



# Erasure Legislation (Part 1 of 2)

## Newer Security Standards for Hard Drive Security - NIST 800-99 vs. DoD 5220

Since 1995, the Information Technology and electronics recycling industries have embraced parts of a U.S. Department of Defense document created as part of the “National Industrial Security Program”. This document, entitled “DoD 5220.22.M”, defines a broad range of I.T. security requirements, methods, and procedures - ranging from facility security, chain of custody, storage and retention, and methods of data destruction.

In this 130+ page document, a mere two page “clearing and sanitization” matrix has directed the industry to either “clear” a hard drive by over-writing each addressable space with a single character or to “sanitize” a hard drive three times to essentially render the same level of data privacy. At the National Association for Information Destruction conference in 2005, however, Dr. Simpson Garfinkel, one of the world’s leading data security experts, opined that a single overwriting pass represented a pragmatic commercial solution for data destruction.

While DoD 5220.22.M addresses hard disks and other computer storage media, there are many other electronics devices that also contain sensitive data. These include cell phones, PDAs, data networking equipment, copiers, SCSI/ Fibre channel hard drives, DRAM, and smart Cards. With the advent of this new equipment, the need for a broader standard for data destruction has developed. In late 2006, with the support of the U.S. Department of Homeland Security, the National Institute of Standards and Technology (“NIST”) published a new document entitled “Guidelines for Media Sanitization: Document 800-88.” This new standard was developed in order to provide a more practical approach to ensuring data security on hard drives and other types of media.

The document is broken in to the following sections:

- **Background** – An overview of the different types of media and the different options for data destruction – see below
- **Roles and Responsibilities** – Describes the required personnel and their respective roles in the process
- **Information Sanitization and Disposition Decision Making** – A methodical discussion on how to determine the most appropriate method of handling data destruction
- **Sanitization Techniques / Recommendations** – A discussion of hard drive security as well as other types of

media. These include cell phones, PDA’s and other IT equipment.

NIST 800-88 describes four different methods of data destruction in order of increasing level of security:

- **Disposal** – the act of discarding with no regard to data privacy
- **Clearing** – Essentially overwriting data so that old data can not be recovered
- **Purging** – employing either degaussing (magnetic exposure to destroy data) or a relatively new self destruct command that is available in all modern day PC hard drives called “Secure Erase”
- **Destroying** – Physical mutilation of the hard drive so that it can be visually validated

NIST 800-88 brings to the forefront two advantages to organizations concerned with data destruction:

- Simplified discussion of how to handle data privacy at multiple levels and across multiple types of information technology assets
- An introduction to a more efficient means of performing data destruction called “Secure Erase”

In a recent interview, Darik Horn, the creator of the world famous DBAN/EBAN data wiping software, stated that he expects that NIST 800-88, “Will become the baseline at most organizations.”

In the June edition of ITAK, the next installment on this topic, LifeSpan will review Secure Erase and analyze the results of research conducted in collaboration with Temple University (Philadelphia, PA)

**Brooks Hoffman**  
*VP of Finance & Operations for  
LifeSpan Technology Recycling Inc.*