Data Destruction Demystified:

Understanding D.O.D. Standards and Certifications

Data Destruction Demystified:
Understanding D.O.D. Standards and Certifications

I. Abstract

This document is designed to provide a basic understanding of data destruction and the importance of the industry's compliance with Department of Defense (D.O.D.) Standard 5220.22-M and The National Institute of Standards and Technology (NIST) publication 800-88.

II. Executive Summary

When an individual or company makes the decision to upgrade their computer network, the older equipment is often restructured to work in another area of the business, sold on the secondary PC market, donated to charity or otherwise destroyed. In any of these scenarios, it is of the utmost importance that the existing data residing on the hard drives of these computers be effectively erased (sanitized).

But, how can IT managers and/or CIOs be sure that their company's sensitive data is being properly destroyed?

The data destruction industry adheres to two specific sets of standards – D.O.D. 5220.22-M and NIST publication 800-88 – both of which state the minimum requirements for an effective data destruction policy.

III. D.O.D. 5220.22-M

The Department of Defense Standard 5220.22-M, Section 5, Subsection 8-5-3 states that to effectively overwrite the data on recordable media, each section of the disk must be overwritten three times, or what's known as three passes. On the first pass, the data in each sector is replaced with a character. On the second pass, the character is replaced with its complement. And, on the third and final pass, the sector is filled with a random character. In addition, items which have been cleared must remain at the original level of classification and in a secure, controlled environment. It is important to note that 5220.22-M DOES NOT recommend the three-pass system for the sanitization of "top-secret" information.

For disc sanitization to fall under the D.O.D. standards, the information on the disc must be removed through a two-step process in which the three-pass procedure is completed first, then followed by the removal of all classified labels, activity logs and markings.

IV. NIST Publication 800-88

NIST describes disc sanitization as "the removal of data from storage media so that, for all practical purposes, the data cannot be retrieved." Currently, there are three primary methods recognized as effective for disc sanitization – overwriting, degaussing and physical disc destruction.

- Overwriting – Overwriting consists of using software to write (1s, 0s, or a combination of both) onto the media where the file to be sanitized is located. The number of times this is performed is relative to the sensitivity of the information being sanitized.
- Degaussing – Two types of degaussing machines exist – electric and strong magnet. Degaussing machines are tested by the Department of Defense and those that meet their standards are placed on the Degausser Product List (DPL) of the National Security Agency's (NSA) Information Systems Security Products and Services Catalogue.
- Destruction – In NCSC-TG-025, the approved methods of disc destruction include:
    - Disc shredding (most common method of physical disc destruction)
    - Destruction at an approved metal destruction facility, i.e., pulverization, smelting or disintegration
    - Application of concentrated hydriodic acid
    - Application of acid activator Dubais Race A (8010 181 7171) and stripper Dubais Race B (8010 181 7170)
    - Application of an abrasive substance

V. FAQ

1. What Does It Mean to Be D.O.D. Certified?

Currently, there are no "certifications" based on D.O.D. guidelines. The guidelines are a set of standards that are recommended by the Department of Defense to ensure the proper sanitization of sensitive data from recordable media or the physical destruction of the disc. The D.O.D. does approve certain pieces of equipment like degaussers and disc shredders, which meet or exceed their requirements.

2. How Do I Know if the IT Asset Management Company I Choose Adheres to D.O.D. 5220.22-M?

To ensure that the company you choose for your disc sanitization/destruction needs follows the D.O.D. 5220.22-M guidelines, verify that they have or can provide:

- An errors and omissions insurance policy (minimum of USD 1 million)
- An auditable report of the disc sanitization and/or destruction including serial numbers and Asset ID/username
- Chain of Custody documentation

3. Are There Industry-Specific Regulations for Data Destruction Above and Beyond D.O.D. Standards?

Industries that utilize sensitive customer information normally have a set of regulations that need to be adhered to in terms of destroying that data. These regulations need to be adhered to in addition to the D.O.D. standards. Examples include:

- FACTA (Fair and Accurate Credit Transactions Act)
- GLB (Gramm-Leach Bliley) - banking and financial institutions
- HIPPA (Health Insurance Portability and Accountability Act) - the healthcare industry
- PCI DSS (PCI Data Security Standard)
- SOX (The Sarbanes-Oxley Act)
- CAL SB1386 (The California Information Practice Act)

4. How Do I Know if the Software Being Used to Overwrite the Data is Effective?

The D.O.D. acknowledges software overwriting as an approved method for data destruction, however, the software needs to be capable of overwriting all addressable locations on the media, including those featuring intermediate errors. If unusable sectors are incapable of being overwritten or if any errors occurred during the overwrite process, the disc should be degaussed and/or physically destroyed. If the overwriting completed successfully, each application should be examined individually for effectiveness.

5. Are There Differences Between D.O.D. 5220.22-M and NIST 800-88?

The primary difference between the two standards is recognized in how many passes are required to prevent data disclosure. D.O.D. 5220.22-M states very clearly that three passes must be conducted to sanitize the disc, whereas NIST 800-88 indicates that one pass is often effective enough to defy conventional forensic recovery on modern hard discs.

6. What are the Requirements for a Degausser to be Approved by the D.O.D.?

The Department of Defense tests degaussing equipment according to the standard set by the National Security Agency (NSA). For a degausser to be approved, it must be able to reduce the analog test signal by 90 decibels (db), or one billionth of its original strength (1 part in 109).

7. What are the Requirements for Disc Shredding Equipment to be Approved by the D.O.D.?

The D.O.D. approves Level 6 superfine shredders. Particle size should meet or exceed the NSA/CSS USA Government specification of 1.0 x 5.0 mm.

VI. Summary

In summary, effective data destruction needs to follow a specified set of guidelines to properly prevent secure or sensitive information from getting into the hands of unauthorized individuals. And, while many industry professionals may claim to be *certified* by the Department of Defense, it is extremely important that the end-user understand the protocol that is required for *compliance* with the guidelines presented by the D.O.D. While there is no-such current certification, a quality Asset Management company will be compliant with government mandates and requirements for the sanitization and/or physical destruction of recordable media.

Liquid Technology, Inc.
15 West 26th Street
9th Floor
New York, NY 10010

Main Telephone: (212) 679-2524
Fax : (212) 214-0424
buyer@liquidtechnology.net

Reach us Toll Free at: 800-797-LIQUID (797-5478)

Regional Offices:
Los Angeles, CA: (949) 753-5124
San Francisco, CA: (650) 249-6368
Hartford, CT: (860) 547-1767
Fort Lauderdale, FL (954) 376-5794
Chicago, IL: (312) 382-8208
Cambridge, MA: (617) 737-6100
Dallas, TX (214) 256-4298
McLean, VA: (703) 533-3100