

SEM
Classified and High Security Data Destruction

Est. 1959
GARNER PRODUCTS

You've Heard of DATA PRIVACY & REGULATIONS . . . So Let's Meet Them

Presented by:
Michael Harstrick
Garner Products
MHarstrick@Garner-Products.com
www.garnerproducts.com

As data protection laws tighten, the consequences of a large data breach increase, including **millions in fines and restitution**, as well as **damage to a company's reputation**. Data destruction takes center stage in these privacy regulations when media reaches end of life.

01 Overview of data privacy regulations impacting US and European companies

02 Data destruction/media sanitization standards for high security information

03 Importance of chain-of-custody for companies and ITADS

SEM
Classified and High Security Data Destruction

GARNER PRODUCTS Est. 1959

HIPAA

U.S. DEPARTMENT OF HOMELAND SECURITY

FACTA
Fair and Accurate Credit Transactions Act

GLBA FISMA SOX

GDPR

01 Data privacy regulations impacting US and European companies

Data privacy regulations impacting US and European companies

BEST KNOWN:

HIPAA/HITECH: Enforced by DHS, OSC and individual state Attorneys General

GLBA: Enforced by FTS, US Treasury Dept., Fed, SEC NCUA and FDIC

FACTA: Enforced by DOJ

GDPR: Enforced by ICO in each EU country

Strategic Intent

PROTECT CUSTOMERS' PRIVACY

SEM
Classified and High Security Data Destruction

GARNER PRODUCTS Est. 1959

NIST

ISO®

IEEE
Advancing Technology for Humanity

02 Data destruction/media sanitization standards for high security information

Data destruction/media sanitization standards for high security information

US & EU STANDARDS/FRAMEWORKS

US Standards/Frameworks

- NSA/CSS
- NIST 800-88 rev. 2
- IEEE 2883-2023
- IRS 1075

EU Standards/Frameworks

- ISO 21964
- IEEE 2883-2023

Data destruction/media sanitization standards for high security information

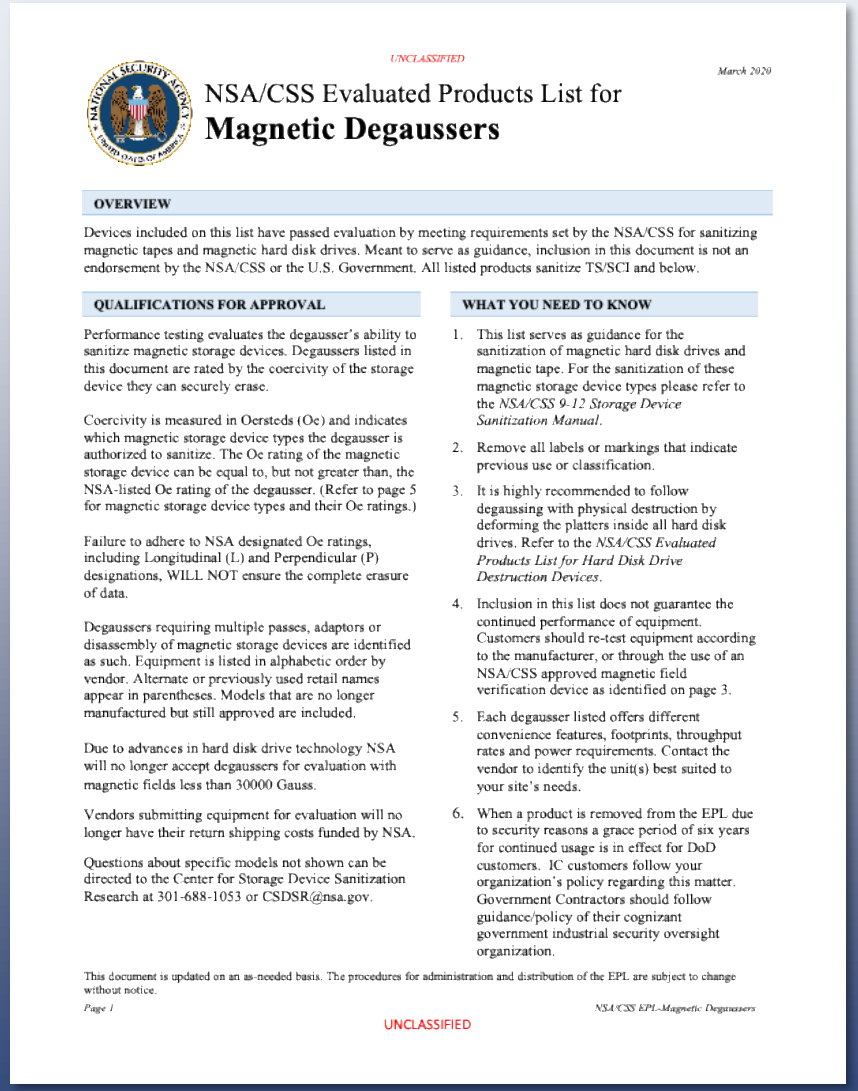
SEM Classified and High Security Data Destruction

GARNER PRODUCTS Est. 1959

NSA/CSS

Highest protection standard in the world

- Governments around the world use as their standard for TOP SECRET data destruction
- NSA Evaluated Products List – Data decommissioning solutions approved by the NSA for classified information
- For TOP SECRET Data the NSA requires:
  - ✓ Shred (2mm particles)
  - ✓ Incinerate
  - ✓ Degauss with NSA-Listed Degausser
  - ✓ **INSIDE the Secure Area**



UNCLASSIFIED

March 2020

NSA/CSS Evaluated Products List for
Magnetic Degaussers

OVERVIEW

Devices included on this list have passed evaluation by meeting requirements set by the NSA/CSS for sanitizing magnetic tapes and magnetic hard disk drives. Meant to serve as guidance, inclusion in this document is not an endorsement by the NSA/CSS or the U.S. Government. All listed products sanitize TS/SCI and below.

QUALIFICATIONS FOR APPROVAL

Performance testing evaluates the degausser's ability to sanitize magnetic storage devices. Degaussers listed in this document are rated by the coercivity of the storage device they can securely erase.

Coercivity is measured in Oersteds (Oe) and indicates which magnetic storage device types the degausser is authorized to sanitize. The Oe rating of the magnetic storage device can be equal to, but not greater than, the NSA-listed Oe rating of the degausser. (Refer to page 5 for magnetic storage device types and their Oe ratings.)

Failure to adhere to NSA designated Oe ratings, including Longitudinal (L) and Perpendicular (P) designations, WILL NOT ensure the complete erasure of data.

Degaussers requiring multiple passes, adaptors or disassembly of magnetic storage devices are identified as such. Equipment is listed in alphabetic order by vendor. Alternate or previously used retail names appear in parentheses. Models that are no longer manufactured but still approved are included.

Due to advances in hard disk drive technology NSA will no longer accept degaussers for evaluation with magnetic fields less than 30000 Gauss.

Vendors submitting equipment for evaluation will no longer have their return shipping costs funded by NSA.

Questions about specific models not shown can be directed to the Center for Storage Device Sanitization Research at 301-688-1053 or CSDSR@nsa.gov.

WHAT YOU NEED TO KNOW

1. This list serves as guidance for the sanitization of magnetic hard disk drives and magnetic tape. For the sanitization of these magnetic storage device types please refer to the *NSA/CSS 9-12 Storage Device Sanitization Manual*.
2. Remove all labels or markings that indicate previous use or classification.
3. It is highly recommended to follow degaussing with physical destruction by deforming the platters inside all hard disk drives. Refer to the *NSA/CSS Evaluated Products List for Hard Disk Drive Destruction Devices*.
4. Inclusion in this list does not guarantee the continued performance of equipment. Customers should re-test equipment according to the manufacturer, or through the use of an NSA/CSS approved magnetic field verification device as identified on page 3.
5. Each degausser listed offers different convenience features, footprints, throughput rates and power requirements. Contact the vendor to identify the unit(s) best suited to your site's needs.
6. When a product is removed from the EPL due to security reasons a grace period of six years for continued usage is in effect for DoD customers. IC customers follow your organization's policy regarding this matter. Government Contractors should follow guidance/policy of their cognizant government industrial security oversight organization.

This document is updated on an as-needed basis. The procedures for administration and distribution of the EPL are subject to change without notice.

Page 1 *NSA/CSS EPL-Magnetic Degaussers*

UNCLASSIFIED

Data destruction/media sanitization standards for high security information

SEM Classified and High Security Data Destruction

GARNER PRODUCTS Est. 1959

NIST 800-88 rev. 2

The most accepted framework for end-of-life media sanitization

CLEAR

Overwrite that replaces target data with non-sensitive data

Overwriting cannot be used for media that are damaged or not rewriteable, and may not address all areas of the device where sensitive data may be retained

PURGE

Purge uses overwrite, block erase, and cryptographic erase methodologies that makes data recovery for the most part infeasible. It provides a higher level of media sanitization than Clear.

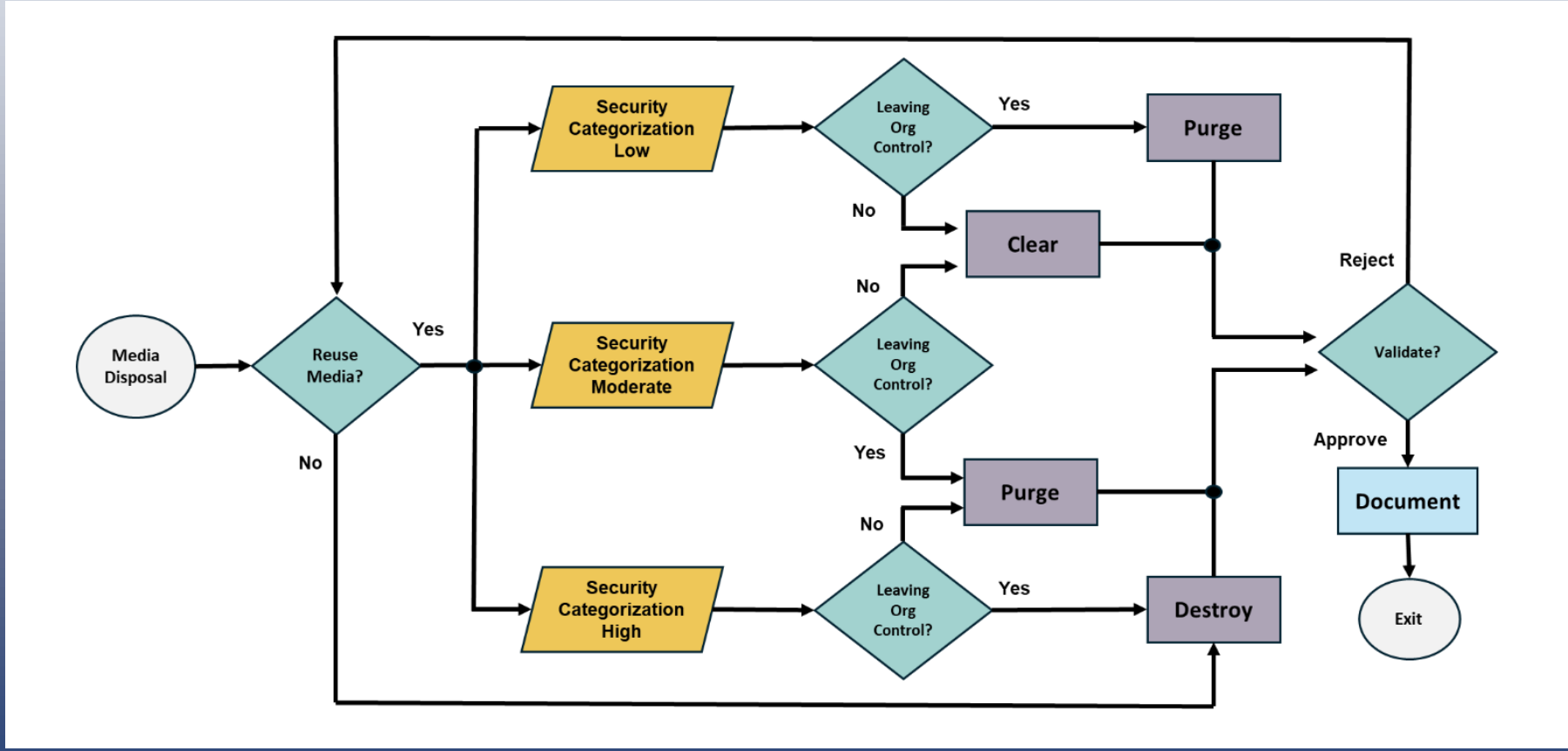
Degaussing is a type of purging.

DESTROY

While clearing and purging provide media sanitization involving less sensitive data, **destroying** is the most effective and permanent solution. Destruction includes electromagnetic degaussing, as well as physical destruction by crushing, shredding, or disintegrating.

Data destruction/media sanitization standards for high security information

NIST: Sanitization and Disposition Decision Flow



Data destruction/media sanitization standards for high security information

IEEE 2883-2023

IEEE 2883 also classifies data sanitization into three categories, which are similar to NIST's, on how to sanitize data by media type:

CLEAR

Data: Non-Sensitive

Technique: Logical – Overwrite, block erase

PURGE

Data: Sensitive

Technique: Logical & Physical – Overwrite, block erase, cryptographic erase, degauss

DESTRUCT

Data: Sensitive

Technique: Physical – Disintegrate, incinerate, melt

Data destruction/media sanitization standards for high security information

IRS 1075

- Protects **Federal Tax Information** — including tax returns and other information provided by the IRS
- Applies to all federal, state, and local government agencies that handle FTI
- Requires following NSA level data destruction regulations

Data destruction/media sanitization standards for high security information

ISO 21964

ISO 21964 replaces the older DIN 66399. It defines 3 protection classes, 6 material categories, and 7 security levels.



Levels 1-3

- Suitable for general documents or internal documents that don't require high security.
- Shred in strips



Level 4

- Recommended for confidential data, like personal information or financial records.
- Shred with cross cut



Levels 5-7

- Used for highly sensitive or top-secret data that requires the highest level of protection.
- Shred with cross cut shape 2mm2

Data destruction/media sanitization standards for high security information

SEM Classified and High Security Data Destruction

GARNER PRODUCTS Est. 1959

Other Regulations & Certifications

NAID AAA

- Policies and procedures but no data sanitization standards
- Requires scheduled and unannounced surprise audits by trained professionals to verify operational security.

E-Steward

- Policies and procedures but no data sanitization standards
- Prohibits exporting hazardous electronic waste from developed countries to developing nations.
- Requires strict data destruction protocols, including NAID AAA certification for residual data sanitization.

R2

- Policies and procedures but no data sanitization standards
- Strict protocols for sanitizing or destroying sensitive personal and corporate data on retired devices.
- Prioritizes testing, repair, and refurbishment to extend device lifecycles before recycling raw materials



SEM
Classified and High Security Data Destruction

Est. 1959
GARNER PRODUCTS

03 Importance of chain-of-custody for companies and ITADS

Importance of chain-of-custody for companies and ITADS

Chain of custody refers to the documented and unbroken trail of accountability that records the lifecycle of a sensitive asset; from creation and use to final destruction.

- Maintaining a secure chain of custody is essential for regulatory compliance and mitigating cybersecurity risk.
- Every handoff—internal or external—introduces opportunities for data loss, theft, or human error.
- Outsourced destruction services can compromise control, increase liability, and make audits harder to pass.
- In-house destruction with high-security equipment ensures traceability, accountability, and audit-ready documentation.



Importance of chain-of-custody for companies and ITADS

DATA CONTROLLER VS. DATA PROCESSOR



Data Controller- A person who determines the purposes for which and the manner in which any personal data are processed.



Data Processor- Any person (other than an employee of the data controller) who processes the data on behalf of the data.

Importance of chain-of-custody for companies and ITADS

ITAD CONSEQUENCES

You are a data processor.

You want your customer to contractually assure you that the media has been sanitized—before it comes to you.



Importance of chain-of-custody for companies and ITADS

If you are contracted to destroy media that has not been sanitized:

- You must have a sanitization technique that meets regulatory guidelines
- You must have a tracking system that captures every sanitization by serial number so you can prove compliance.





SEM
Classified and High Security Data Destruction

Est. 1959
GARNER PRODUCTS

THANK YOU!