pds CONNECT

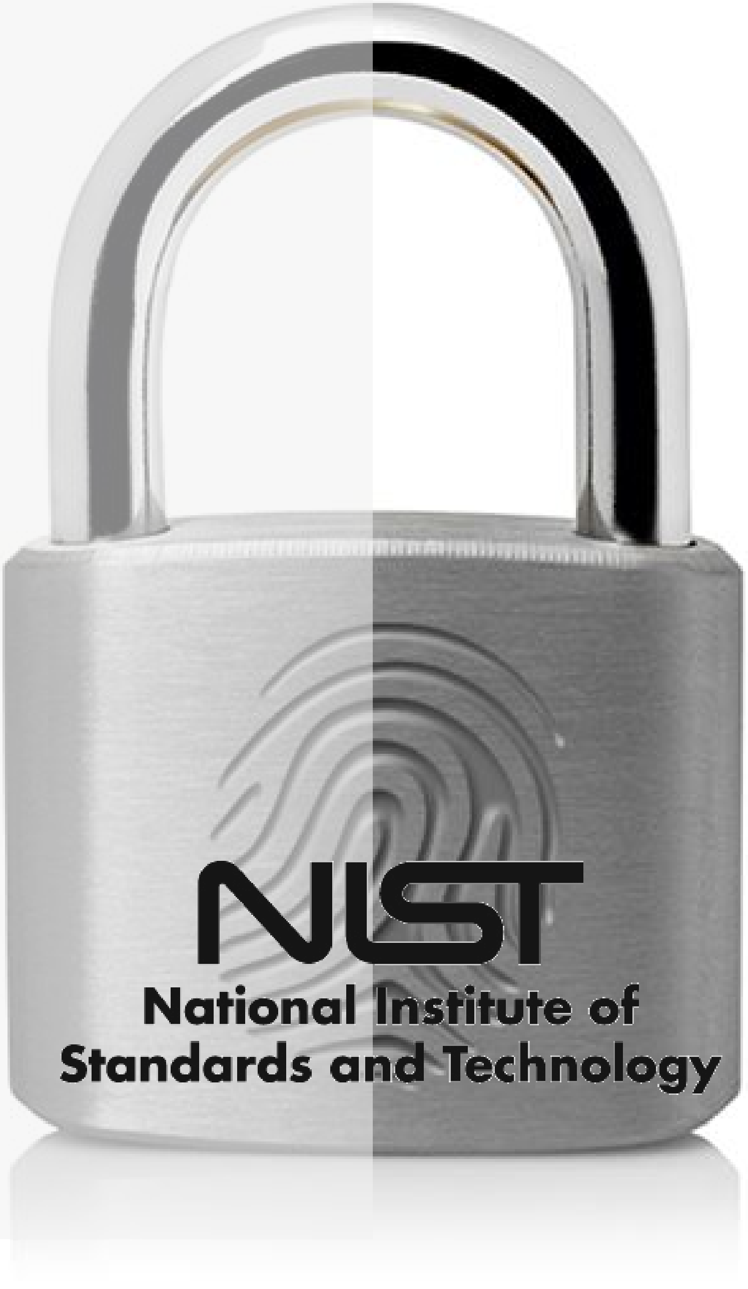
Madison, WI

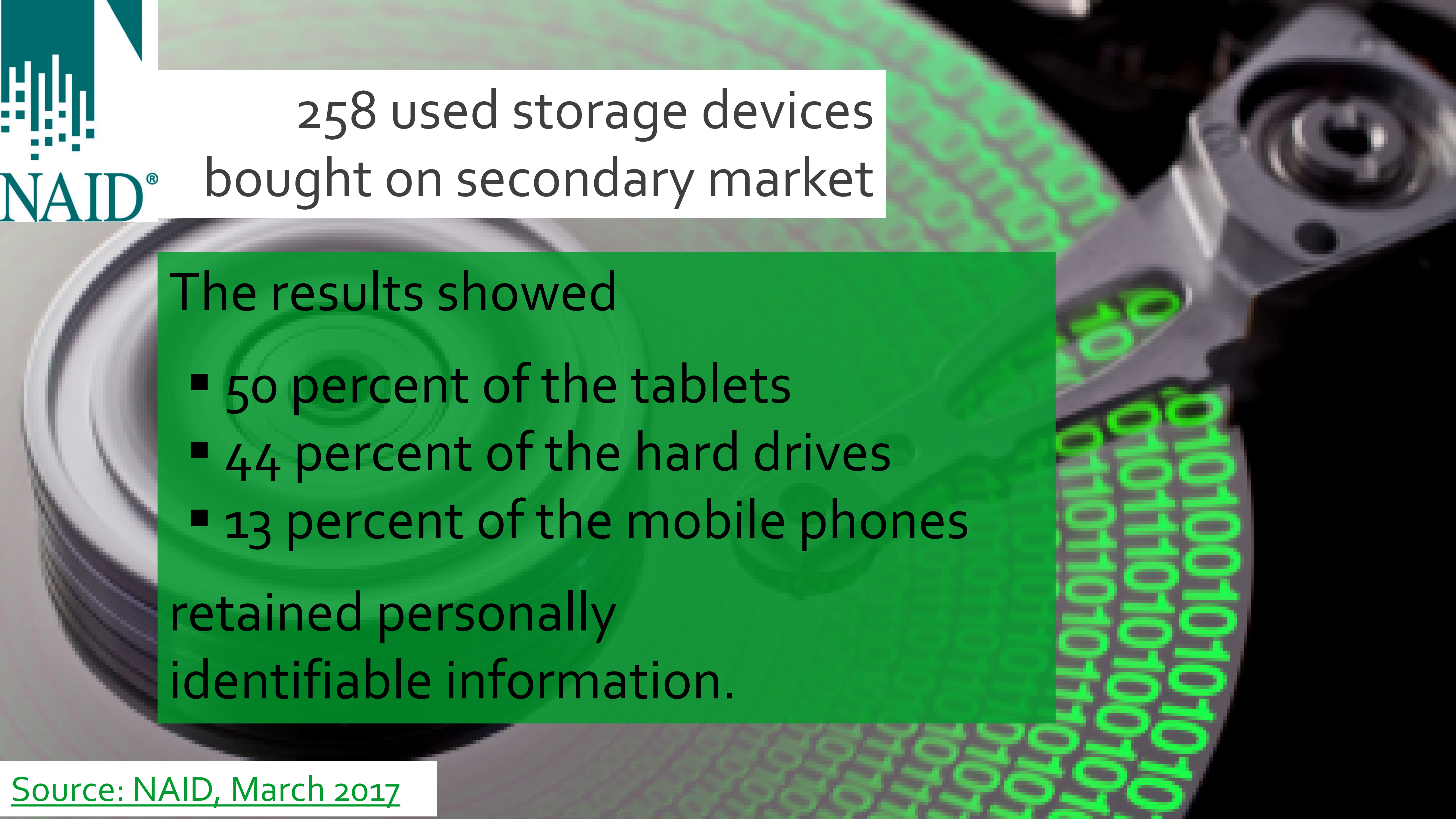
October 18, 2018

A flexible & effective framework for secure data destruction

Neil Peters-Michaud, CEO

Cascade Asset Management





258 used storage devices bought on secondary market

The results showed

- 50 percent of the tablets
- 44 percent of the hard drives
- 13 percent of the mobile phones

retained personally identifiable information.

Source: NAID, March 2017

Topics

- Where data is stored
- When data needs to be destroyed
- Why data needs to be destroyed
- NIST 800-88: Guidelines for Media Sanitization – a framework for a comprehensive data destruction program

Where data is stored

When data needs to be destroyed

Internal redeployment

- Employee changes
- Business changes

Repair/Replace – internal or external

- Scheduled refresh
- Break/fix

Disposal – leave organization

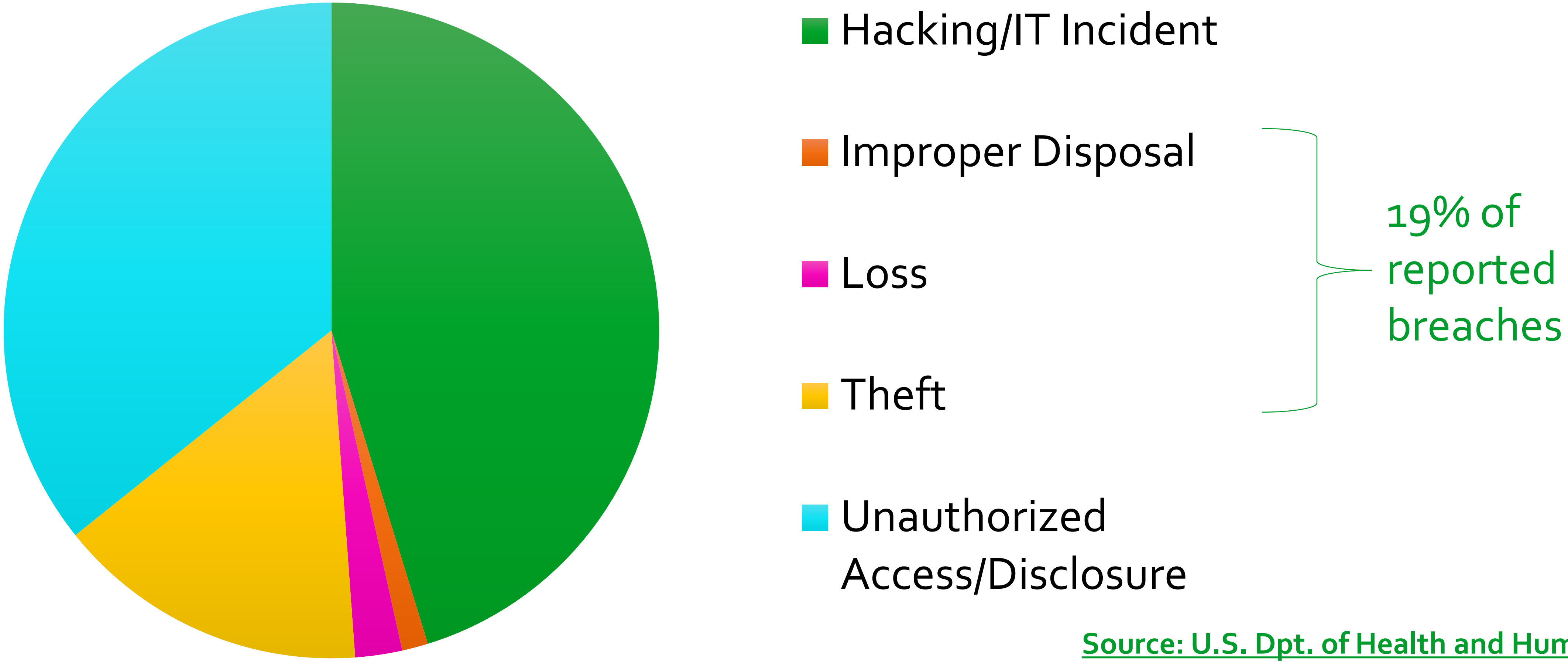
- ITAD vendor
- Lease returns
- Donations, employee sales

Why data needs to be destroyed

- Prevent a data breach
- Comply with law: HIPAA, CJIS, FACTA, etc.
- Organizational Policy
  - Risk Assessment – where are you at risk from a data breach?
    - §164.308(a)(1)(ii)(A) Risk analysis (Required): Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by the covered entity or business associate

(Security Rule of HIPAA, 1996)

Healthcare Data Breach Investigations
Nov 2015 – Nov 2017

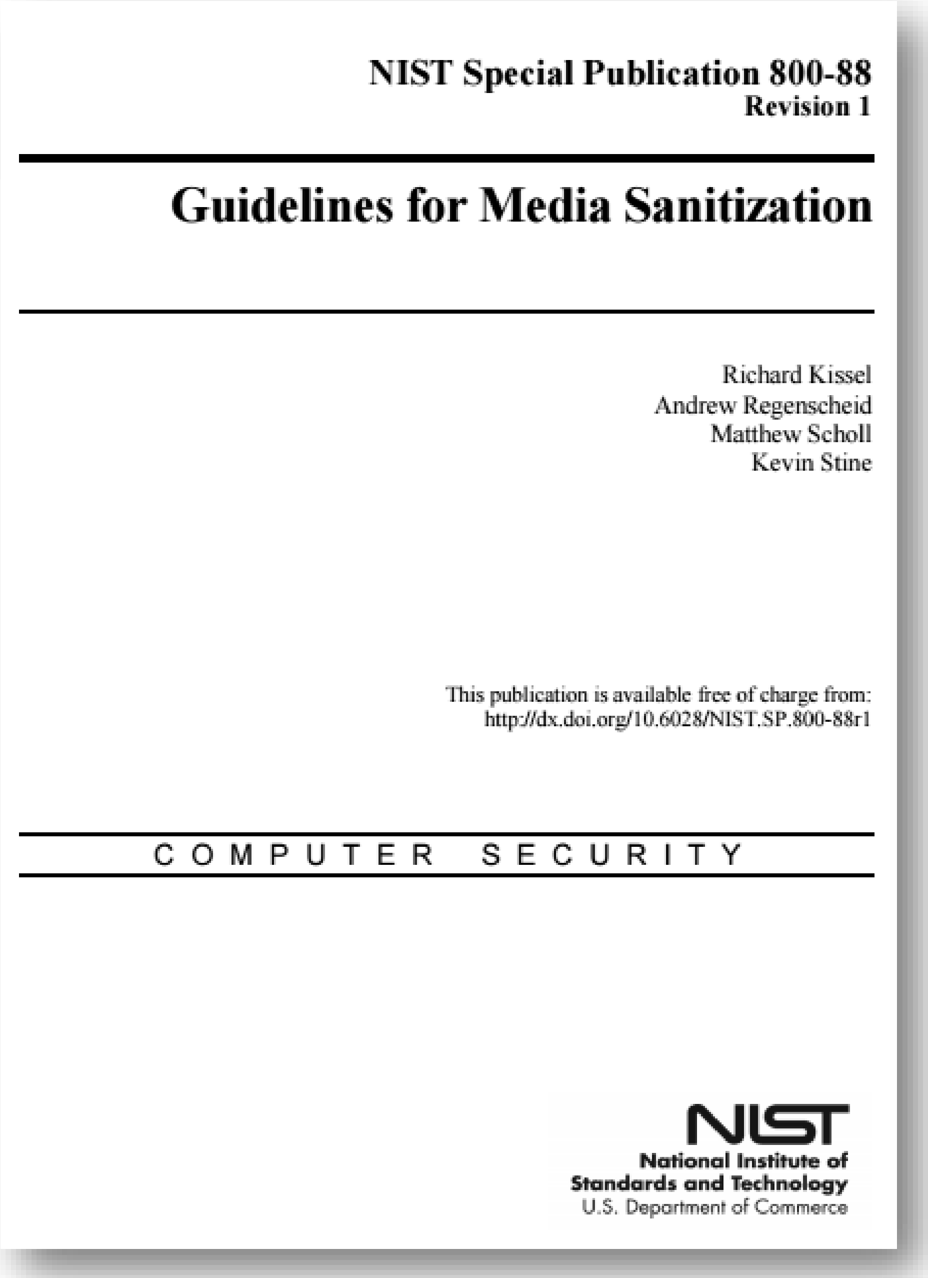


19% of reported breaches

Source: U.S. Dpt. of Health and Human Services Office for Civil Rights

NIST 800-88

“This guide will assist organizations…
in making practical sanitization decisions
based on categorization of information”



NIST Special Publication 800-88
Revision 1

Guidelines for Media Sanitization

Richard Kissel
Andrew Regenscheid
Matthew Scholl
Kevin Stine

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NIST 800-88

- » Practical, real world reference for media sanitization guidance and compliance
- » Introduced in 2006, updated Dec, 2014 (Revision 1) to address changing technologies
- » Replaced DoD 5220.22M standard in regulatory and certification practice
- » Referenced in many other security rules, regulations and standards

How to destroy data

» Electronic sanitization

- Over-writing
- Cryptographic erase

» Physical destruction

- Degaussing magnetic media
- Shredding (shred size depends on media)
- Pin, waffling

Media sanitization is a process by which data is irreversibly removed from media or the media is permanently destroyed.

Note:

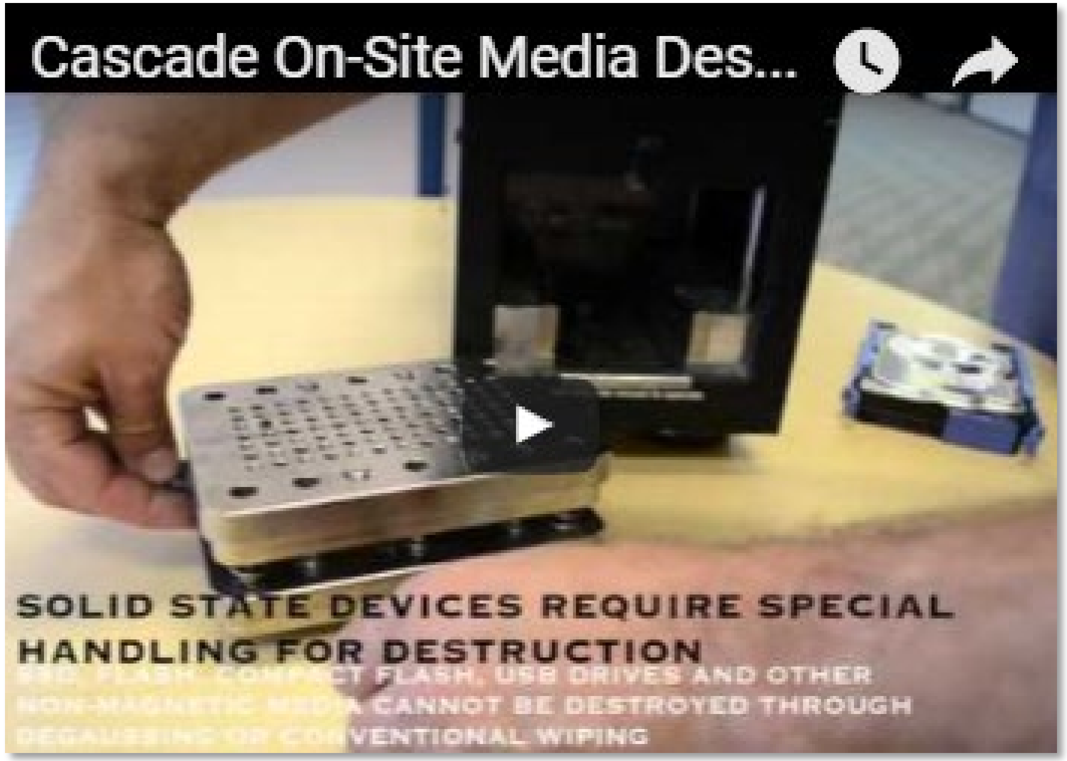
NIST considers any of these forms of data destruction as a type of "Sanitization."

Classification of sanitization methods

Clear: protection against a keyboard attack

Purge: protection against a laboratory attack

Destroy: media cannot be reused *(physical destruction)*



Cascade On-Site Media Des...

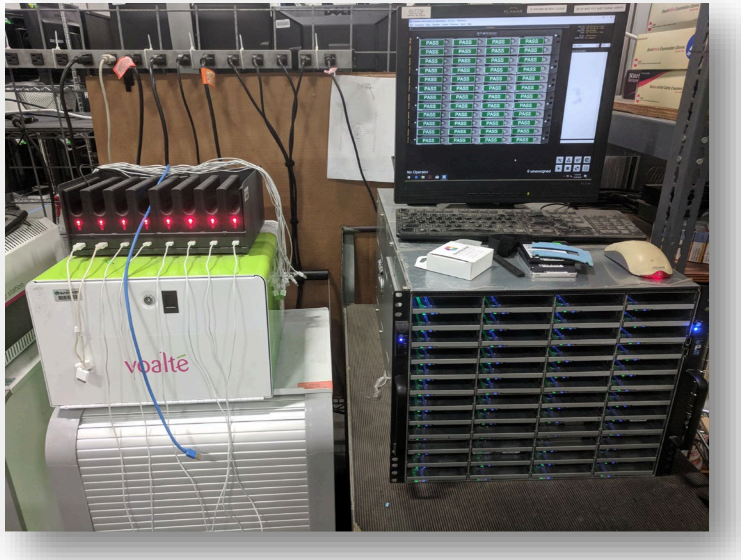
SOLID STATE DEVICES REQUIRE SPECIAL HANDLING FOR DESTRUCTION

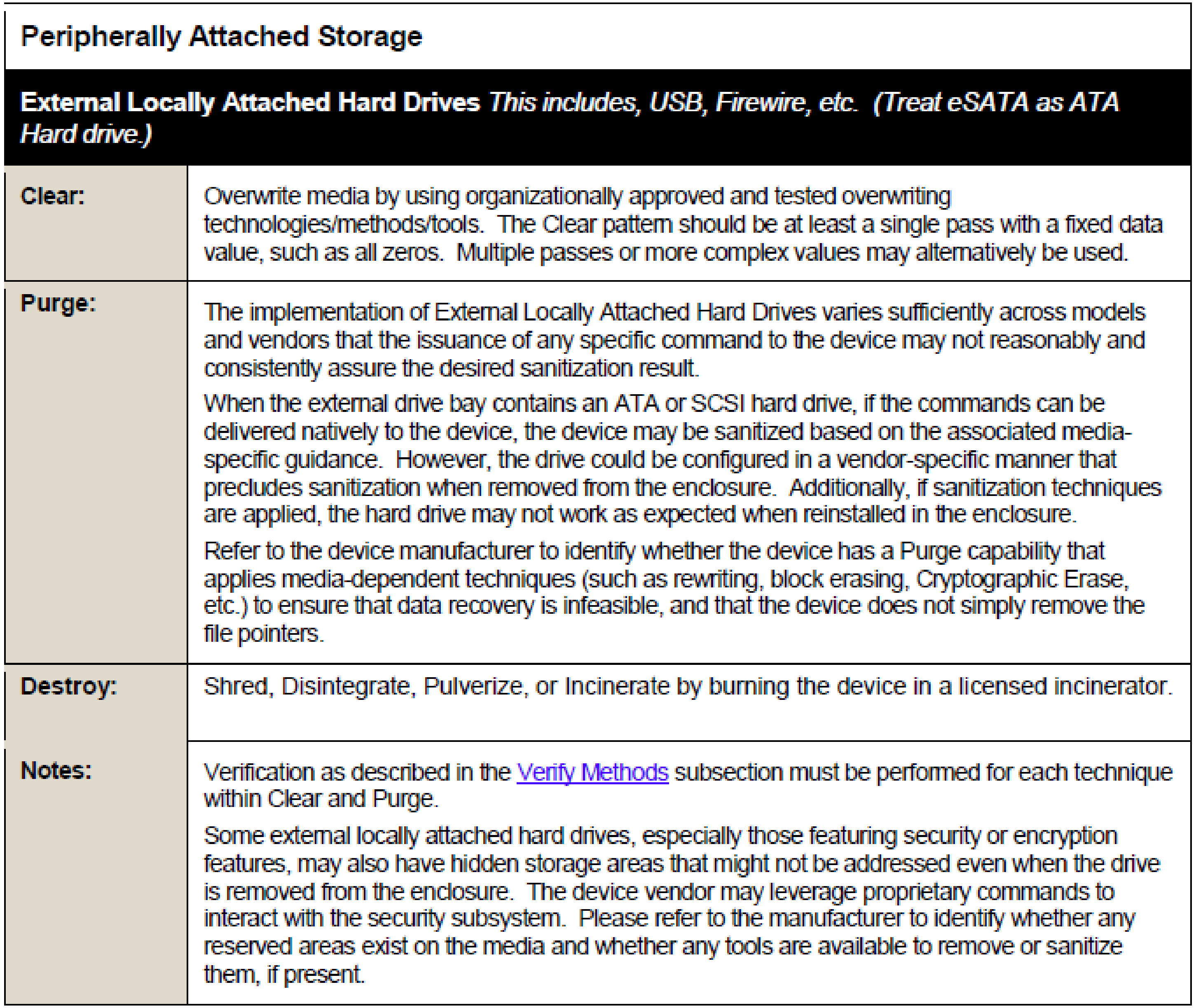
SSD, FLASH, COMPACT FLASH, USB DRIVES AND OTHER NON-MAGNETIC MEDIA CANNOT BE DESTROYED THROUGH DEGAUSSING OR CONVENTIONAL WIPING

Increasing complexity of testing & sanitization

Sanitization is more complex with SSDs, mobile devices, enterprise equipment, increased customization, flash media, etc.

- Larger volumes of specialized testing required
- Requires higher level of knowledge & skill from technicians
- Additional hardware, software, and peripherals – flexible testing stations
- Increase in servers X increase in HDD storage = more capacity needed
- Testing requirements (e-Stewards, R2, NAID, etc)
- Licensing requirements





Peripherally Attached Storage

External Locally Attached Hard Drives *This includes, USB, Firewire, etc. (Treat eSATA as ATA Hard drive.)*

Clear:	Overwrite media by using organizationally approved and tested 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.
Purge:	The implementation of External Locally Attached Hard Drives varies sufficiently across models and vendors that the issuance of any specific command to the device may not reasonably and consistently assure the desired sanitization result. When the external drive bay contains an ATA or SCSI hard drive, if the commands can be delivered natively to the device, the device may be sanitized based on the associated media-specific guidance. However, the drive could be configured in a vendor-specific manner that precludes sanitization when removed from the enclosure. Additionally, if sanitization techniques are applied, the hard drive may not work as expected when reinstalled in the enclosure. Refer to the device manufacturer to identify whether the device has a Purge capability that applies media-dependent techniques (such as rewriting, block erasing, Cryptographic Erase, etc.) to ensure that data recovery is infeasible, and that the device does not simply remove the file pointers.
Destroy:	Shred, Disintegrate, Pulverize, or Incinerate by burning the device in a licensed incinerator.
Notes:	Verification as described in the Verify Methods subsection must be performed for each technique within Clear and Purge. Some external locally attached hard drives, especially those featuring security or encryption features, may also have hidden storage areas that might not be addressed even when the drive is removed from the enclosure. The device vendor may leverage proprietary commands to interact with the security subsystem. Please refer to the manufacturer to identify whether any reserved areas exist on the media and whether any tools are available to remove or sanitize them, if present.

Example in NIST Guidelines of how to meet each sanitization level for a type of media.

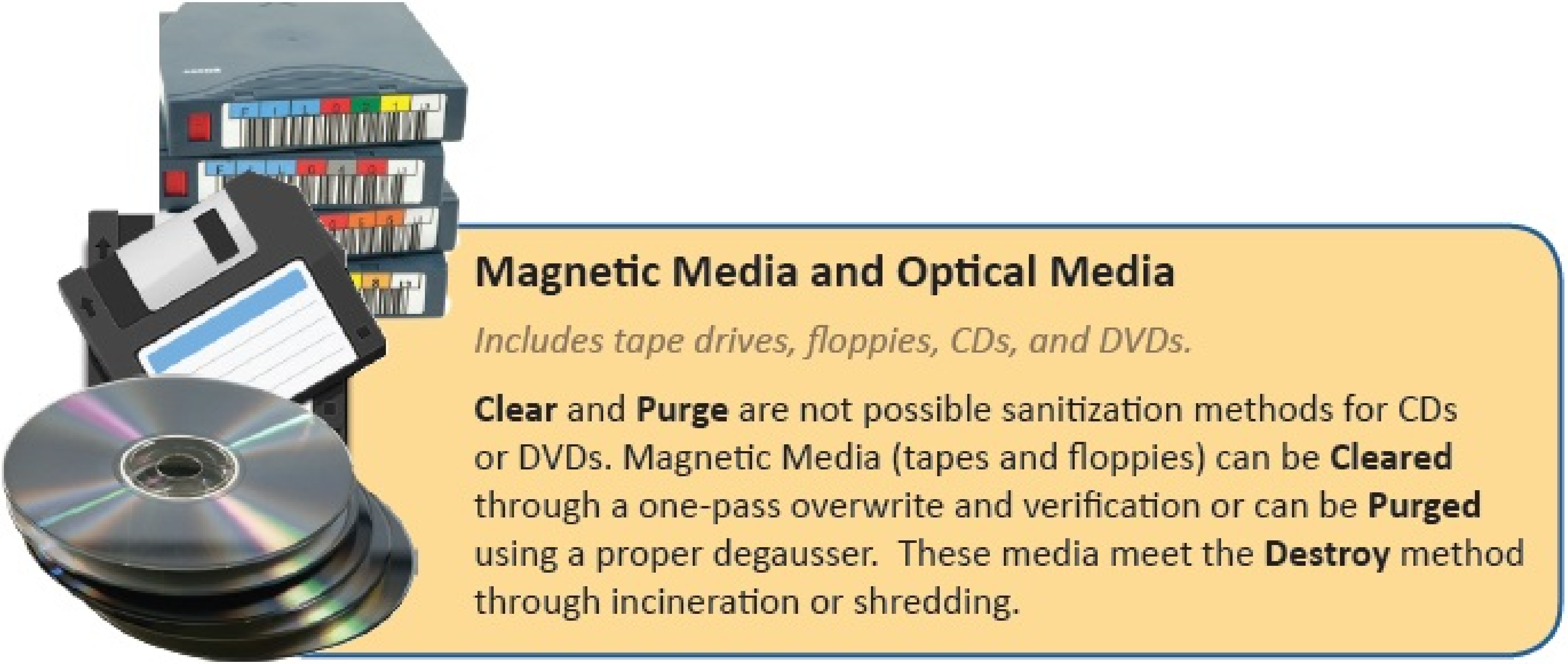
Sanitization methods for various media

Hard Copy Storage

Includes paper and microforms

Clear and **Purge** are not possible sanitization methods for these media. To **Destroy**, paper must be shredded using a cross cut process into particles 1mm x 5mm in size or smaller. Paper may also be pulverized through a 2.4mm screen. Microforms (microfilm, microfiche or photo negatives) are considered destroyed when burnt to a white ash.

Sanitization methods for various media

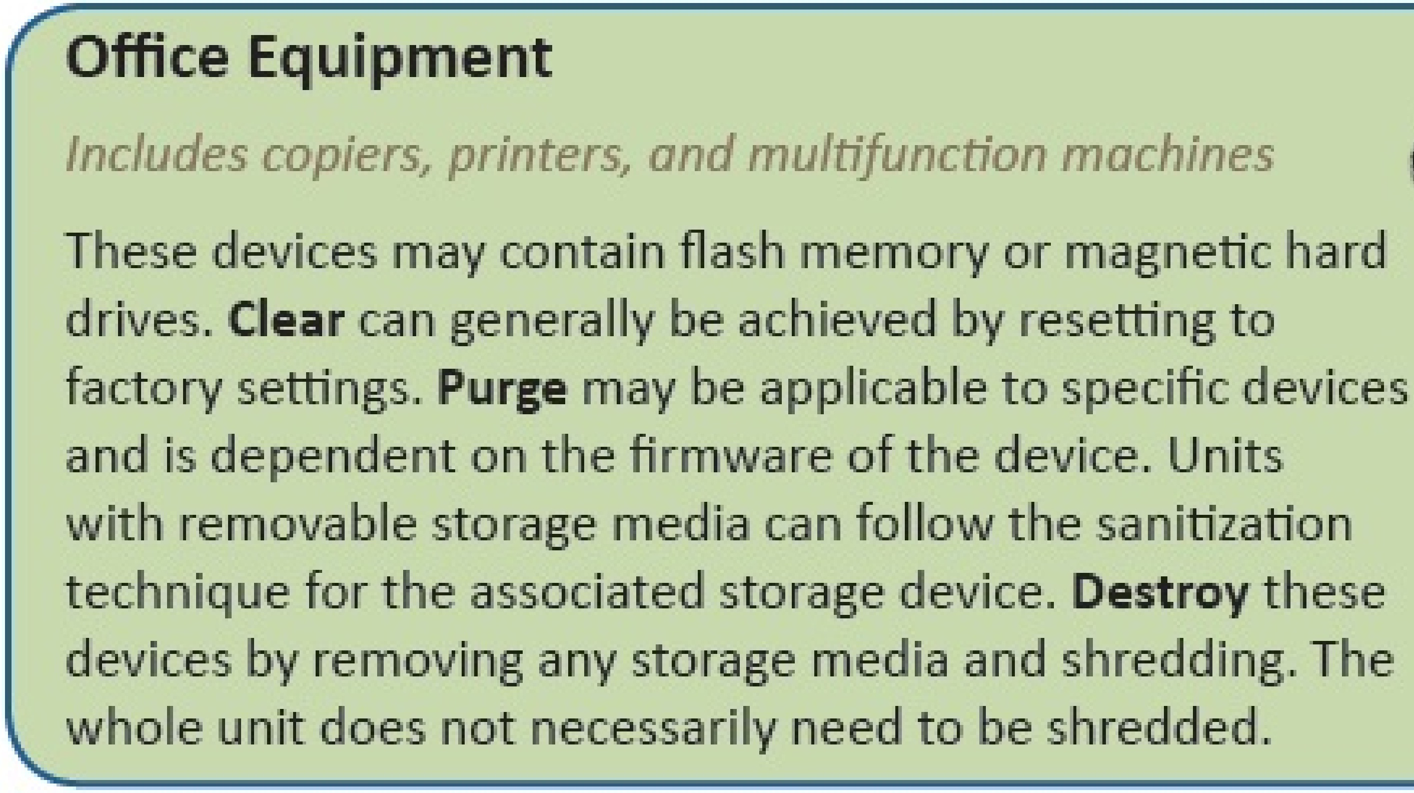


Magnetic Media and Optical Media

Includes tape drives, floppies, CDs, and DVDs.

Clear and **Purge** are not possible sanitization methods for CDs or DVDs. Magnetic Media (tapes and floppies) can be **Cleared** through a one-pass overwrite and verification or can be **Purged** using a proper degausser. These media meet the **Destroy** method through incineration or shredding.

Sanitization methods for various media



Office Equipment

Includes copiers, printers, and multifunction machines

These devices may contain flash memory or magnetic hard drives. **Clear** can generally be achieved by resetting to factory settings. **Purge** may be applicable to specific devices and is dependent on the firmware of the device. Units with removable storage media can follow the sanitization technique for the associated storage device. **Destroy** these devices by removing any storage media and shredding. The whole unit does not necessarily need to be shredded.

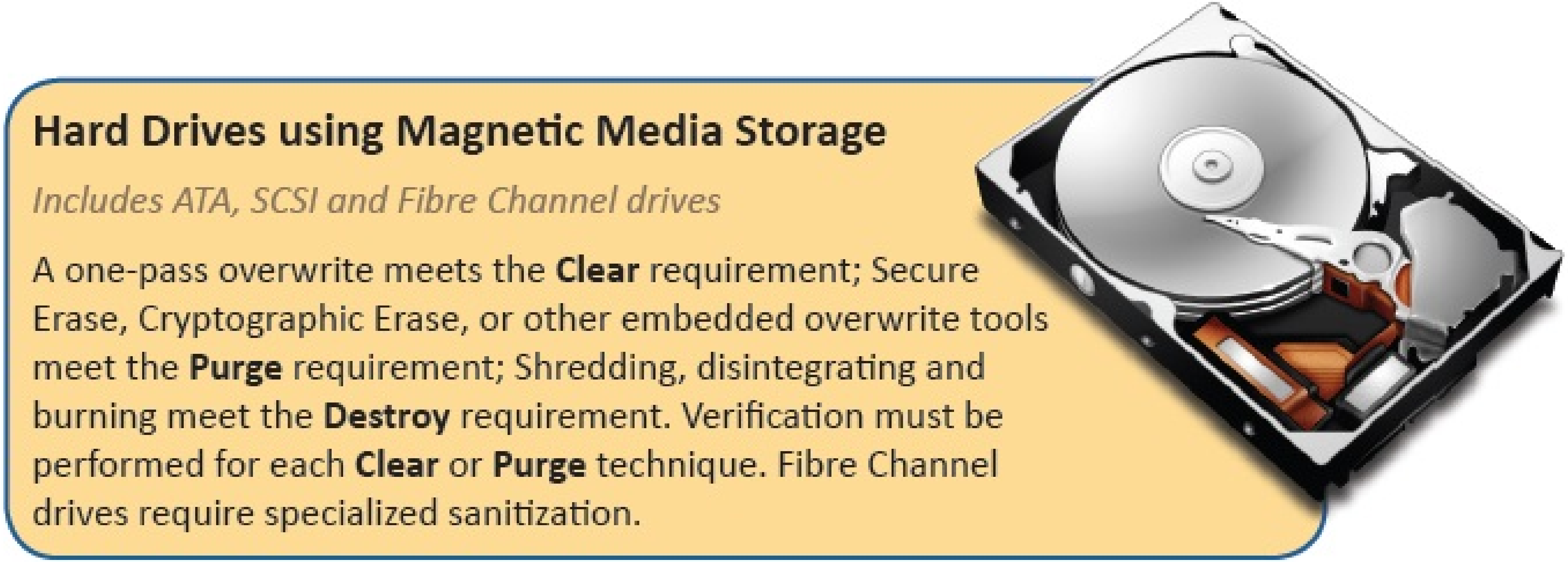
Sanitization methods for various media

Networking Devices

Includes routers and switches

Routers and switches may contain IP addresses and other identifiable information that can facilitate hacking into a network. The **Clear** method of sanitization involves performing a full manufacturer's reset back to default factory settings. **Purge** may be available on some devices using block erasing. **Destroy** is achieved through shredding.

Sanitization methods for various media

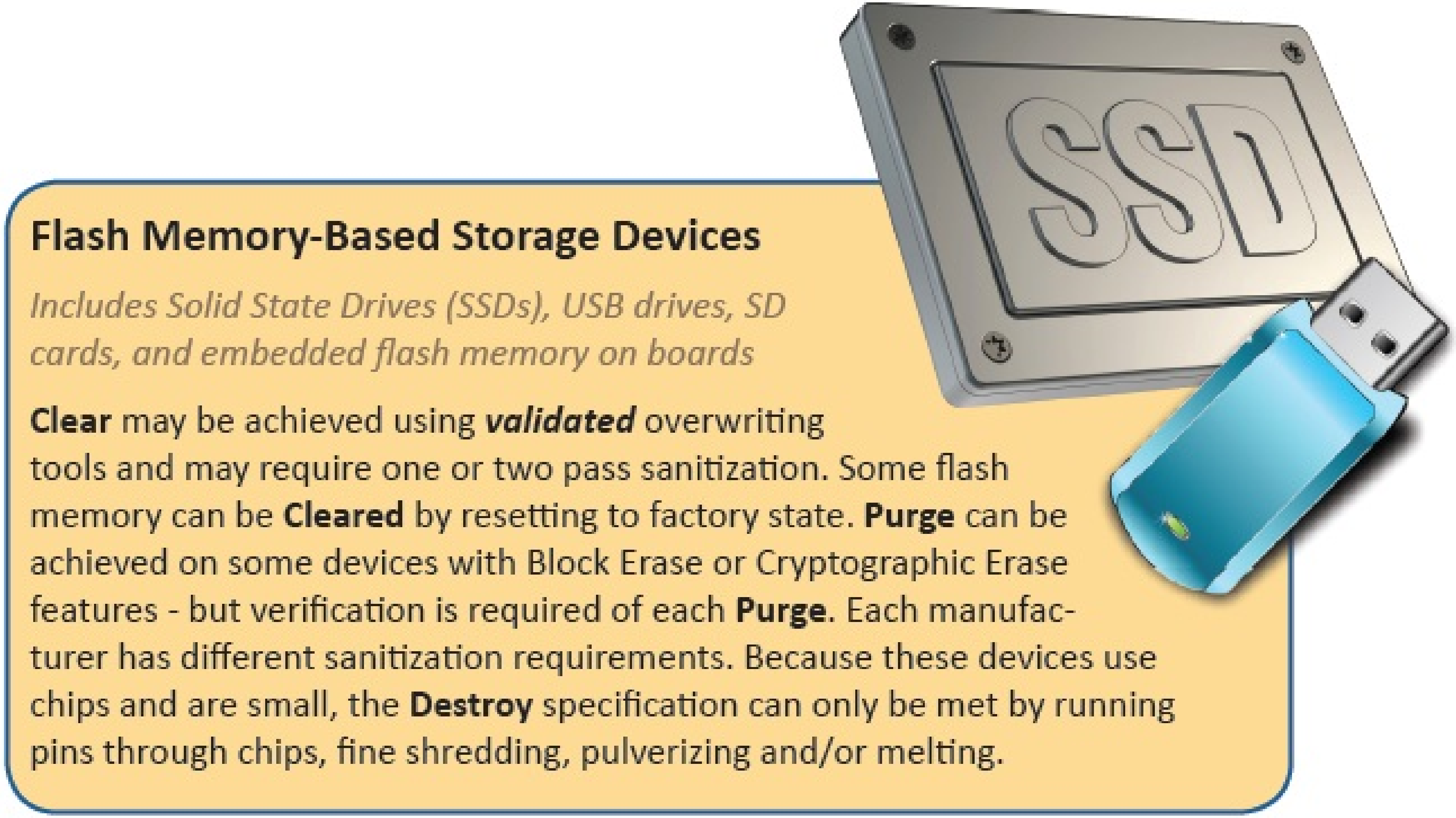


Hard Drives using Magnetic Media Storage

Includes ATA, SCSI and Fibre Channel drives

A one-pass overwrite meets the **Clear** requirement; Secure Erase, Cryptographic Erase, or other embedded overwrite tools meet the **Purge** requirement; Shredding, disintegrating and burning meet the **Destroy** requirement. Verification must be performed for each **Clear** or **Purge** technique. Fibre Channel drives require specialized sanitization.

Sanitization methods for various media



Flash Memory-Based Storage Devices

Includes Solid State Drives (SSDs), USB drives, SD cards, and embedded flash memory on boards

Clear may be achieved using ***validated*** overwriting tools and may require one or two pass sanitization. Some flash memory can be **Cleared** by resetting to factory state. **Purge** can be achieved on some devices with Block Erase or Cryptographic Erase features - but verification is required of each **Purge**. Each manufacturer has different sanitization requirements. Because these devices use chips and are small, the **Destroy** specification can only be met by running pins through chips, fine shredding, pulverizing and/or melting.

Sanitization methods for various media

Mobile Devices with Flash Memory

Includes smart phones and tablets

Clear or **Purge** can generally be achieved by resetting to factory settings and/or selecting a full sanitize (“Erase All Content”) option. Each manufacturer and Operating System requires a unique sanitization process. **Destroy** by shredding (remove batteries first!) - Ensure SIM cards are removed and destroyed as well.

Which type of sanitization level to choose?

Potential Impact Analysis:

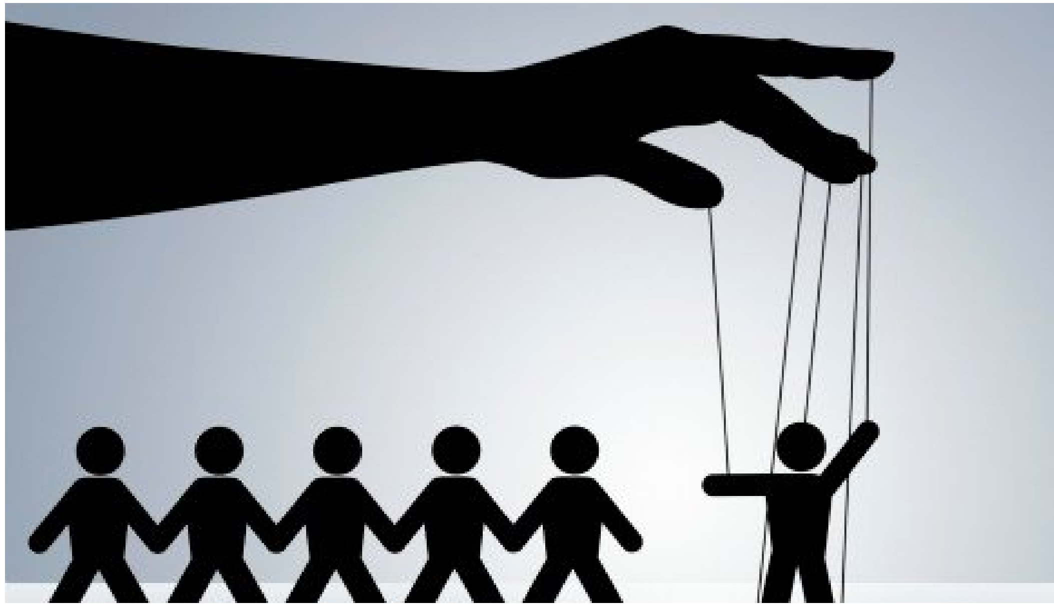
Potential Impact	Definitions
Low	Loss of confidentiality, integrity, or availability could be expected to have a ***limited*** adverse effect on organizational operations, organizational assets, or individuals.
Moderate	Loss of confidentiality, integrity, or availability could be expected to have a ***serious*** adverse effect on organizational operations, organizational assets, or individuals.
High	Loss of confidentiality, integrity, or availability could be expected to have a ***severe or catastrophic*** adverse effect on organizational operations, organizational assets, or individuals.

NIST FIPS 199 Standards for Security Categorization of Federal Information and Information Systems

Where will data bearing devices go?

Under Organizational Control:

- Media are considered under organizational control if contractual agreements are in place with the organization and the [vendor] specifically provides for the confidentiality of the information.
- "Maintenance" being performed on an organization's site, under the organization's supervision.



Not Under Organizational Control:

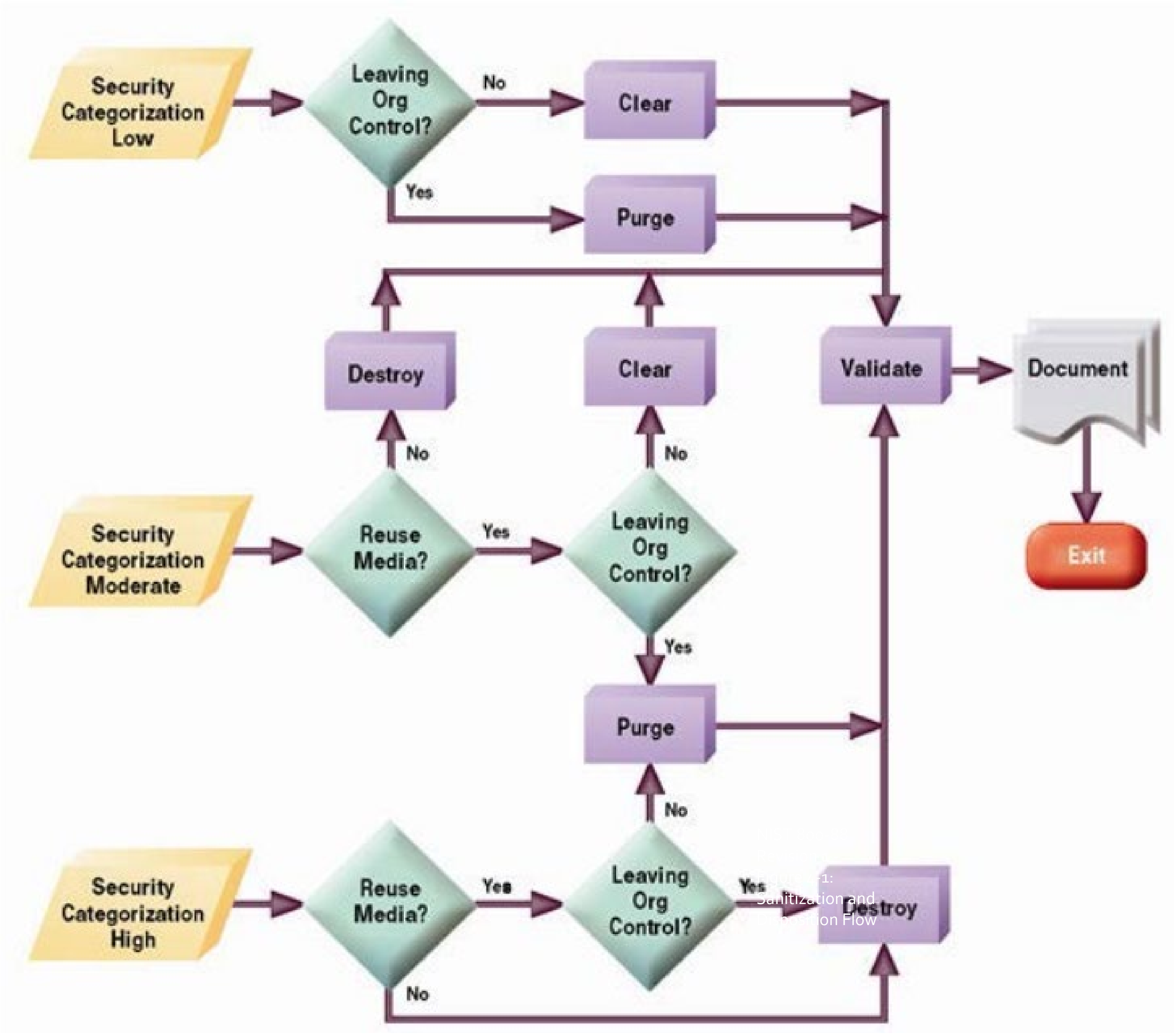
- Media exchanged for warranty, cost rebate, or other purposes and where the specific media will not be returned to the organization.

Using NIST Guidelines to build your data destruction program

- Identify data storage media
- What is the organization’s control of data (internal/external)?
- What is the potential impact of loss of data
- Assign the correct sanitization level
  - Types of media
  - What info may be on media (potential impact)
  - Who controls media

NIST 800-88

Guidance on Sanitization and Disposition Decisions



NIST 800-88 Revision 1

Figure 4-1: Sanitization and Disposition Flow

CASCADE ASSET MANAGEMENT

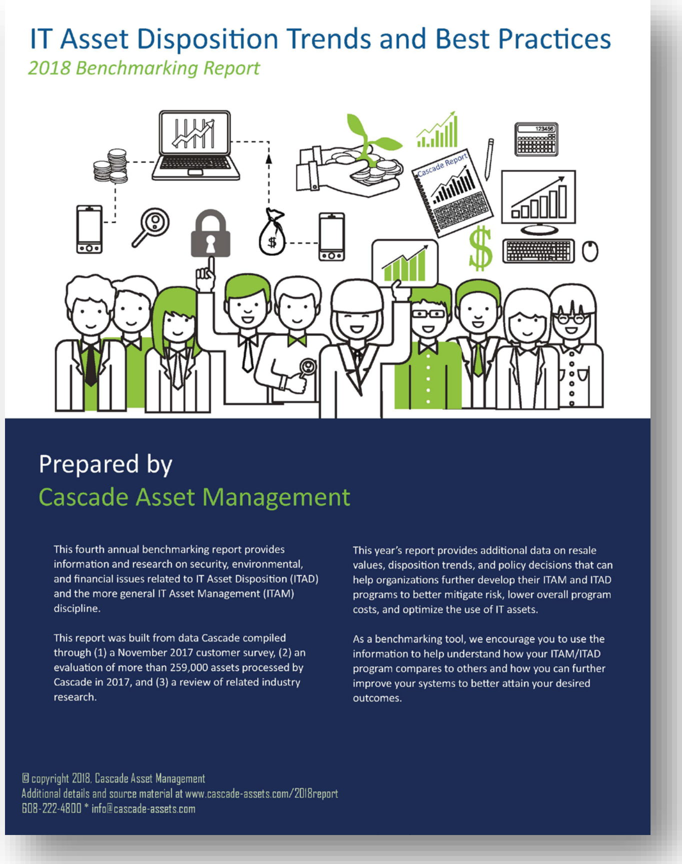
NIST 800-88

Use NIST guidelines to:

- Set a policy for managing data risk on retired, repurposed and reused assets
- Provide a comprehensive review of what data bearing devices you own and manage
- Develop and implement training and controls (including sanitization methods) consistent with policy
- Ensure proper implementation within and outside of the organization's control

Elements of a data security management program

- Multi-stakeholder involvement
- Understanding of risks
- Comprehensive Policies and Procedures
- Tools to manage assets throughout their lifecycle
- Training and accountability of staff to implement processes
- Integrated solutions with providers
- Processes to evaluate and continually improve
- Separate data security element from value recovery goals



IT Asset Disposition Trends and Best Practices

2018 Benchmarking Report

Prepared by

Cascade Asset Management

This fourth annual benchmarking report provides information and research on security, environmental, and financial issues related to IT Asset Disposition (ITAD) and the more general IT Asset Management (ITAM) discipline.

This report was built from data Cascade compiled through (1) a November 2017 customer survey, (2) an evaluation of more than 259,000 assets processed by Cascade in 2017, and (3) a review of related industry research.

This year's report provides additional data on resale values, disposition trends, and policy decisions that can help organizations further develop their ITAM and ITAD programs to better mitigate risk, lower overall program costs, and optimize the use of IT assets.

As a benchmarking tool, we encourage you to use the information to help understand how your ITAM/ITAD program compares to others and how you can further improve your systems to better attain your desired outcomes.

Additional details and source material at www.cascade-assets.com/2018report
608-222-4800 * info@cascade-assets.com

Neil Peters-Michaud

Cascade Asset Management

npm@cascade-assets.com

www.cascade-assets.com

CASCADE
ASSET MANAGEMENT