Technical Reference Document:
Moving Beyond the DoD 5220.22-M "Standard"

- The U.S. Department of Defense no longer references DoD 5220.22-M as a method for secure HDD erasure
- Regulations and certification programs now cite NIST SP 800-88 media erasure guidelines
- Why independent erasure verification has moved to the forefront of certified compliance oversight

DESTRUCTDATA, INC. 12 Rogers Rd. Unit 8 Haverhill, MA 01835 Toll Free: 800-781-4799 www.destructdata.com

Moving Beyond DoD 5220.22-M:

The Data Wipe "Standard" That Would Not Die

The DoD 5220.22-M standard for "erasing" or wiping data from a hard drive emerged early on in the evolving electronic data destruction business. A classic case of "echo chamber" knowledge distribution, the de facto adaption of this process was more of a marketing phenomenon than it was the result of any official policy supported by the Department of Defense.

DoD 5220.22-M specifies a process that overwrites data on a hard drive with random patterns of 1s and 0s. The fact that the DoD 5220.22-M protocol required 3 overwriting passes made it seem all the more secure, as did the implied Department of Defense imprimatur. At some point, this pseudo standard took on a life of its own as third-party computer recycling and refurbishing companies, IT asset disposal (ITAD) firms and other types of organizations asserted DoD compliance on websites and marketing collateral.

But DoD 5220-M was never "approved" by the Department of Defense for civilian media sanitization, and even more importantly, the DoD never intended for it to be a standard for classified data. The DoD is not in the business of certifying data destruction standards and has no mechanism for policing any given company's procedures. For its own classified data, DoD requires a combination of wiping, degaussing and/or physical destruction.

But that is old news. Over the past several years, the National Institute for Standards and Technology's (NIST) *Special Publication 800-88: Guidelines for Media Sanitization* has become the real world reference for data erasure compliance. Originally issued in 2006 and revised in 2012, SP 800-88 spells out preferred methodologies for wiping hard drives and other media under Minimum Sanitization Recommendations in Appendix A (see our summary, page 25). These methods include both over-writing and Secure Erase, a protocol built into the hard drive. This document has replaced the DoD "standard" in terms of regulatory and certification practice, and yet good old DoD 5220.22-M continues to hang on in marketing statements.

The intent of the NIST document is to provide meaningful guidelines for sanitizing electronic media. It does not provide requirements, standards or specifications. In actual practice, most commercial data wiping software and hardware products reliably deliver the technology to erase hard drives beyond the possibility of reasonable forensic recovery and to comply with mainstream certification programs. In terms of performance, the differentiators among such products are about price, processing speed, scale and auditing capabilities. But it would be surprising to see any modern data wipe product invoke DoD 5220.22-M because the multiple overwrite passes it specifies involve unnecessary energy use, time and cost.

Key Points:

- The U.S. Department of Defense no longer references DoD 5220.22-M as a method for secure HDD erasure
- Regulations and certification programs now cite NIST SP 800-88 media erasure guidelines
- Multiple overwrite passes can waste time and money
- "Approved by DoD" claims are misleading
- Independent erasure verification has moved to the forefront of certified compliance oversight

Moving Beyond DoD 5220.22-M

Continued from page 2

Virtually all certification organizations now cite NIST Special Publication 800-88 for guidelines in developing these programs and directly reference the Minimum Sanitization Recommendations. The *Safe Harbor Principle* paper provides more context for this topic.

Erasure Verification Moves To the Forefront

In terms of compliance, the implementation of data erasure technology is only one component of an overall data security program. Concurrent with the ascendancy of NIST's data wiping guidelines, the erasure verification component in SP 800-88 has been significantly expanded. Issued in 2012, Revision 1 of SP 800-88 adds several pages of new recommendations to section 4.7 (Verification Methods) and 4.8 (Documentation). Recognizing the importance of a comprehensive data security plan, the document places additional emphasis on the deployment of independent tools and personnel for erasure verification.

For more, please reference *Summary of Certified Erasure Verification Standards* and *Identifying & Correcting Failures in the Media Sanitization Process*.

The Department of Defense is not in the business of establishing or enforcing data erasure standards for commercial applications.

ABOUT DESTRUCTDATA, INC.
DestructData is the largest independent provider of End of Life data destruction/security solutions. Our specialty is integrating the best data erasure solutions available with purpose built hardware to accommodate any volume and application. To compliment and certify the data erasure process, we provide independent QC tools that satisfy world wide certifications requirements and standards. If physically destroying the media is required, we provide all methods of physical destruction for any type of electronic media including smartphones and tablets. As a pioneer in the specialized field of end of life cycle data destruction, DestructData implements the nuts and bolts solutions that assure compliance with complex data disposal legislation.

Please feel free to submit comments or questions to:

DESTRUCTDATA, INC.
12 Rogers Rd. Unit 8
Haverhill, MA 01835
www.destructdata.com
Toll Free: 800-781-4799
seanoleary@destructdata.com

For inquiries on DestructData products, please e-mail info@destructdata.com

DESTRUCTDATA
MEDIA SANITIZATION SOLUTIONS