ACE 2020

IAITAM NASHVILLE·TN

BRINGING YOUR BUSINESS INTO FOCUS

There's a lot to lose when shredding your hard drives

Neil Peters-Michaud, CEO
Cascade Asset Management

CASCADE ASSET MANAGEMENT

IAITAM

There’s a lot to lose . . . from shredding

Agenda

1. Value choices to shred vs. wipe drives
2. Understanding data sanitization technology
3. Customer case study
4. Recommendations

Speaker Bio

- Neil Peters-Michaud
- CEO, Cascade Asset Management
- 25 year ITAD/ITAM career
- Univ. of Wisconsin surplus mngr
- CHAMP, MBA
- iNEMI HDD value recovery team

IAITAM

ACE 2020 NASHVILLE·TN

CASCADE ASSET MANAGEMENT

Vendor names provided as an example (others are available)

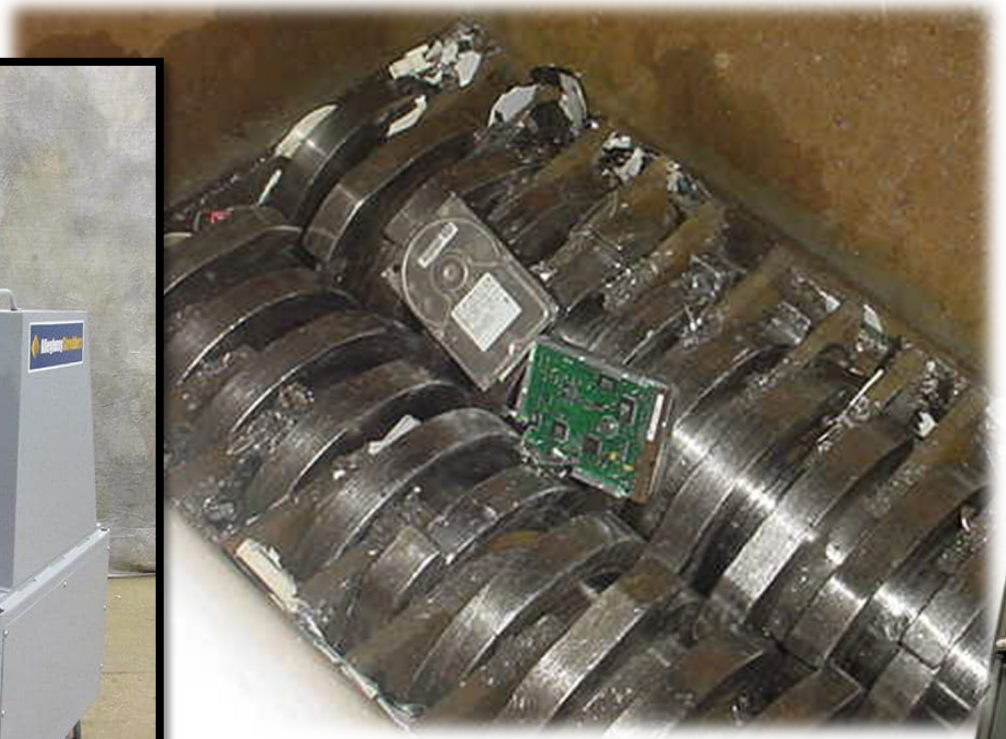
Electronic sanitization tools

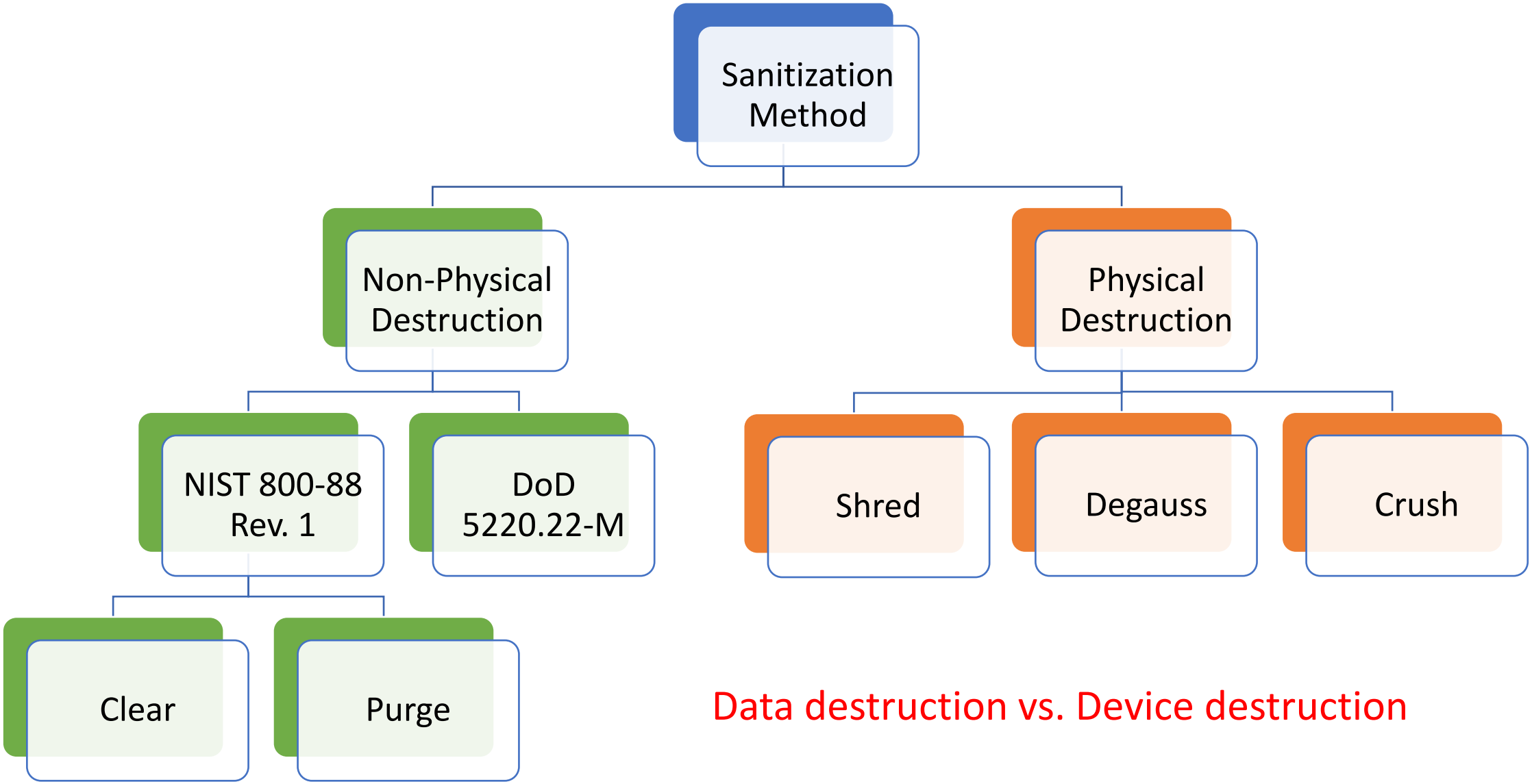
WHITE CANYON SOFTWARE

EPS Extreme Protocol Solutions

phonecheck

Media shredding





Data destruction vs. Device destruction

iNEMI
International Electronics Manufacturing Initiative

DEMONSTRATION PROJECT 5: CREATING A BUSINESS MODEL TO SUPPORT REUSE & RECOVERY

DEMONSTRATION PARTICIPANTS

Carleen Matuska, Microsoft
Ines Sousa, Google
Ikenna Ike, Google
Hongyue Jin, University of Arizona
Neil Peters-Michaud, Cascade Asset Management

LEADERS

Gary Spencer, GEODIS SCO USA
Carol Handwerker, CMI, Purdue University

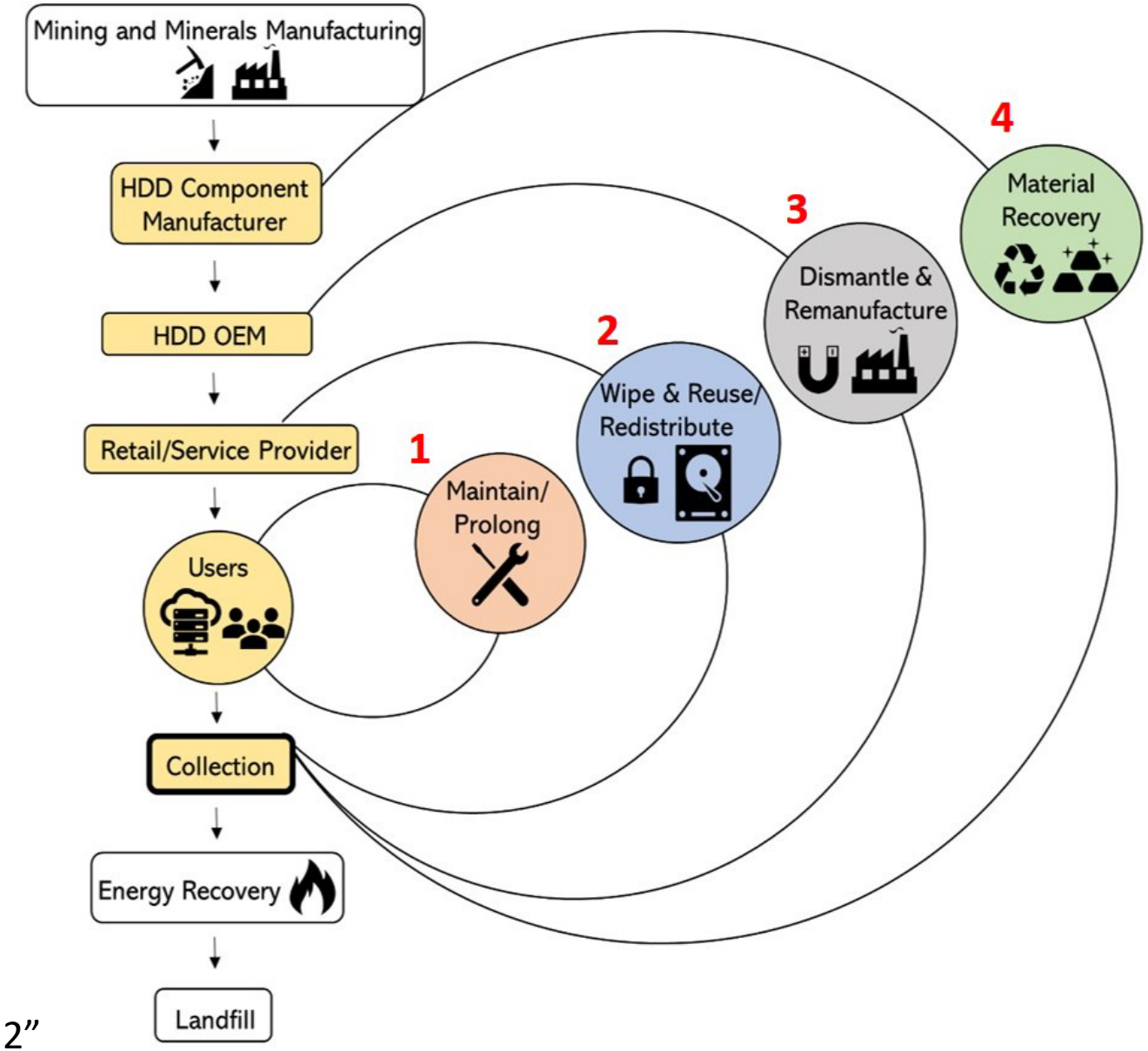
IAITAM

IAITAM ACE 2020 NASHVILLE·TN

CASCADE ASSET MANAGEMENT

Circular economy

Move from a linear “use and dispose” model to one that recovers value throughout the lifecycle process.

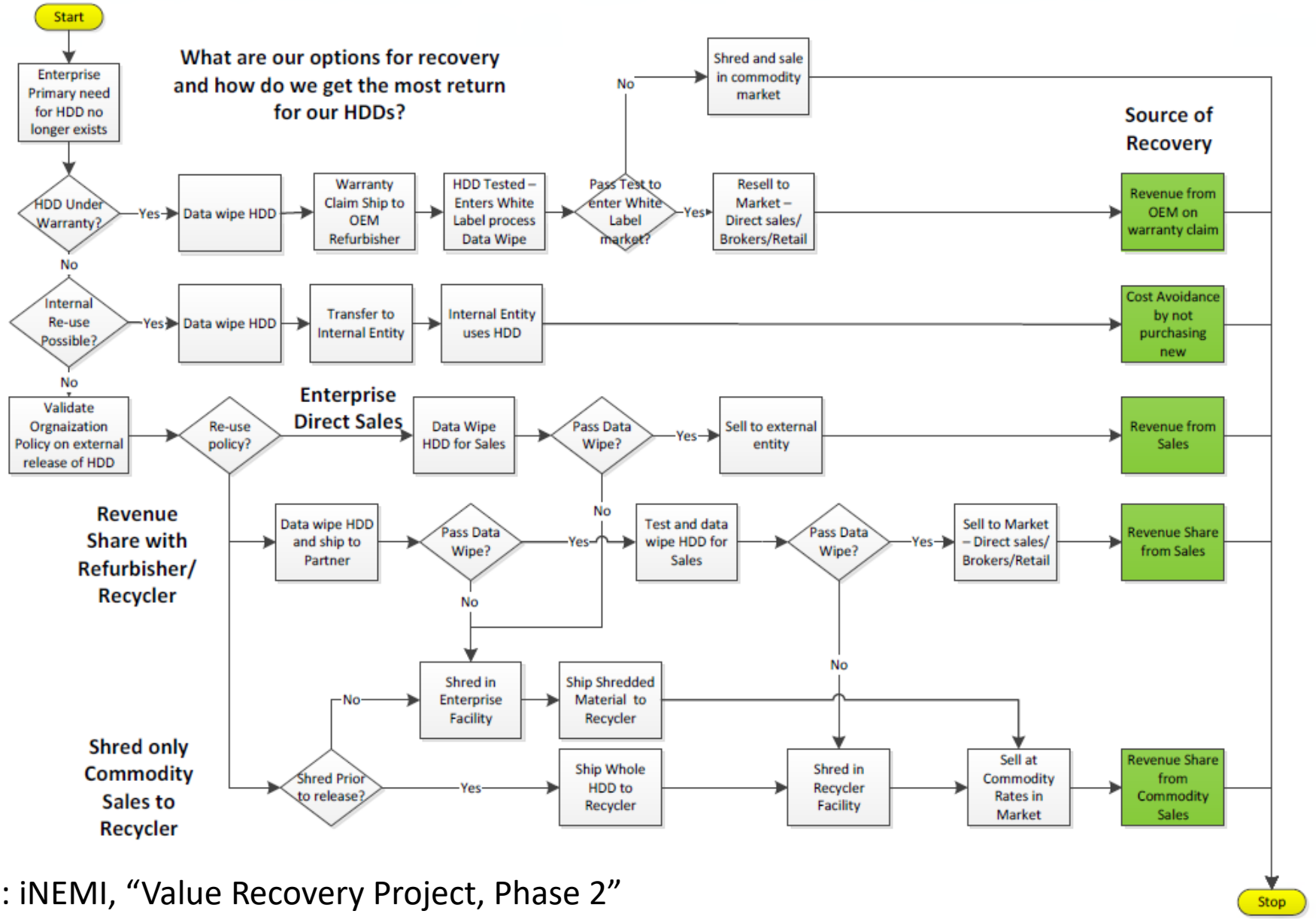


Source: iNEMI, “Value Recovery Project, Phase 2”

REFURBISH / REMANUFACTURE:

Once servers from data centers are decommissioned, they are sent back to the central hub. At the hub servers are dismantled and de-kitted to their usable components (CPU, motherboard, Flash devices, hard disks, memory modules and other components). After quality inspection, components are stored to be reused as refurbished inventory.

Google custom builds its own servers for data centers through a program called the Servers Build program. Refurbished parts (mentioned above) are used to build remanufactured servers and are then deployed back into data centers. In Google data centers, there is a mix of the servers running the latest technology platforms and also older platforms. Once components are in inventory, there is no distinction made between refurbished and new inventory, both are considered equivalent.



Source: iNEMI, “Value Recovery Project, Phase 2”

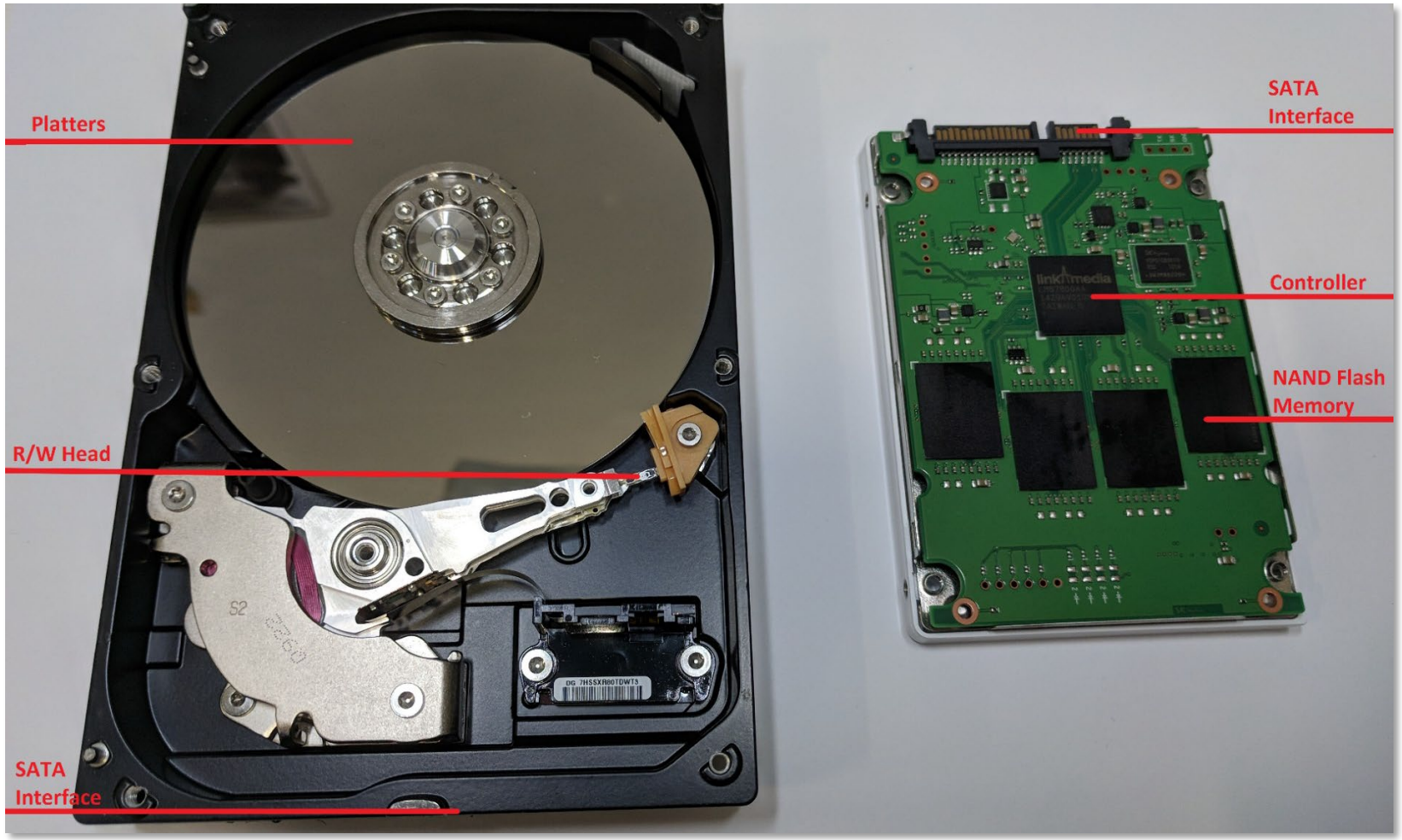
Example value of a 1 TB 3.5" HDD

Recovery Method	Value As Is?	Re-Use Method	Value when recovered
Warranty Claim	No – needs refurbished	Refurbish and resale as White Label drive – prorated value	$10 to $35
Internal Re-use	Yes	Data Wipe and avoid purchase of new drive	$42
Enterprise Direct Sales	Yes	Data wipe and directly manage retail sales	$22
Revenue Share with Recycler	Yes	Data wipe and have Recycler manage sales – 50% share back model	$11
Shred for Commodities	No – needs to be shredded	Shred drive for commodity recovery – mixed aluminum	$0.44

*Value recovered does not include bundled within a server, which could drive the individual value of the drive higher

Source: iNEMI, "Value Recovery Project, Phase 2," August 2019

Understanding data sanitization technology



Examples of different storage media form factors

Hard Drive Disk

- Records data on platters
- Available in different sizes
  - Most common sizes are 3.5” and 2.5”
- Common types of interfaces:
  - SATA, IDE, SCSI, Fibre Channel

HDD 3.5”

HDD 2.5”

HDD 1.8”

Examples of different storage media form factors

Solid State Drive

- Records data on memory chips
- Available in many different form factors and sizes
- Many available interfaces:
  - SATA, M.2, PCIe, mSATA, etc.

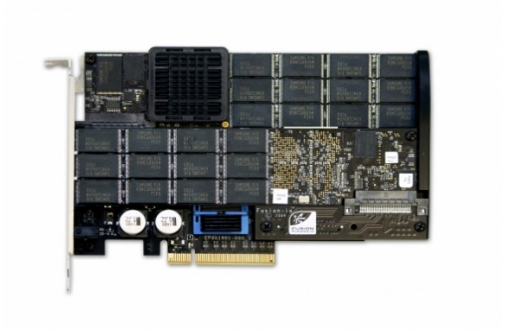
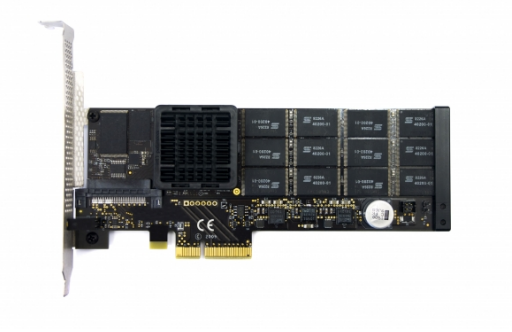
2.5 inch SSD

M.2 SSD

mSATA SSD

Examples of different storage media form factors

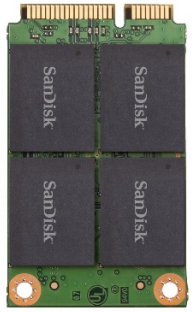
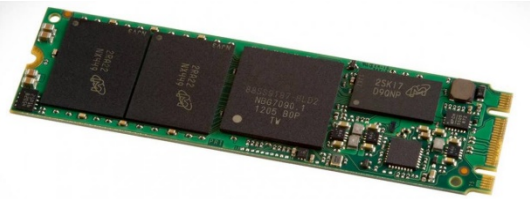
Solid State Cards – PCIe Form Factor Examples

Full Height/Half Length	Low Profile
	

» These are often found in PCs and Servers

Examples of different storage media form factors

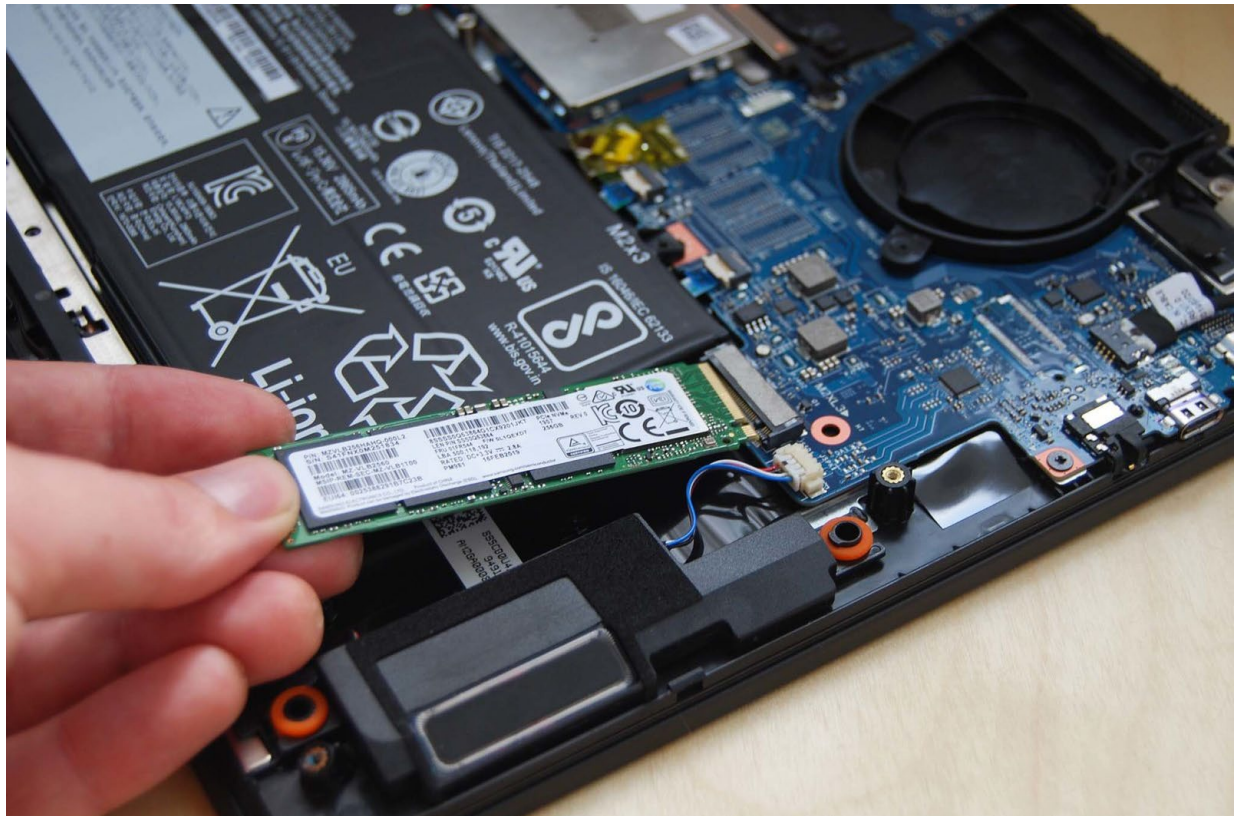
Solid State Modules – mSATA, etc.

mSATA	mSATA Mini	M.2
		

» These are often found in laptops (often under the back panel)

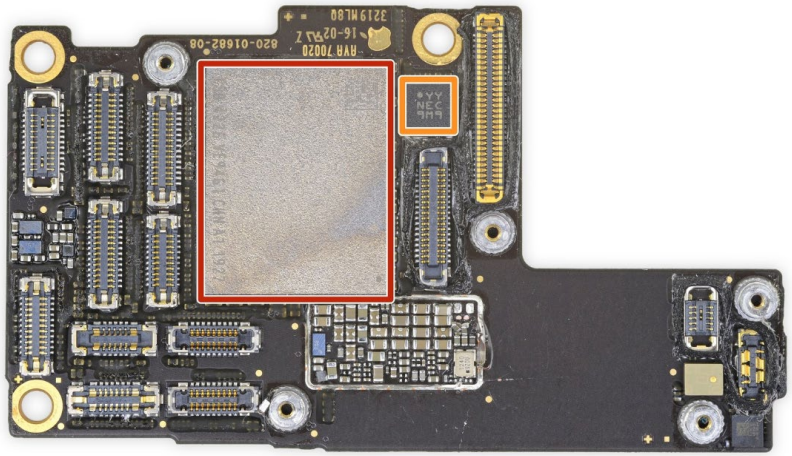
Examples of different storage media form factors

Solid State Modules – M.2 in laptop



Examples of different storage media form factors

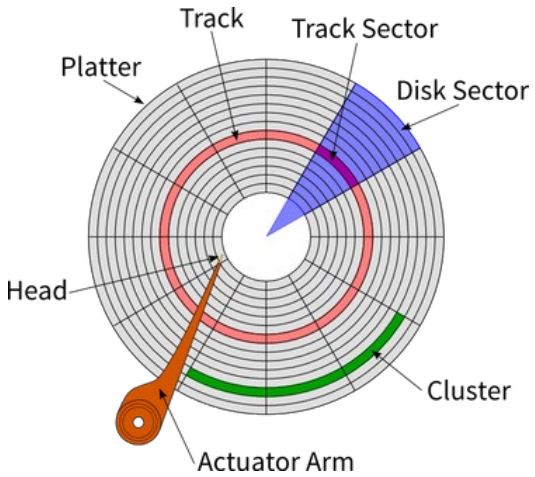
Solid State Drives – iPhone 11

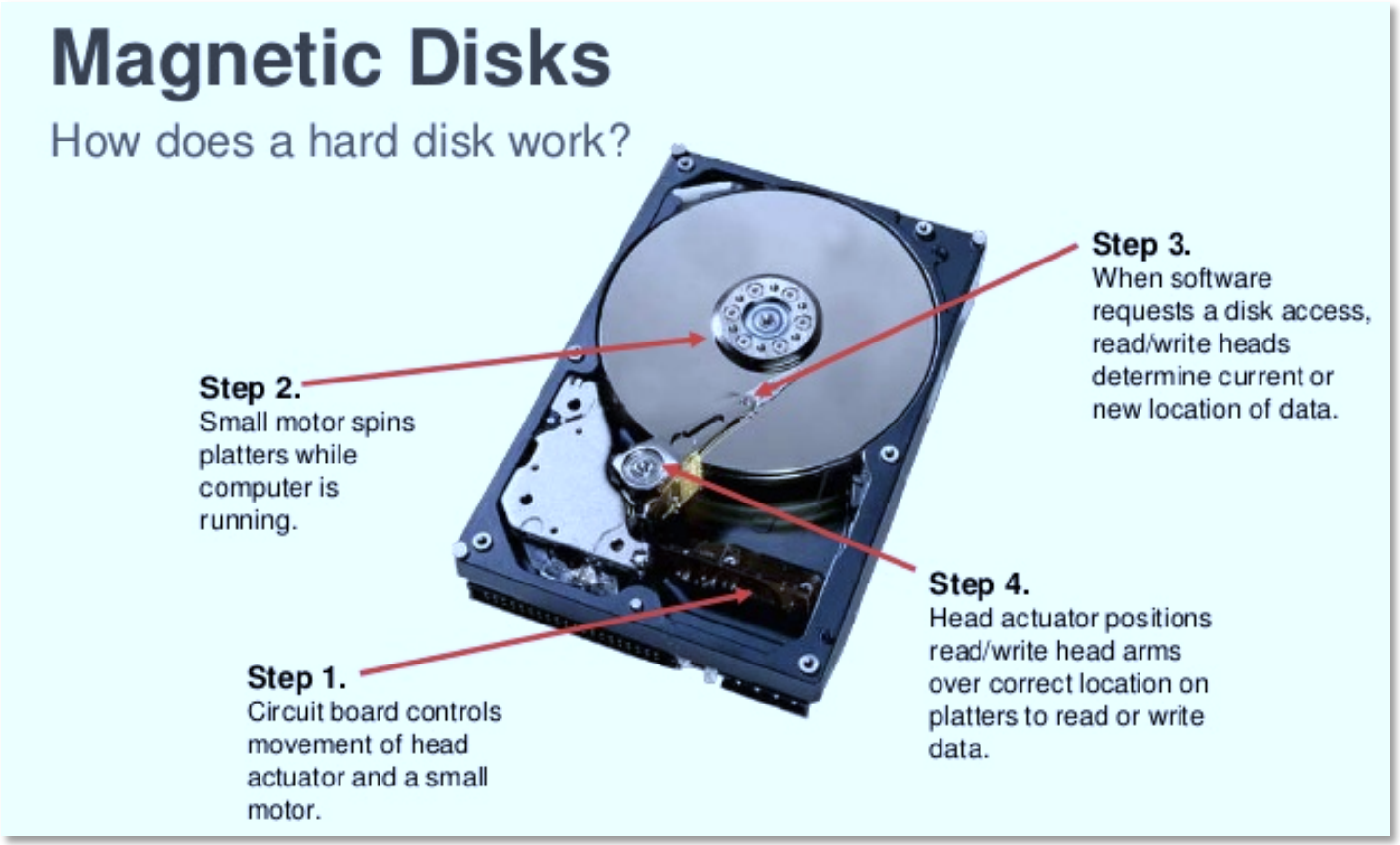


Difference in how hardware stores information

Hard Drive Disks

- Use **magnetic** recording
- Reads/writes bits (1s & 0s) by changing polarity of bits on the platter

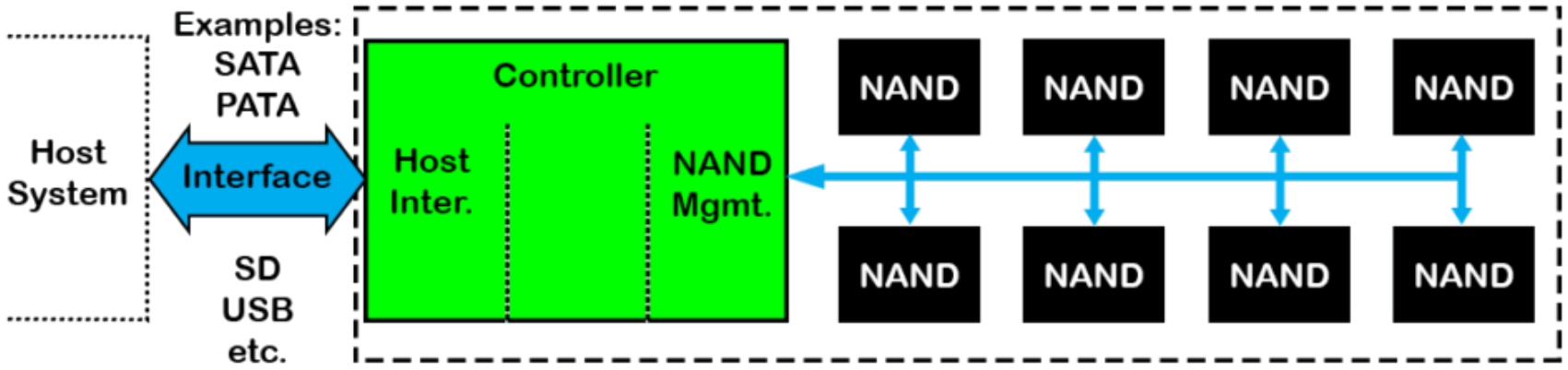




Difference in how hardware stores information

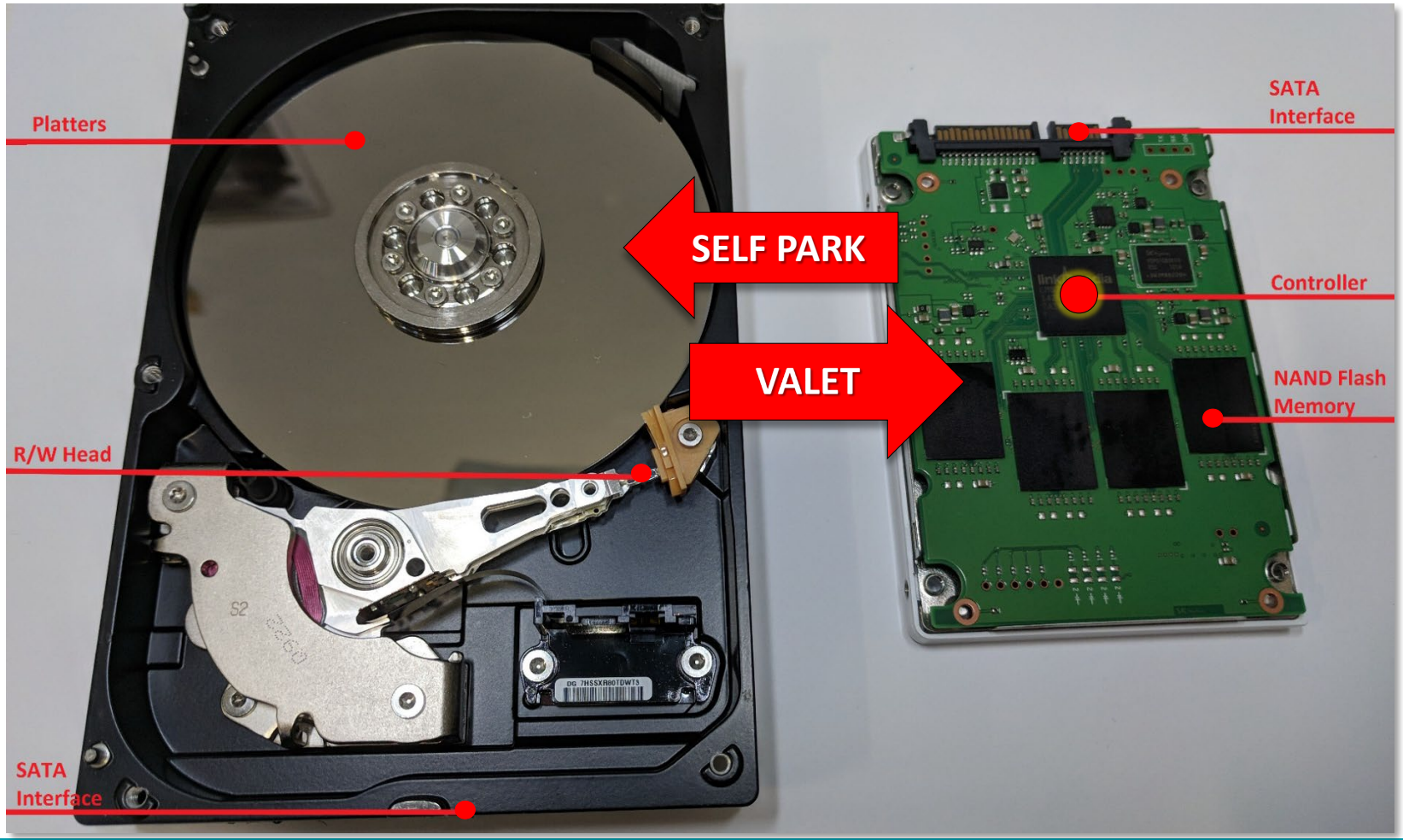
Solid State Drives

- Use **flash** memory
- Reads/writes bits (1s & 0s) using electrons that are charged or not charged
- Similar to RAM but is non-volatile memory (NVRAM) meaning it retains information after the device is powered off



Basic Solid State Drive (SSD) Architecture

Sanitization methods for media – limitations & risks



Effective data sanitization options

PROPER

Physical Destruction

The process of shredding hard drives, smartphones, printers, laptops and other storage media into tiny pieces.

Cryptographic Erasure (Crypto Erase)

The process of using encryption software (either built-in or deployed) on the entire data storage device, and erasing the key used to decrypt the data.

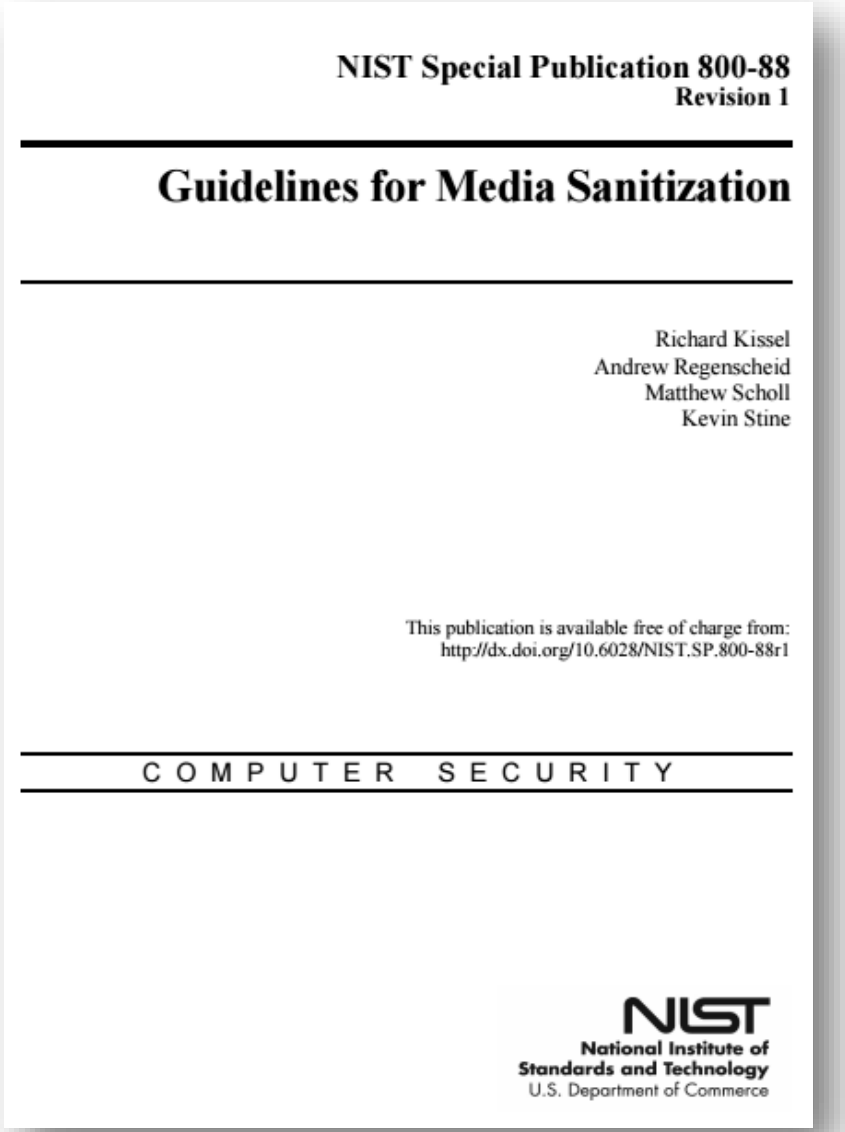
Data Erasure

The software-based method of securely overwriting data from any data storage device using zeros and ones onto all sectors of the device.

Graphic from International Data Sanitization Consortium, https://www.datasanitization.org/

Developing your sanitization policy

"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

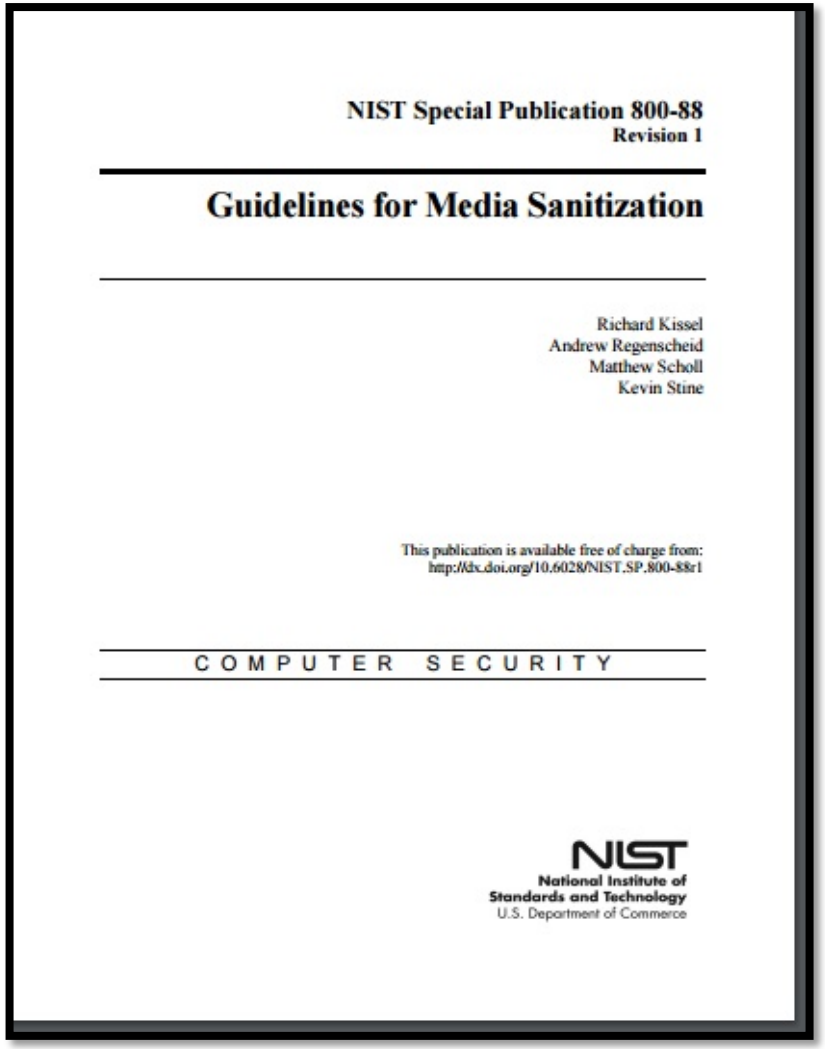
- Practical, real world reference for media sanitization guidance and compliance
- Introduced in 2006, updated Dec, 2014 (Revision 1) to address changing technologies
- Replaced DoD 5220.22M standard in regulatory and certification practice
- Referenced in many other security rules, regulations and standards

NIST 800-88 sanitization levels

- **Clear** uses software or hardware products to overwrite user-addressable storage space on media with non-sensitive data. Manufacturer resets and procedures that do not include rewriting might be the only option to Clear the device. Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust **keyboard attack.**

- **Purge** may be an overwrite, block erase, or Cryptographic Erase through the use of dedicated, standardized device sanitize commands that apply media-specific techniques to bypass the typical read and write commands. Purging information is a media sanitization process that protects the confidentiality of information against a **laboratory attack**.

- **Destroy** is a physical process that makes data retrieval infeasible using state of the art laboratory techniques. Destruction methods include shredding, incineration, melting and pulverizing. Degaussing is also considered a destruction technique when used properly.


NIST Special Publication 800-88
Revision 1

Guidelines for Media Sanitization

Richard Kissel
Andrew Regenscheid
Matthew Scholl
Kevin Stine

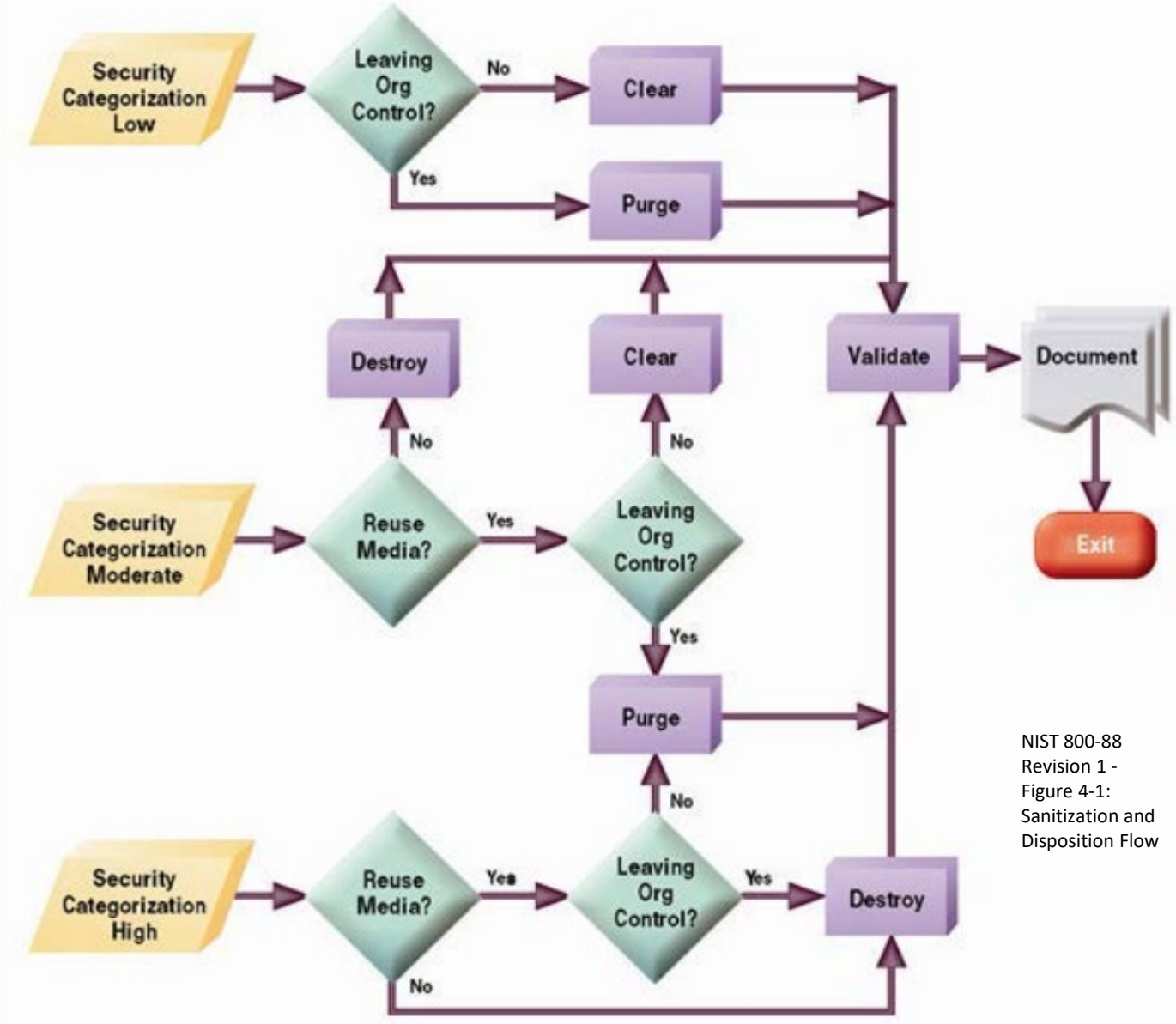
This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-88r1

COMPUTER SECURITY

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

NIST 800-88

Guidance on Sanitization and Disposition Decisions



NIST 800-88 Revision 1 - Figure 4-1: Sanitization and Disposition Flow

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

Compliance with privacy laws

The Criminal Justice Information Services (CJIS) Security policy allows for data sanitization of digital media after a 3 pass wipe.

The FTC manages FACTA and allows for electronic media sanitization.

IRS Publication 1075 allows for media to be sanitized by electronically "purging" the data prior to reuse.

HHS governs HIPAA and allows for "clearing" or "purging" to safeguard personal health information.

Case study: changing from drive shred to reuse

- Healthcare organization
- Security policy – remove, inventory, and shred all drives from desktops, laptops, and servers
- Environmental interest – reuse is better than recycling
- Hard drives shipped to Cascade loose or in devices
  - 10,929 loose hard drives received (2016 to 2019) – all inventoried then shredded at a cost of about $45,000
  - 11,704 laptops and desktops refurbished and resold – 55% included drives from client that were removed and shredded
  - Additional devices demanufactured and recycled (obsolete/damaged)

The opportunity cost of shredding drives

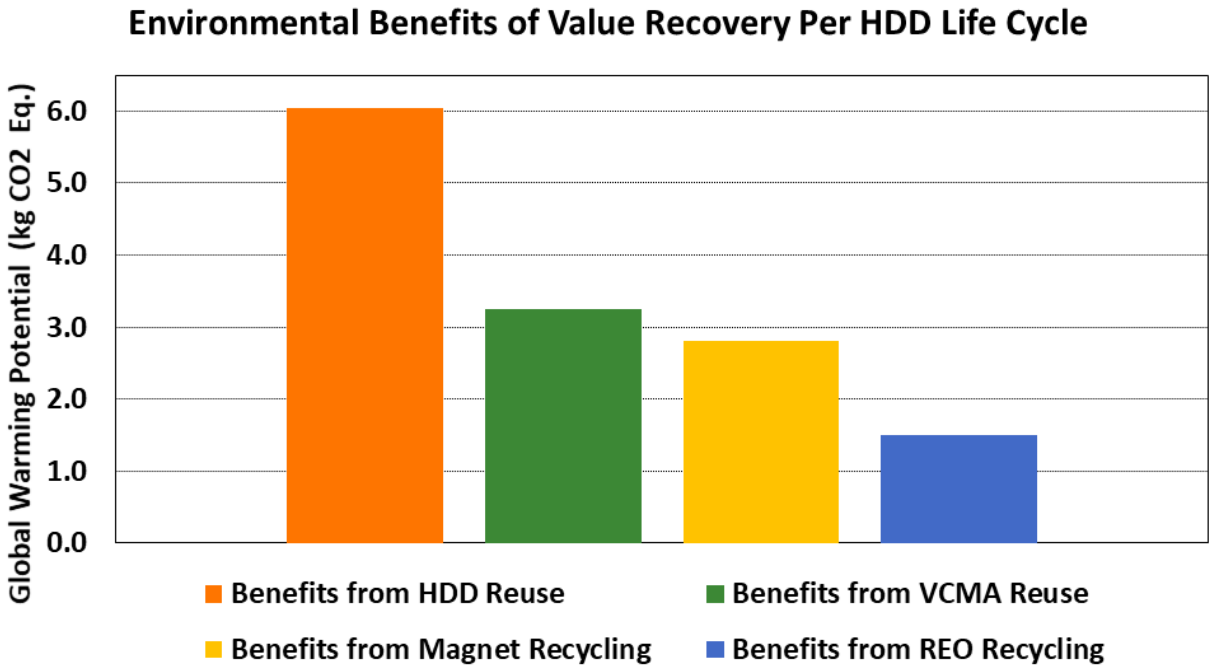
	Year (quantities)					
Disposition, HDD status, device	2016	2017	2018	2019	Total	Lost Revenue from missing HDDs
Hard drive removed by Cascade	343	573	753	4,724	6,393	$35,162
Computing Device	314	499	575	3,860	5,248	$28,864
Laptop Computer	29	71	177	847	1,124	$6,182
No hard drive in device	1,136	1,108	1,681	1,386	5,311	$29,211
Computing Device	963	659	1,108	950	3,680	$20,240
Laptop Computer	173	434	572	435	1,614	$8,877
Refurbished and Resold devices	1,479	1,681	2,434	6,110	11,704	**$64,373**

10,929 loose drive potential lost value

Hard drive replacement value ~ $5.50 each

- **$40,000** additional inventory/processing costs (vs. keeping drives in devices)
- If these drives could have been sold, resale revenue = **$60,000**

Environmental Impact

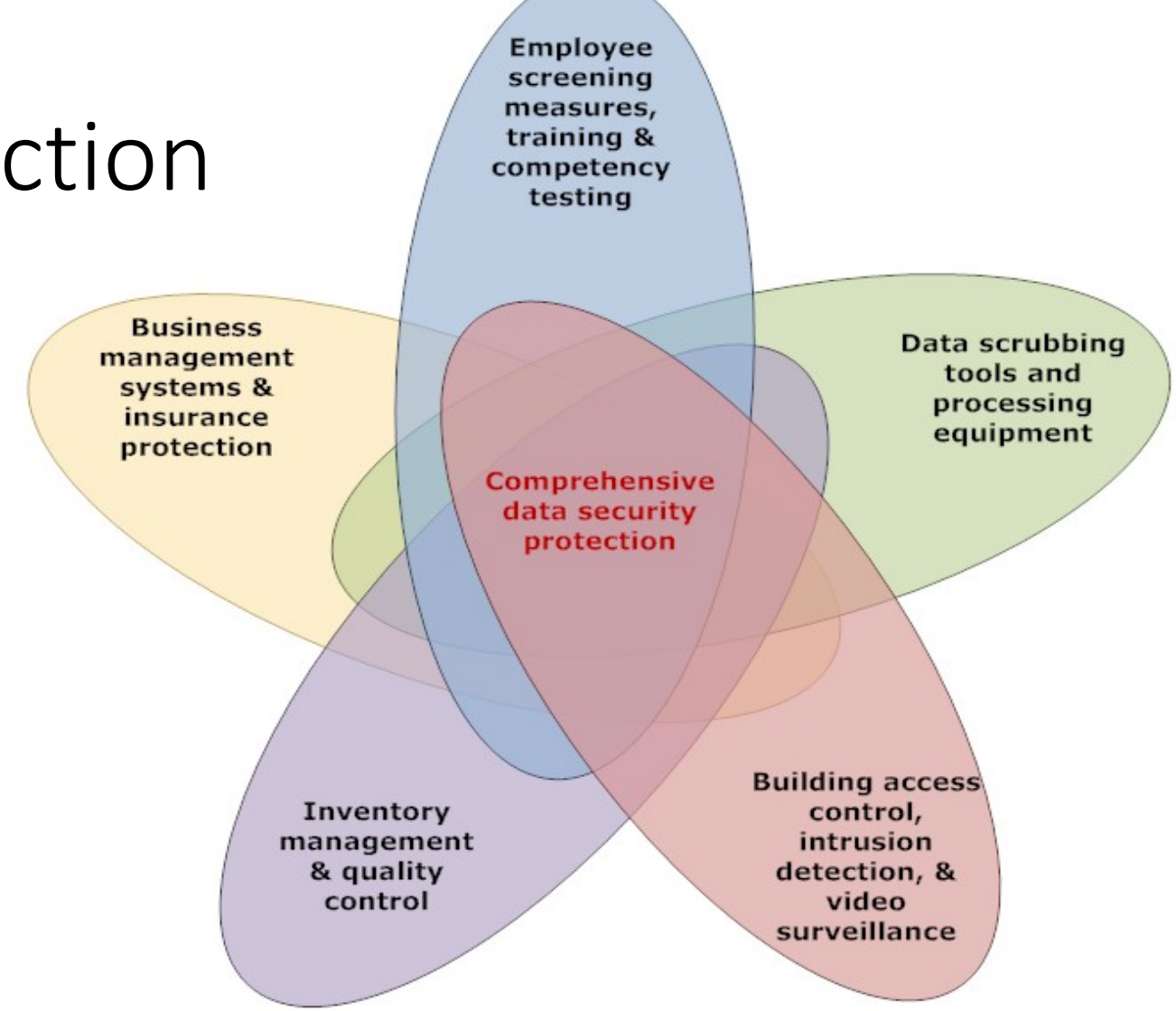


International Electronics Manufacturing Initiative (iNEMI), "Value Recovery from Used Electronics Project, Phase 2", July 2019

Case study environmental impacts		
Number of HDDs removed/loose & shredded	17,322	
Enviro benefit per reused drive (vs. disposal)	6.00	kg CO_2
Enviro benefit per shredded/recycled drive	0.02	kg CO_2
Net enviro impact of reuse vs. recycle	5.98	kg CO_2
Total net carbon savings of reuse vs. (kg)	103,586	kg CO_2
Total net carbon savings of reuse vs. (tons)	**51.79**	**tons CO_2**

Equivalent to keeping 84 cars off the road for one year

Layers of security protection



Considerations when selecting data sanitization methods

- Multi-stakeholder involvement (IT, security, sustainability, procurement)
- Understand the risks of data loss throughout lifecycle of products
- Define a data security policy consistent with risk tolerance and compliance requirements
- Determine value recovery goals and opportunities within security framework
- Integrate solutions with providers
- Evaluate risks and returns to continually improve

Thank You

Neil Peters-Michaud
CEO
Cascade Asset Management
npm@cascade-assets.com
608-316-6637