Rule includes several examples of "reasonable measures" to protect consumer information in connection with its disposal. Reasonable measures for disposing of electronic consumer report information could include destroying or erasing electronic files or media containing consumer report information so that the information cannot be read or reconstructed. It also includes hiring a document destruction contractor to dispose of data consistent with the Rule. Due diligence could include reviewing an independent audit of the service provider's operations and/or its compliance with the Rule or requiring that the disposal company be certified by a recognized trade association.

AGENCIES: FACTA directs the FTC, the Federal Reserve Board, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, and the Securities and Exchange Commission to adopt comparable and consistent rules regarding the disposal of sensitive consumer report information.

ENFORCEMENT / PENALTIES: Although the FACTA rules have been established by the FTC, their enforcement may fall under the jurisdiction of multiple agencies, federal and state.

Penalties for violating the rule include actual damages, statutory damages up to $1,000 punitive damages per violation (with no cap on class action damages), attorneys' fees, and civil penalties up to $3,500.

FACTA (Disposal Rule)

FULL NAME:
Fair and Accurate Credit Transactions Act of 2003
(an amendment to the Fair Credit Reporting Act)

STATUS:
Effective June 1, 2005

Additional Red Flag rules have been issued since 2007, but continue to be stalled by challenges and lawsuits regarding its scope.

TARGET:
The FACTA Disposal Rule applies to people and organizations of any kind that use consumer reports for business purposes, including: consumer reporting companies; lenders; insurers; employers, landlords, government agencies, mortgage brokers, car dealers, attorneys, private investigators, debt collectors, individuals who perform credit checks on private employees such as nannies or contractors. It also applies to and organizations that maintain information in consumer reports as part of their role as a service provider to other organizations covered by the Rule.

DESCRIPTION: In general, GLB requires that financial institutions provide notices to their customers about their information collection and sharing practices, and restricts their ability to disclose a consumer's personal financial information to nonaffiliated third parties. The GLB has directed the FTC to develop the Safeguards Rule, which applies to the protection of private information and requires companies to ensure security and confidentiality. A key component of the Rule deals with data storage and proper destruction (see next section).

DATA SECURITY FACTORS: The Federal Trade Commission (FTC) issued the Safeguards Rule as part of GLB Act implementation. It requires financial institutions to have measures in place to keep customer information secure. It further requires disposal of customer information in a secure way, consistent with the FTC Disposal Rule. Section 682.1(c) of the Rule defines "disposal" as including the discarding or abandonment of consumer information, as well as the sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored. The FTC recommends that financial institutions incorporate secure data disposal practices into the information security program required by the Safeguards Rule.

Under the Disposal Rule, the FTC allows covered entities to consider their unique scenarios when determining disposal methods, which it refers to as "reasonable measures". The method may reflect the sensitivity of the consumer information, the nature and size of the entity's operations, the costs and benefits of different disposal methods, and relevant technological changes*. In non-committal language, the Rule is likely to require elements such as the establishment of policies and procedures governing disposal, as well as appropriate employee training.

With regard to computers, disks, CDs, magnetic tapes, hard drives, laptops, PDAs, cell phones or other electronic media, the Safeguards Rule directs the data be erased or destroyed so that the information "cannot practicably be read or reconstructed". The Rule also includes service providers in the examples, which suggest monitoring compliance when a contract with a third party engaged in the business of record destruction to dispose of material. Due diligence could include reviewing an independent audit of the disposal company's operations, requiring that the disposal company be certified by a recognized trade association or similar third party, plus reviewing and evaluating the disposal company's information security policies.

ENFORCEMENT / PENALTIES: The GLB Act provides severe penalties for non-compliance:

Fines up to $100,000 per violation

Imprisonment up to five years

The officers and directors of the financial institution could be subject to, and personally liable for, a civil penalty of up to $10,000.

Both the Safeguards Rule and Disposal Rule were issued prior to the issuance of Special Publication 800-88.

Gramm-Leach-Bliley)

FULL NAME:
The Gramm-Leach-Bliley Act of 1999 (GLBA)

The Financial Modernization Act of 1999

(Safeguards Rule / Disposal Ruie)

STATUS:
GLB Safeguards Rule issued May 2003

The Disposal Rule in effect June 1, 2005

TARGET:
Companies that collect personal information from their customers, including names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers. The GLBA universe includes banks, credit unions, securities brokers, real estate appraisers, insurance companies, auto leasing companies, retailers issuing credit cards. The Safeguards Rule applies to all businesses, regardless of size, that are "significantly engaged" in providing financial products or services. Under the final Rule, service providers are expressly covered, and bear responsibility for proper disposal of consumer information that they maintain or otherwise possess.

AGENCIES:
Federal Trade Commission (FTC), Federal Reserve Board (FRB), Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), Office of Thrift Supervision (OTS), National Credit Union Administration (NCUA), Securities and Exchange Commission (SEC), and Federal Trade Commission (FTC).

DESCRIPTION: Intended to encourage the use of Electronic Health Records by medical and health services organizations, this legislation also takes the scope and enforcement of HIPAA (Health Insurance Portability and Accountability Act of 1996 privacy protection to a new level. Penalties for violations can now include criminal prosecution.

DATA SECURITY FACTORS: Portions of HITECH specify standards for protecting private medical data and new penalties for lack of compliance. New guidance for technologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals have been established and are published in the Federal Register 74 FR 19006 of April 27, 2009. If the entities subject to the regulations apply the technologies and methodologies specified in the guidance, they will not be required to provide the notifications required by the regulations in the event the information is breached. Among the scenarios specified in the Federal Rules and Regulations is destruction or purging of electronic media in accordance with methods specified in *NIST Special Publication 800-88: Guidelines for Media Sanitatio*n.

ENFORCEMENT / PENALTIES: OCR is responsible for enforcing Privacy Rule standards and may conduct compliance reviews. Covered entities that fail to comply voluntarily with the Privacy Rule may be subject to civil penalties (fines). In addition, certain violations may be subject to criminal prosecution. Penalties will vary significantly depending on factors such as the date of the violation, whether the covered entity knew or should have known of the failure to comply, or whether the covered entity's failure to comply was due to willful neglect.

HITECH

FULL NAME:
Health Information Technology for Economic and Clinical Health Act

STATUS:
Signed into law February 17, 2009

TARGET:
Doctors, hospitals and other medical services organizations, plus vendors of personal health records and other non-HIPAA covered entities.

FUNDING:
$19.2 Billion

AGENCIES:
Department of Health and Human Services (HHS) Office for Civil Rights (OCR), Federal Trade Commission (FTC)

DESCRIPTION: The Sarbanes-Oxley Act introduced significant legislative changes to financial practices and corporate governing regulation for publically traded companies. The intent of the Act is to force publicly held companies to promptly make available and maintain all meaningful business related information in order to protect the investing public. While the primary focus of this act is to make corporate finances more transparent, it also specifies best practices for the disposal and documentation of financial records. Because of the Sarbanes-Oxley Act, intentional document destruction is now a process that must be carefully monitored. Because the legislation is concerned with financial transparency, it has created a Catch 22 for electronic records management and security. Many legal firms recommend establishing a data destruction protocol which provides for methodical and verifiable destruction of data may create a legal safe harbor from plaintiffs records

DATA SECURITY FACTORS: Section 404 of the Sarbanes-Oxley (SOX) Act requires you to create and monitor controls of systems that affect your ability to deliver accurate financial reports. It also makes company management responsible for this "internal control" over financial reporting.

ENFORCEMENT / PENALTIES: Violations of this Act are accompanied with very strict fines and jail time. The severest of fines could get up to as high as $5,000,000 and up to 20 years in prison.

The Sarbanes-Oxley Act

FULL NAME:
Public Company Accounting Reform and Investor Protection Act (Senate)

Corporate and Auditing Accountability and Responsibility Act (House)

STATUS:
Enacted July 30, 2002

TARGET:
Publically traded companies

AGENCIES:
Securities and Exchange Commission (SEC))

Summary of NIST Special Publication 800-88

Guidelines for Media Sanitization

Recommendations of the National Institute of Standards and Technology

Overview of NIST Special Publication 800-88

Special Publication 800-88 recommends a number of methods for sanitizing electronic data on hard drives and other electronic media. Media 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. 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 the 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 such factors as 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 summary of the NIST publication report provides a "thumbnail" version of the essential information found in the original 41 page document. Appendix A, *Media Sanitization Decision Matrix*, encapsulates the core concepts of the original NIST publication and is reproduced in part at the end of this document. The matrix provides a useful greater context for the practical product and policy choices a complete program will require.

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.

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.

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.

Best practices have changed since 2001 and will continue to change. 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. For ATA disk drives manufactured after 2001 (over 15 GB) clearing by overwriting the media once (single pass) is adequate to protect the media from both keyboard and laboratory attack.

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

The category descriptions that follow here are summations of those in Table 2.1 and Table 5.1 (which are essentially duplicates of each other) in the NIST original.

Disposal: Discarding media without sanitizing the data is contains (throwing it away).

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.

The two primary examples of purging are 1) executing the firmware Secure Erase command and 2) degaussing. 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.

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.

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?

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.

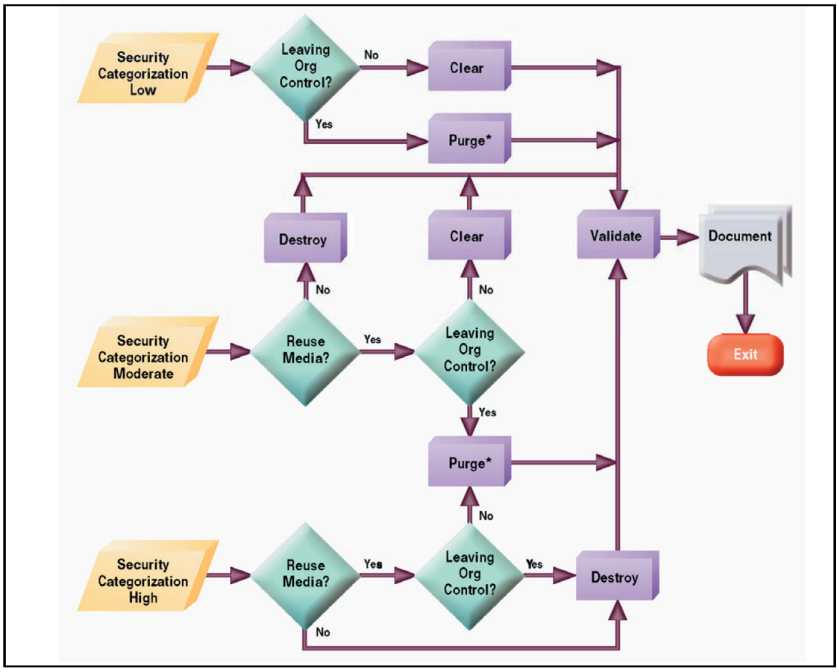

Figure 4-1. Sanitization and Disposition Decision Flow
Original on page 12 NIST Special Publication 800-88

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:
Verifying sanitization is essential. This phase of sanitization policy includes taking a representative sample of media. All verification must be conducted by personnel with no stake in the process. Tools used in sanitization must be calibrated, tested and maintained. Personnel must be trained and attain the proper level of expertise to perform sanitization tasks.

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

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.***

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 and optical media, the matrix in the original document covers a wider range of hard copy, data storage and telecommunication devices.

Appendix A. Media Sanitization Decision Matrix
(*Abridged* - Original on page 17 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)

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.

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.
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.*

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.*