# ! A; MD9J " JAN= 'FAA9LAN=

Jonmichael Hands, Secretary CDI, Member IEEE SISWG

# The current state of storage security...

## “We shred everything”

Data leak

Encryption

Trust

Policies & Risk

Privacy

2XzJ̉
zìXXä Xãöî

Security

# The future state of storage security…

## “We lead in circularity”

Robotics for Recovery

Encryption & Sanitization

Trust Assurance

Policies for Risk Mgmt

EJ̓ §X
>Xî J̓ X

Update Legal Agreements

# Mobilizing the Industry

## Cooperate - Innovate - Educate - Mobilize

### ; JìöãXíî| Äêî

, ©êXíîNJ Xíî
$çä ê§öXí #ìJãTî
8 ( 5 î
.A &î
>XNç¶Xí©; JìöãXíî

### Standards

Data Security
Cryptography
Sanitization
Data Privacy & Protection

### Best Practices

Sanitization
GHG Reduction
Circulatory Processes

### Alliances

IEEE SISWG
OCP Security, Storage, and Sustainability
SNIA
SERI
International Data Sanitization Consortium

### Reporting

GHG Reduction
Landfill Diversion
Value Recovery
Resource Efficiency

### Verification

Security
Erasure
Companies
Grading

# CDI Projects

- Media Sanitization
  - Guidelines
  - Training
- Health Grading Tool
  - Alpha working
- Academic Research
  - Media sanitization
  - Health grading
  - Carbon impact (MSFT)
- Carbon accounting
- Alliances – OCP, SNIA, IEEE, Adisa

# CDI Security, Cryptography, Sanitization, Verification

Circular Drive Initiative

IEEE 2883 Purge
Media Sanitization

IEEE 2883 Verification

.?8 –.( $ □∘ ℅□ ℅
$ Xîḟ ` NJöXçZ
?JãÄ̈ ™Jḟ çã

Hardware roots of trust
Firmware audits
Forensic Analysis

IEEE SA STANDARDS ASSOCIATION

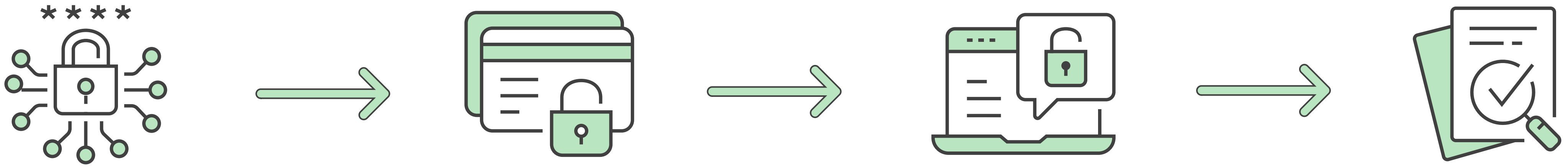
ISO IEC

OPEN Compute Project®

ADISA®

# CDI Media Sanitization

Circular Drive Initiative



Use IEEE 2883 approved purge technique

Check Sanitize Log

Perform verification on host interface

%=F=J9L= ;=JLA>A;9L= G>
K9FALAR9LAGF

# Roadmap – Increase Trust

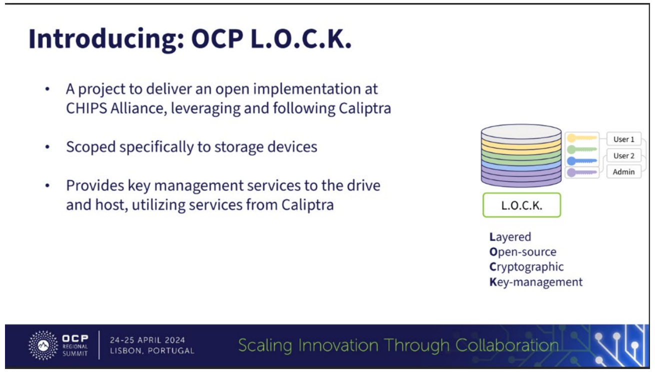
Vendor validation of sanitize

Certifications, TCG OPAL, FIPS 140-3

3rd party audit

Firmware attestation / measurement, hardware roots of trust

# Roadmap - OCP



## Introducing: OCP L.O.C.K.

- A project to deliver an open implementation at CHIPS Alliance, leveraging and following Caliptra
- Scoped specifically to storage devices
- Provides key management services to the drive and host, utilizing services from Caliptra

User 1
User 2
Admin
L.O.C.K.

**L**ayered
**O**pen-source
**C**ryptographic
**K**ey-management

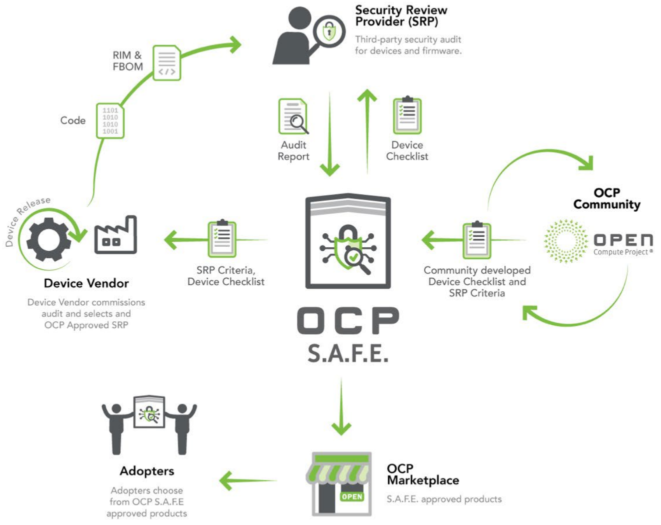
OCP REGIONAL SUMMIT | 24-25 APRIL 2024 LISBON, PORTUGAL Scaling Innovation Through Collaboration

- ! . * - ! )

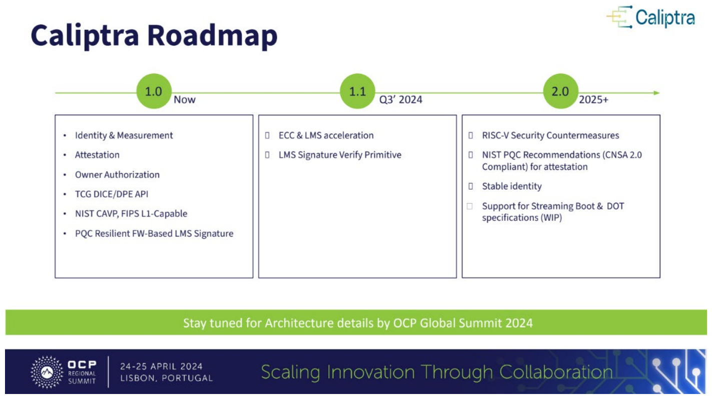
! 9DAHLJ9 ➡️ ) + . ) =Q+ 9F9?=E =FL

DG; Ç ➡️ 1LGJ9?=! GFLJGDD=J $AE O9J=

➡️ #1 ! JQHLG#F?AF=


Security Review Provider (SRP)
Third-party security audit for devices and firmware.
RIM & FBOM
Code
1101 1010 1010 1001
Audit Report
Device Checklist
Device Release
Device Vendor
Device Vendor commissions audit and selects and OCP Approved SRP
SRP Criteria, Device Checklist
OCP S.A.F.E.
OCP Community
OPEN Compute Project
Community developed Device Checklist and SRP Criteria
Adopters
Adopters choose from OCP S.A.F.E approved products
OCP Marketplace
OPEN
S.A.F.E. approved products

OCP S.A.F.E. Update



## Caliptra Roadmap

| 1.0 Now | 1.1 Q3’ 2024 | 2.0 2025+ |
|---|---|---|
| Identity & Measurement<br>Attestation<br>Owner Authorization<br>TCG DICE/DPE API<br>NIST CAVP, FIPS L1-Capable<br>PQC Resilient FW-Based LMS Signature | ECC & LMS acceleration<br>LMS Signature Verify Primitive | RISC-V Security Countermeasures<br>NIST PQC Recommendations (CNSA 2.0 Compliant) for attestation<br>Stable identity<br>Support for Streaming Boot & DOT specifications (WIP) |

Stay tuned for Architecture details by OCP Global Summit 2024

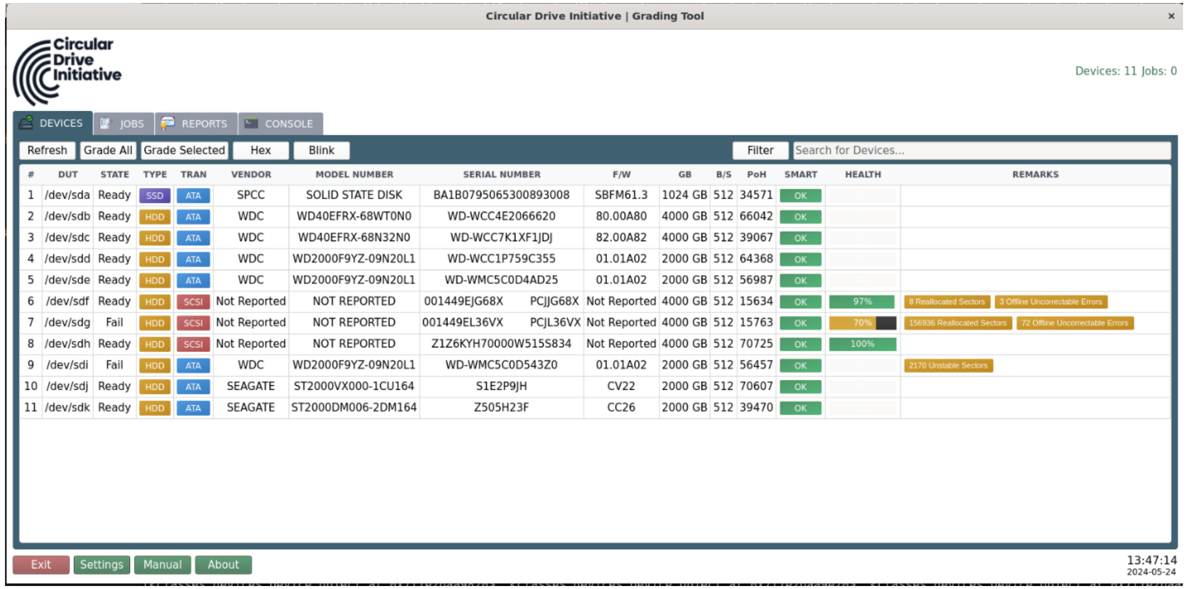
OCP REGIONAL SUMMIT | 24-25 APRIL 2024 LISBON, PORTUGAL Scaling Innovation Through Collaboration

Project Caliptra Update

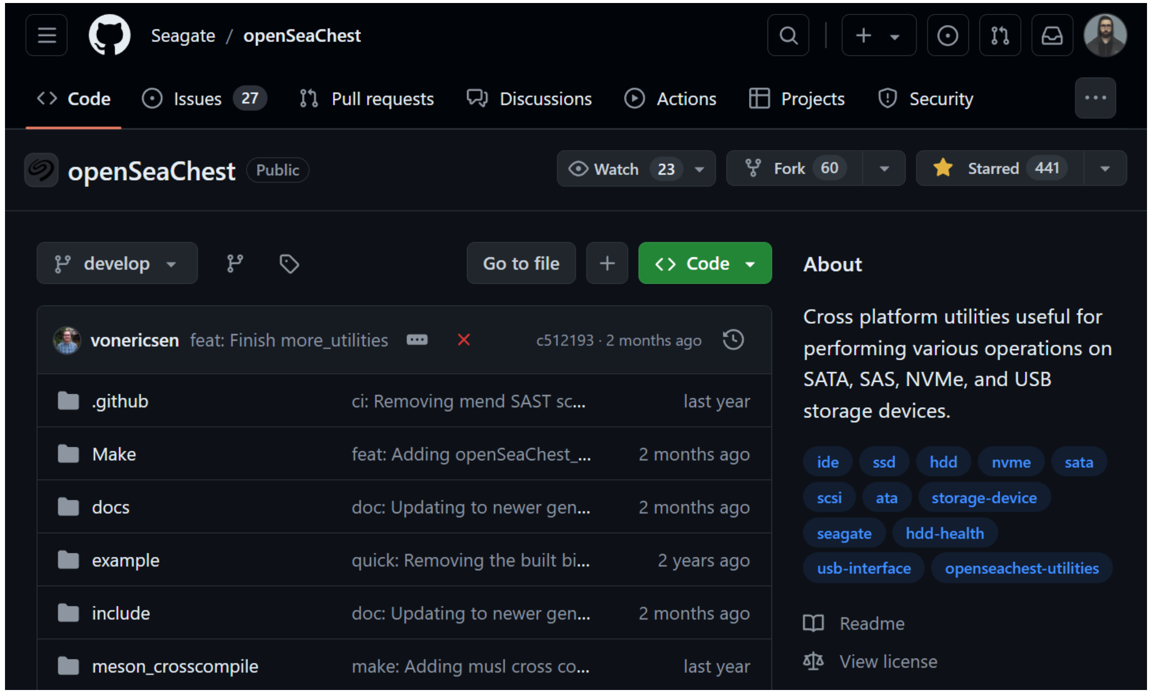
# CDI Health Grading Tool

- H=F KGM;=KGOO9J=KML=>GJ 11" 9F< &" " @=9D@9F< J=DA:AQ

- Transparency required to build trust in secondhand market
- CDI workgroup deep understanding of SSD and HDD quality and reliability
- Grading system designed to accurately assess the health and remaining use left
- Includes endurance, power on hours, errors, device self-test, signed vendor firmware



| # | DUT | STATE | TYPE | TRAN | VENDOR | MODEL NUMBER | SERIAL NUMBER | F/W | GB | B/S | PoH | SMART | HEALTH | REMARKS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | /dev/sda | Ready | SSD | ATA | SPCC | SOLID STATE DISK | BA1B0795065300893008 | SBFM61.3 | 1024 GB | 512 | 34571 | OK | 0% | |
| 2 | /dev/sdb | Ready | HDD | ATA | WDC | WD40EFRX-68WT0N0 | WD-WCC4E2066620 | 80.00A80 | 4000 GB | 512 | 66042 | OK | 0% | |
| 3 | /dev/sdc | Ready | HDD | ATA | WDC | WD40EFRX-68N32N0 | WD-WCC7K1XF1JDJ | 82.00A82 | 4000 GB | 512 | 39067 | OK | 0% | |
| 4 | /dev/sdd | Ready | HDD | ATA | WDC | WD2000F9YZ-09N20L1 | WD-WCC1P759C355 | 01.01A02 | 2000 GB | 512 | 64368 | OK | 0% | |
| 5 | /dev/sde | Ready | HDD | ATA | WDC | WD2000F9YZ-09N20L1 | WD-WMC5C0D4AD25 | 01.01A02 | 2000 GB | 512 | 56987 | OK | 0% | |
| 6 | /dev/sdf | Ready | HDD | SCSI | Not Reported | NOT REPORTED | 001449EJG68X PCJJG68X | Not Reported | 4000 GB | 512 | 15634 | OK | 97% | 8 Reallocated Sectors<br>3 Offline Uncorrectable Errors |
| 7 | /dev/sdg | Fail | HDD | SCSI | Not Reported | NOT REPORTED | 001449EL36VX PCJL36VX | Not Reported | 4000 GB | 512 | 15763 | OK | 70% | 156936 Reallocated Sectors<br>72 Offline Uncorrectable Errors |
| 8 | /dev/sdh | Ready | HDD | SCSI | Not Reported | NOT REPORTED | Z1Z6KYH70000W515S834 | Not Reported | 4000 GB | 512 | 70725 | OK | 100% | |
| 9 | /dev/sdi | Fail | HDD | ATA | WDC | WD2000F9YZ-09N20L1 | WD-WMC5C0D543Z0 | 01.01A02 | 2000 GB | 512 | 56457 | OK | 0% | 2170 Unstable Sectors |
| 10 | /dev/sdj | Ready | HDD | ATA | SEAGATE | ST2000VX000-1CU164 | S1E2P9JH | CV22 | 2000 GB | 512 | 70607 | OK | 0% | |
| 11 | /dev/sdk | Ready | HDD | ATA | SEAGATE | ST2000DM006-2DM164 | Z505H23F | CC26 | 2000 GB | 512 | 39470 | OK | 0% | |



vonericsen feat: Finish more_utilities c512193 · 2 months ago

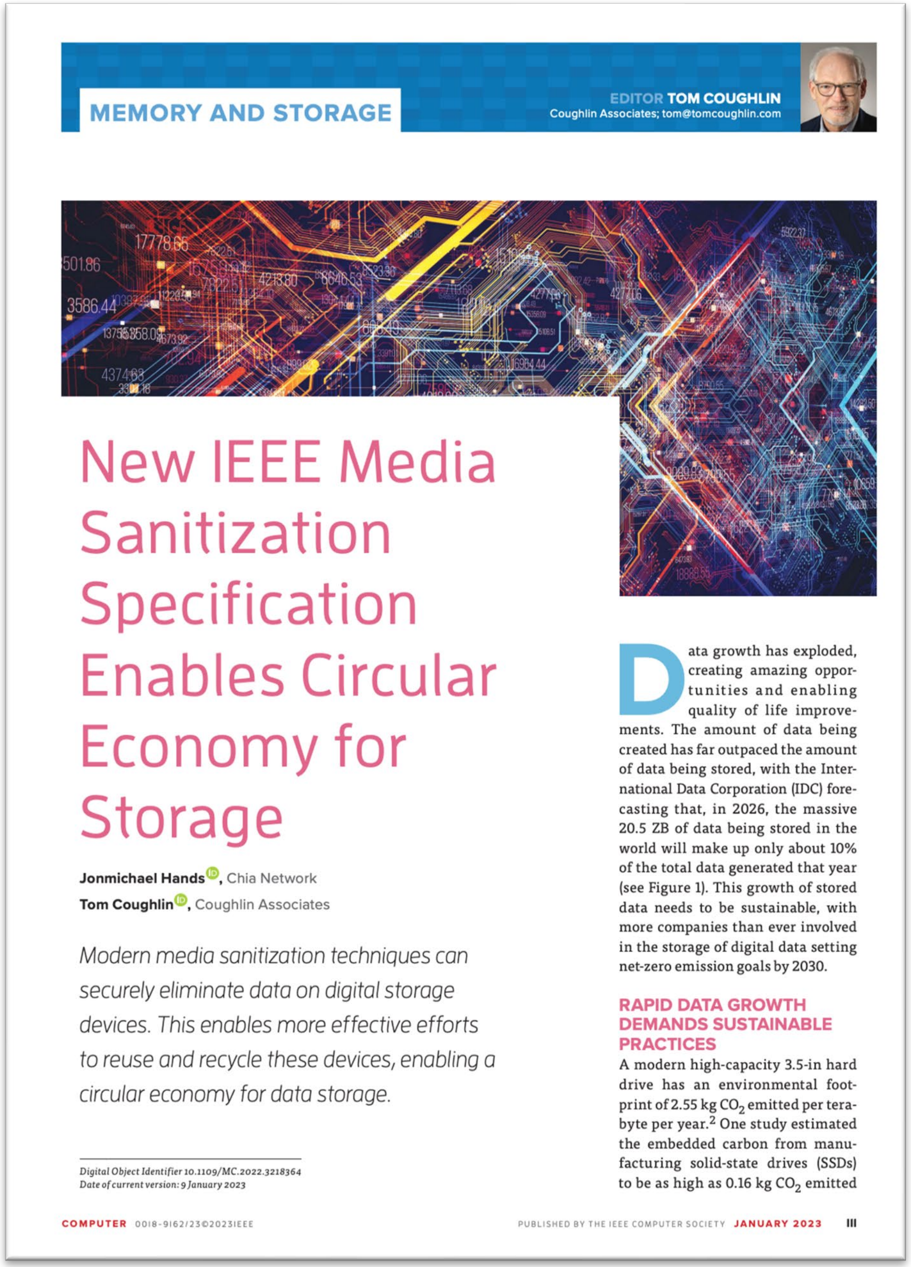
| | | |
|---|---|---|
| .github | ci: Removing mend SAST sc... | last year |
| Make | feat: Adding openSeaChest_... | 2 months ago |
| docs | doc: Updating to newer gen... | 2 months ago |
| example | quick: Removing the built bi... | 2 years ago |
| include | doc: Updating to newer gen... | 2 months ago |
| meson_crosscompile | make: Adding musl cross co... | last year |

Cross platform utilities useful for performing various operations on SATA, SAS, NVMe, and USB storage devices.

# Data Sanitization Research

! GE HML=+9?9RAF=9JLA;D=

- Storage market, intro to circular economy
- History of media sanitization specs
  - Show that DoD and NIST are old
- Highlight new IEEE 2883-2022 spec
- Review purge techniques



MEMORY AND STORAGE

EDITOR TOM COUGHLIN
Coughlin Associates; tom@tomcoughlin.com

## New IEEE Media Sanitization Specification Enables Circular Economy for Storage

Jonmichael Hands, Chia Network
Tom Coughlin, Coughlin Associates

*Modern media sanitization techniques can securely eliminate data on digital storage devices. This enables more effective efforts to reuse and recycle these devices, enabling a circular economy for data storage.*

Data growth has exploded, creating amazing opportunities and enabling quality of life improvements. The amount of data being created has far outpaced the amount of data being stored, with the International Data Corporation (IDC) forecasting that, in 2026, the massive 20.5 ZB of data being stored in the world will make up only about 10% of the total data generated that year (see Figure 1). This growth of stored data needs to be sustainable, with more companies than ever involved in the storage of digital data setting net-zero emission goals by 2030.

### RAPID DATA GROWTH DEMANDS SUSTAINABLE PRACTICES

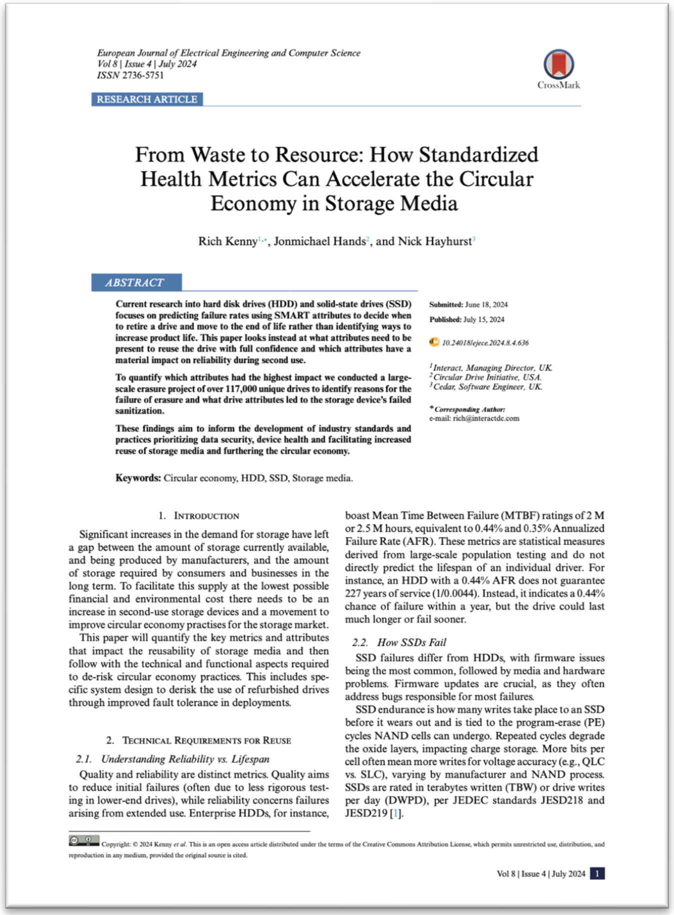
A modern high-capacity 3.5-in hard drive has an environmental footprint of 2.55 kg $CO_2$ emitted per terabyte per year.[2] One study estimated the embedded carbon from manufacturing solid-state drives (SSDs) to be as high as 0.16 kg $CO_2$ emitted

Digital Object Identifier 10.1109/MC.2022.3218364
Date of current version: 9 January 2023

# CDI Health Grading – Academic Paper

## From Waste to Resource: How Standardized Health Metrics Can Accelerate the Circular Economy in Storage Media

- Background on how HDDs and SSDs fail
- Designing systems for high durability with used drives
- Importance of media sanitization
- Results from Interact – 117k drives decommissioned and sanitized
- 87% suitable for reuse



*European Journal of Electrical Engineering and Computer Science*
*Vol 8 | Issue 4 | July 2024*
*ISSN* 2736-5751

RESEARCH ARTICLE

### From Waste to Resource: How Standardized Health Metrics Can Accelerate the Circular Economy in Storage Media

Rich Kenny[1,*], Jonmichael Hands[2], and Nick Hayhurst[3]

*ABSTRACT*

**Current research into hard disk drives (HDD) and solid-state drives (SSD) focuses on predicting failure rates using SMART attributes to decide when to retire a drive and move to the end of life rather than identifying ways to increase product life. This paper looks instead at what attributes need to be present to reuse the drive with full confidence and which attributes have a material impact on reliability during second use.**

**To quantify which attributes had the highest impact we conducted a large-scale erasure project of over 117,000 unique drives to identify reasons for the failure of erasure and what drive attributes led to the storage device's failed sanitization.**

**These findings aim to inform the development of industry standards and practices prioritizing data security, device health and facilitating increased reuse of storage media and furthering the circular economy.**

**Keywords:** Circular economy, HDD, SSD, Storage media.

**Submitted:** June 18, 2024

**Published:** July 15, 2024

*10.24018lejece.2024.8.4.636*

[1] *Interact, Managing Director, UK.*
[2] *Circular Drive Initiative, USA.*
[3] *Cedar, Software Engineer, UK.*

[*] ***Corresponding Author:***
e-mail: rich@interactdc.com

#### 1. Introduction

Significant increases in the demand for storage have left a gap between the amount of storage currently available, and being produced by manufacturers, and the amount of storage required by consumers and businesses in the long term. To facilitate this supply at the lowest possible financial and environmental cost there needs to be an increase in second-use storage devices and a movement to improve circular economy practises for the storage market.

This paper will quantify the key metrics and attributes that impact the reusability of storage media and then follow with the technical and functional aspects required to de-risk circular economy practices. This includes specific system design to derisk the use of refurbished drives through improved fault tolerance in deployments.

#### 2. Technical Requirements for Reuse

##### *2.1. Understanding Reliability vs. Lifespan*

Quality and reliability are distinct metrics. Quality aims to reduce initial failures (often due to less rigorous testing in lower-end drives), while reliability concerns failures arising from extended use. Enterprise HDDs, for instance, boast Mean Time Between Failure (MTBF) ratings of 2 M or 2.5 M hours, equivalent to 0.44% and 0.35% Annualized Failure Rate (AFR). These metrics are statistical measures derived from large-scale population testing and do not directly predict the lifespan of an individual driver. For instance, an HDD with a 0.44% AFR does not guarantee 227 years of service (1/0.0044). Instead, it indicates a 0.44% chance of failure within a year, but the drive could last much longer or fail sooner.

##### *2.2. How SSDs Fail*

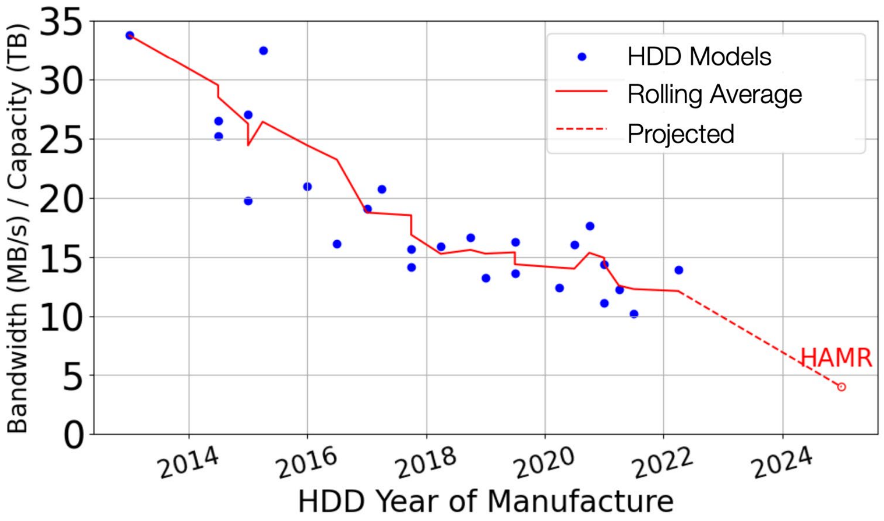
SSD failures differ from HDDs, with firmware issues being the most common, followed by media and hardware problems. Firmware updates are crucial, as they often address bugs responsible for most failures.

SSD endurance is how many writes take place to an SSD before it wears out and is tied to the program-erase (PE) cycles NAND cells can undergo. Repeated cycles degrade the oxide layers, impacting charge storage. More bits per cell often mean more writes for voltage accuracy (e.g., QLC vs. SLC), varying by manufacturer and NAND process. SSDs are rated in terabytes written (TBW) or drive writes per day (DWPD), per JEDEC standards JESD218 and JESD219 [1].

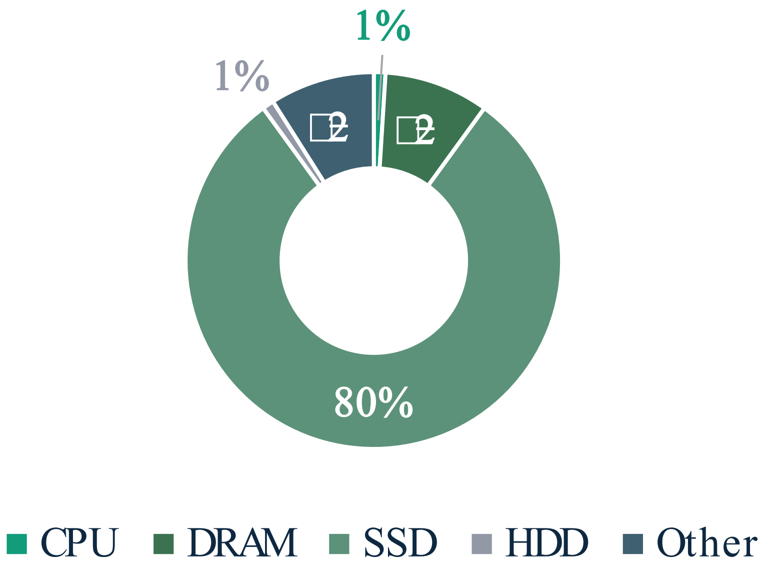
# A Call for Research on Storage Emissions

Carnegie Mellon University, Microsoft Azure

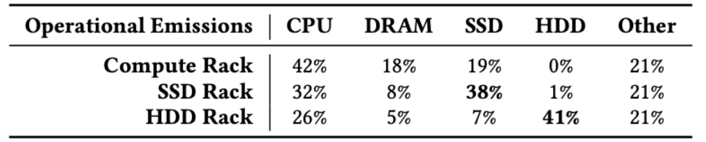
- Storage accounts for **33%** of operational and **61%** of embodied emissions in Azure DCs
- LCAs leveraging IMEC and Makersite (its likely much worse)
- Suggest extension of use and second life as ways to reduce impact



Increase of areal density on HDD helps but performance challenges

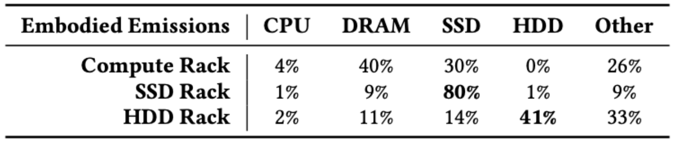


SSD Rack



| Operational Emissions | CPU | DRAM | SSD | HDD | Other |
|---|---|---|---|---|---|
| **Compute Rack** | 42% | 18% | 19% | 0% | 21% |
| **SSD Rack** | 32% | 8% | **38%** | 1% | 21% |
| **HDD Rack** | 26% | 5% | 7% | **41%** | 21% |

*Table 2: Operational emission breakdown for Azure rack types.*



| Embodied Emissions | CPU | DRAM | SSD | HDD | Other |
|---|---|---|---|---|---|
| **Compute Rack** | 4% | 40% | 30% | 0% | 26% |
| **SSD Rack** | 1% | 9% | **80%** | 1% | 9% |
| **HDD Rack** | 2% | 11% | 14% | **41%** | 33% |

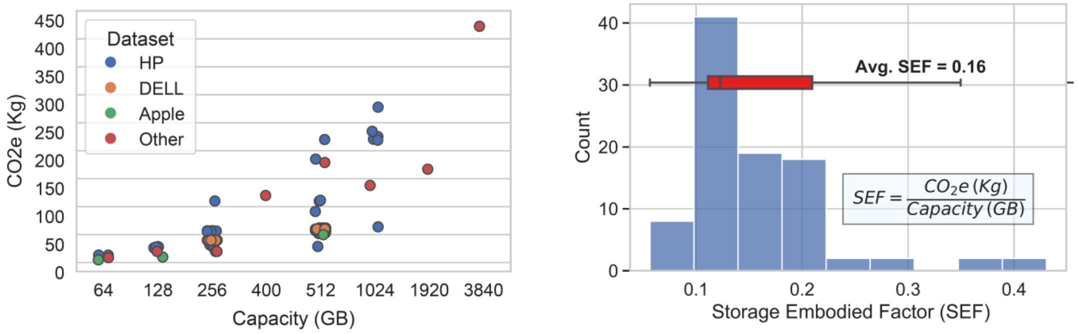
*Table 3: Embodied emission breakdown for Azure racks.*

Source: Hotcarbon

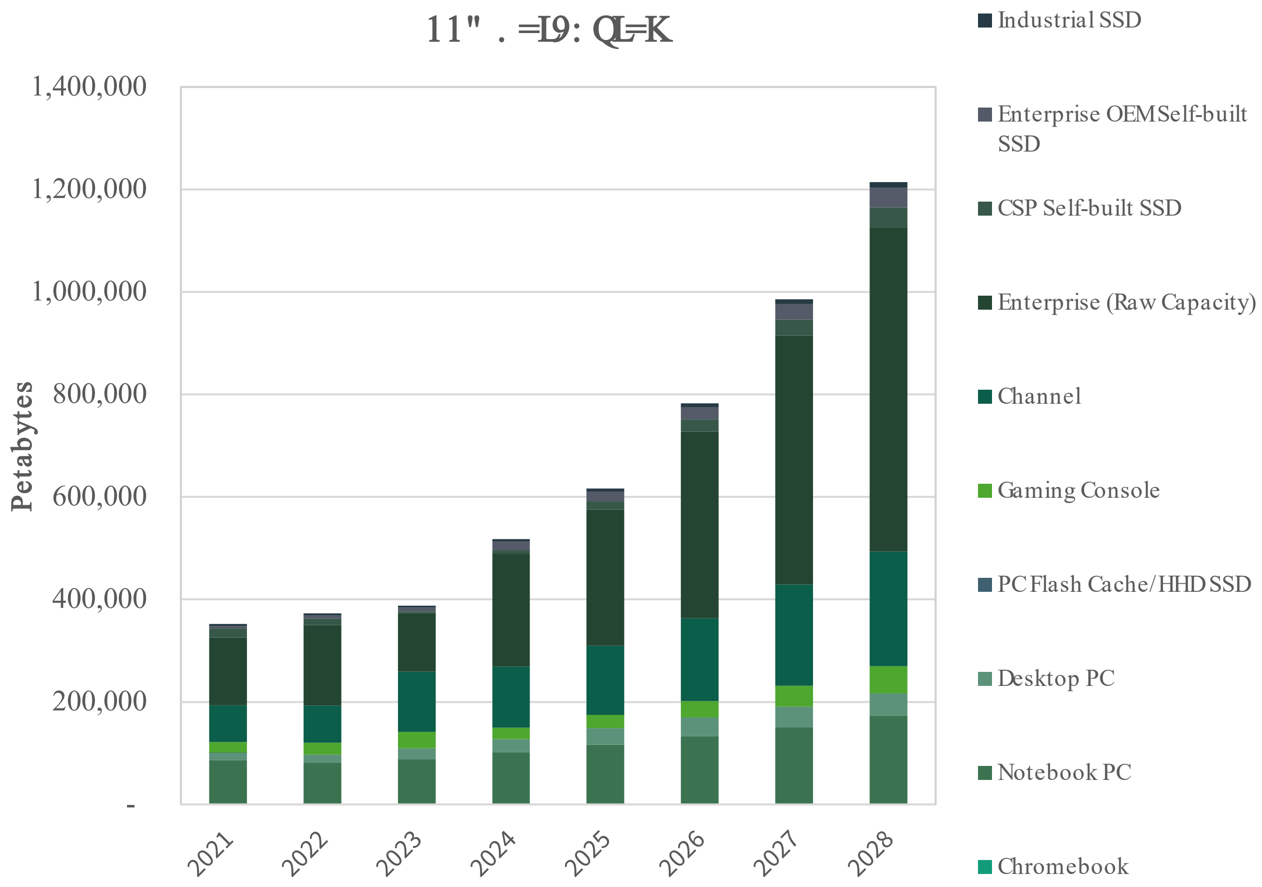
# Carbon Accounting

## The problem

- SSD carbon scales with capacity
- Apple 2023 sustainability report – carbon from iPhone flash only is **59.88g/GB**
- at 517EB in 2024, rough math is **31MMT C02e**



29FFM1 9F<, 9A. ( . □□□□ 2@=<AILQK=; J=LG>KK<KV#E: G<A=<
; 9J: GF 9J6AMGJ? N9A9: D=9L @LHK. 9JPANGJ? 9: K□□□□ □□□□□



Source: Forward Insights SSD Insights Q2'24

# Backup

# IEEE 2883-2022

Circular Drive Initiative

## Standard for Sanitizing Storage

- DAR?F AF<MKLJQGF L=JE AFGDG?Q9F< E G<=JF E =L@G<K9F< L=; @FAIM=K>GJ E =<A9 K9FALAR9LAGF
- 5 @9LAK K9FALAR9LAGF HJG; =KKGJ E =L@G< LG J=F<=J 9; ; =KKLGL9J?=L<9L9 GF KLGJ9?= E =<A9 AF>=9KA:D= >GJ 9 ?AN=F D=N=DG>=MGJL
- " =>AF=K1 9FALAR9LAGF + =L@G<K9F< 2=; @FAIM=K >GJ KH=; AAA E =<A9 LQH= &" " 11" GHLA9D J=E GN9: D= =L; .
- 1H=; AA=KAFL=J>9; = KH=; AAA L=; @FAIM=K 1 2 1 1 , 4+= @A@DQ>G; MK=< GF MKAF? L@= K9FALAR= ; GE E 9F<
- 29J?=L9DDG? A9D9F< H@QKA9DDG; 9LAGFK>GJ <9L9 AF; DM<AF? MK=J <9L9 GD< <9L9 E =L9<9L9 GN=JHJGNAKAGFAF? " =>AF=K@GKLE =L@G<K>GJ N=JAA9LAGF G>K9FALAR9LAGF

IEEE SA
STANDARDS ASSOCIATION

IEEE Standard for Sanitizing Storage

STANDARDS

IEEE Computer Society

Developed by the
Cybersecurity and Privacy Standards Committee

IEEE Std 2883™-2022

IEEE

# Media Sanitization Methods

Circular Drive Initiative

## Clear

*G?A;9DL=; @FAMK9J=
9HHDA=< LG9DD9<<J=KK9: D=
KLGJ9?= DG; 9LAGFK
HJGL=; LAF? 9?9AFKL KAE HD=
FGF AFN9KAN= <9L9
J=; GN=JQL=; @FAMK

## " =KLJM;L

Makes data recovery nearly impossible but results in the storage media becoming unusable.

Disintegrate, Incinerate, and Melt

## Purge

Logical or physical techniques rendering data recovery infeasible even with state-of-the-art laboratory techniques.

The goal of purge is to maintain the storage media and device in **reusable** state.

# Purge Media Sanitization Techniques

Circular Drive Initiative

## - N=JOJAL=

Using interface specific sanitize command, overwrite all LBAs with a fixed pattern, minimum of one pass. Multiple pass optional, but is not required anymore.

## Block Erase

Use NAND erase blocks, can sanitize a modern SSD in a few seconds to a few minutes.

Doesn’t waste NAND endurance, but verification requires no-deallocate.

## Crypto Erase

Requires that the devices supports encryption. Sanitize by deleting the media encryption key (MEK), leaving all the data scrambled.

Very fast, completes in seconds.

# Verification

Why Verify?

- Prove compliance with policies
- Assure data breach prevention
- Build trust with stakeholders

Verification Methods (IEEE 2883):

- Clear: Representative sampling (at least 5% of addressable space)
- Purge: Full verification (entire addressable space) recommended
- Destruct: Physical inspection ONLY

" G; ME =FL9LAGF

- 0=; GJ< C==HAF? AK; JM; A9DO@G O@=F O@9L
- ⅓ =JLAA;9L= G>19FALAR9LAGF⅓ '1-. '#! □□□□□

! GE HD=PALA=K

- , =O=J L=; @FGDG? A=KE 9Q@9N= HGKL K9FALAR= J=9< =JJGJK
- ! JQHLG=J9K= D9N=K; AH@=JL=PL FGL HD9AFL=PL
- , GF 9<<J=KK9: D= KH9; = FGL N=JA>9: D= L@JGM? @@GKLAFL=J>9; =

MAD<AF? 2JMKL

- $AIE O9J= 9M<ALK: QE 9FM>9; LMJ=JK
- 4=JAA;9LAGF G>K9FALAR= ; GE E 9F< =P=; MLAGF
- $MDDN=JAA;9LAGF O@=J= >=9KA:D=

# IEEE 2883.1

## Recommended Practice for Use of Storage Sanitization Methods

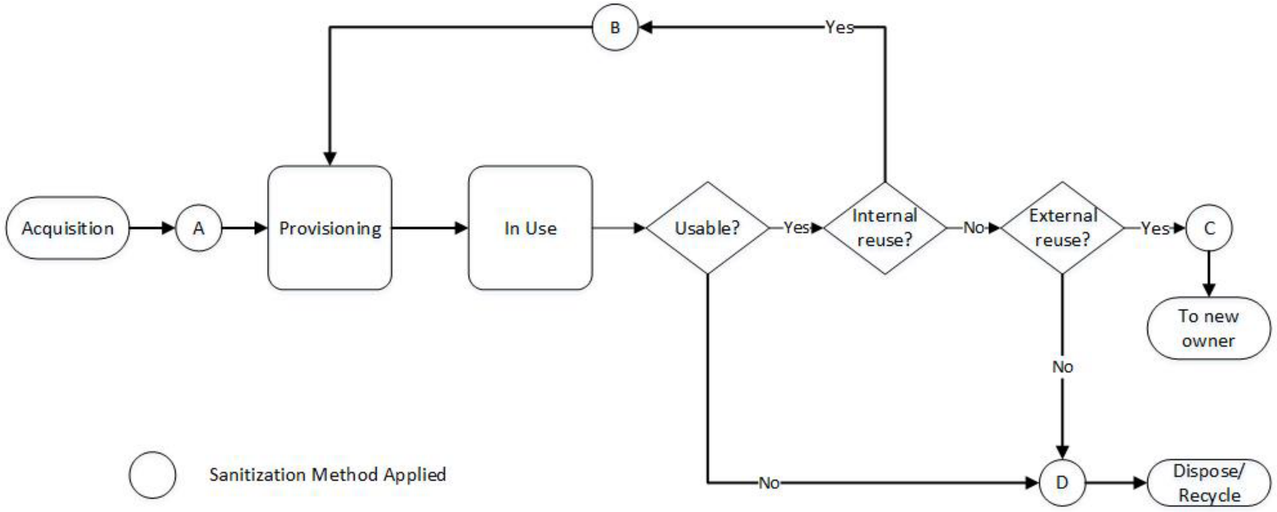
Circular Drive Initiative

- Storage Lifecycle, Risk and Management, Cryptography
- Choosing the Appropriate Sanitization Method: (clear, purge, or destruct) based on the intended use of the storage media, considering factors like risk and the sensitivity of the information
- Verification of Sanitization: Knowing that the data is gone

# Storage Lifecycle

## Sanitization in the storage lifecycle

- ; I MAKAAGF
- . JGNAKAGF AF?
- ; LAN= 3 K=
- #F< G>! MJJ=FL3 K=
- 0=HJGNAKAGF AF? >GJ J=MK=
- " AK; 9J< 0=; Q D=



# #P9E HD=G>*AC=DA@GG< G>" 9L9 0=; GN=JQ 9O=J 19FALAR9LAGF

| Sanitization Method | Adversary Capability | | |
|---|---|---|---|
| | Novice | Expert | Virtuoso |
| None | Almost Certain | Almost Certain | Almost Certain |
| Clear | Unlikely | Likely | Almost Certain |
| Purge | Almost Impossible | Almost Impossible | Unlikely |
| Destruct | Almost Impossible | Almost Impossible | Almost Impossible |

# Risk and Risk Management

- Classify data based on data sensitivity: low, medium, and high
- Interest=f( Gain, WorkFactor, LikelihoodOfSuccess )
- Managing risk: Accept, Avoid, Transfer, Treat/Mitigate

**Table 4—Risk as a function of likelihood and magnitude of loss**

| Likelihood of Retrieving Meaningful Data | Magnitude of Loss | | |
|---|---|---|---|
| | Low | Medium | High |
| Almost certain | Medium | High | Very High |
| Likely | Low | Medium | High |
| Unlikely | Very Low | Low | Low |
| Almost impossible | Very Low | Very Low | Very Low |

# Cryptography in Storage

## Encryption for Data Protection

- Symmetric Encryption: Same key for encrypting and decrypting (e.g. AES-XTS). Used for bulk storage due to efficiency.
- Two Key Types:
  - Media Encryption Key (MEK): The key that directly encrypts your data.
  - Key Encryption Key (KEK): Protects the MEK, allows for secure key changes.

# Cryptographic Erase: The Sanitization Power Tool

## Cryptographic Erase: Not Just Deletion

- **Principle**: Destroying the encryption keys makes the data practically unrecoverable.
- **Advantages**: Extremely fast, strong sanitization assurance (under certain conditions).
- **Conditions** for Use:
  - All data is encrypted.
  - Strong algorithm (at least 128-bit, 256-bit for high security).
  - High entropy keys (hard to guess).
  - All copies of the keys are destroyed.

# The Future of Encryption: Quantum Considerations

## Cryptographic Algorithm Lifetime

- Algorithm Lifetime: Cryptographic methods have a lifespan due to math advancements and computing power.
- Quantum Threat: Quantum computing may break current algorithms in the future.
- Relevance for Sanitization: Long-lived data might be vulnerable if an attacker stores ciphertext until a better attack is possible.
- Recommendation: Consider this for high-value, long-term data, but it's less of a concern for most everyday use cases.

# Choosing the Right Sanitization Method

## Mitigating Risk: The Sanitization Imperative

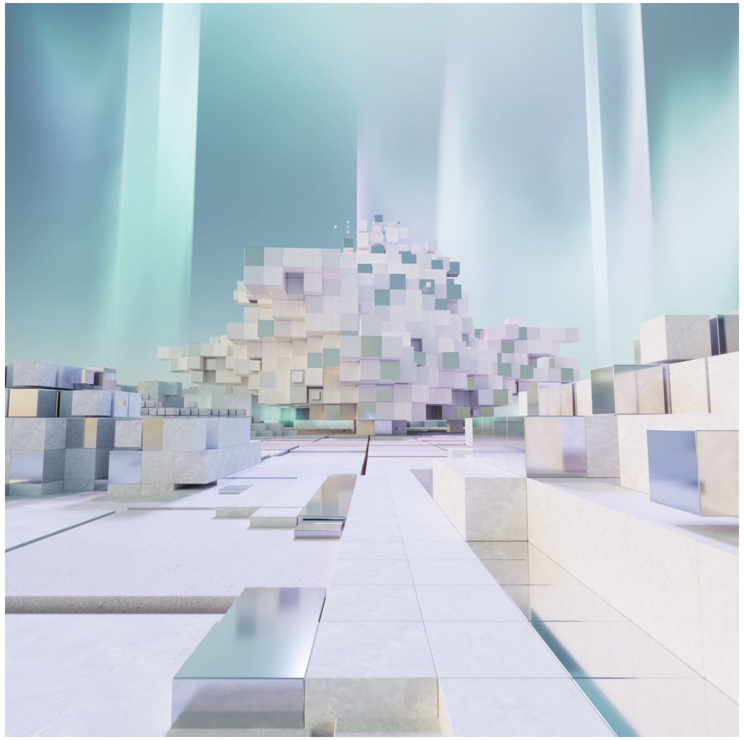
- **Goal**: Align data removal with your organization's risk tolerance.
- **Factors**: Consider economic and environmental impacts.

- **Clear**: Affects user-accessible data. Best for low risk data, internal reuse.
- **Purge**: Affects all data, including hidden areas. Best for almost all use cases.
- **Destruct**: Physically destroys the storage media. Best for storage that is obsolete, or no longer operable (broken)

# Sanitization Before Provisioning

## Supply Chain Threats: Don't Assume Trust

- **Threat**: Compromised supply chains, pre-installed malware, stolen encryption keys.
- **Risk**: Unauthorized access, data exfiltration.
- **Mitigation**: Sanitize storage BEFORE it enters your system. Generate new encryption keys.



# Sanitization Before Internal Reuse

## Internal Threats: Curiosity and Malice

- **Threat**: Curious employees, malicious insiders.
- **Risk**: Data breaches, unauthorized access to sensitive information.
- **Mitigation**: Match sanitization level to data sensitivity. Clear for low risk, Purge for high risk.

# Sanitization Before External Reuse

## External Threats: A Wider Landscape

- **Threat**: A broad range of actors with varying motivations and capabilities.
- **Risk**: Data breaches, competitive disadvantage, potential for deep forensic analysis.
- **Mitigation**: Purge is generally recommended due to increased exposure. Clear may suffice for low-risk data.

Circular Drive Initiative