The Persistence of Memory

A data erasure standard that refuses to die

A data standard that refuses to die

Companies adopt standards in a broad range of areas to ensure consistent execution; to enhance efficiency and performance; and to manage risk. Whether you're earning ISO certification, responding to regulators, optimizing your business processes, or demonstrating quality to your customers, choosing and adhering to appropriate standards is a way to guide and measure success.

Standards in any given area tend to reflect the consensus on best practices for accomplishing a specific task. In the area of data sanitization, the most prevalent standard has long been based on a Department of Defense document: DoD 5220.22M.

After it was introduced, the DoD 5220.22M standard – and the 3-pass erase process it references – quickly became the default standard for drive erasure. With changes in hard drives over time, however, a 3-pass overwrite is no longer necessary to successfully erase modern hard drives.

The evolution of the hard drive

Technology has advanced significantly since PCs first starting showing up on desktops and server farms sprouted around the world. Hard drives have become smaller and able to store more data at significantly lower cost. Solid state drives (SSDs) are beginning to overtake the traditional mechanical hard disk drives (HDDs) in terms of reliability and capacity.

As memory capacity has gone up, so has the size and complexity of the programs we run on our devices. Businesses are constantly upgrading to new and more powerful equipment and retiring older assets from service as the need for speed, reliability, and portability grows. Regardless of your refresh cycle, very few businesses keep assets in service for longer than 6 years, and those that do usually retain only the few machines necessary to run legacy software programs.

Changes to hard drives have brought with them changes to data erasure. Why is this? Let's take a look.

If you're still referencing DoD 5220.22M and specifying a 3-pass standard for data sanitization it's time to align your corporate requirements with current thinking and standards.

Peter Gutmann and history of the multi-pass protocol

In 1996, a man named Peter Gutmann wrote a paper - "Secure Deletion of Data from Magnetic and Solid-State Memory" - in which he concluded it might be possible to recover information from storage media if the data thereon had been overwritten only one time.

Based on theoretical analysis, Gutmann concluded that intelligence agencies might use sophisticated recovery tools like magnetic force microscopes and image analysis to determine the previous value of an overwritten bit. In response to this possibility, Mr. Gutmann devised a 35-pass overwrite protocol to ensure that all data would be overwritten so many times that any prior values would be meaningless. The 35-pass scheme also meant you didn't need to know which magnetic media encoding scheme was in use for any particular drive…the large number of passes would take care of any variations.

While the likelihood of actual data recovery through advanced tools – and the perceived benefit of high- number overwrite passes – was criticized even at the time, it's also useful to note that the underlying assumptions around drive technology and media encoding were, by necessity, retrospective in nature. Gutmann considered only drives that existed in 1996, and he cast a wide net for drive technologies going as far back as1966.

To be fair, advances in storage technology took place at a much slower pace than today and the cycle of constant upgrades to newer and newer technologies was still to come as Gutmann considered clearing drives manufactured from the mid-1960s to the mid-1990s. And too, even a state-of-the-art drive from 1996 is not the same as a device in service today.

For example, it took eight 3.5-inch platters to store 1GB of data in 1991 and by 1997 a five-platter 3.5- inch drive would still hold only 16.8GB. (For an interesting overview of disk development over the years, see 50 Years of Hard Drives https://www.pcworld.com/article/127105/article.html.) Today you can easily purchase 3.5-inch hard drives that hold 6 Terabytes of data, with each Terabyte representing 1,000 Gigabytes!

What difference does increased density make? The idea of data recovery using magnetic force microscopes and image analysis on older drives with sectors that take up more physical space hinges on the idea that a poorly aligned write heads might not completely overwrite each bit. If a bit was only partially overwritten there might be a trace indication of the prior value, thus making it possible to determine that value. Obviously the larger the space holding the bit, the "easier" it would be to identify and analyze using a microscope. But even then, considering it takes 1 byte (8 bits) to represent a single letter, the chance of accurately figuring out the original value of each bit and byte then reconstructing entire words or other usable content was already unlikely to the point of irrelevance.

> The underlying assumptions around drive technology, media encoding, and the multi-pass erasure protocol were developed based on hard drives that existed before 1997.

After Gutmann

Even while drives evolved and the probability of accurately determining prior bit values remained statistically at or near zero, companies found they needed to have a standard they could follow that would assure clients

and regulators that they'd taken the necessary steps to erase their data. Clearly a 35-pass method was both unnecessary and too time consuming to be practical, so many U.S. companies looked to the Department of Defense for guidance. If they simply used the same standard as the DoD, then surely nobody would question the decision.

And indeed, the DoD referenced methods for data destruction in a document known as DoD 5220.22M. While the DoD never intended their recommendations to be applied to commercial businesses, companies embraced the standard because it was clear and came from an unimpeachable authority.

In parallel with corporations adopting the 3-pass standard, IT Asset Disposition (ITAD) providers began to advertise their ability to deliver a 3-pass process. So in spite of research showing a single pass would do the job, the 3-pass "standard" became a positive-feedback loop between beliefs and behavior: as more companies believed the 3-pass process to be the only safe option, ITAD companies increasingly promoted it as proof of process safety. Over time, repetition increased awareness and exposure made it true. This prompted some companies to take it even further: if a 3- pass wipe was good for an "ordinary" company then a 7-pass wipe must be even better.

But even with the self-reinforcing rise of the 3-pass "standard," not everybody bought into the general consensus. In 2008 the research firm "16 Systems" – which focused on computer forensics, encryption technologies, data analysis, and data recovery – offered a prize to any individual, professional data-recovery firm, or governmental agency who could recover data from a hard drive that had been overwritten just one time, with only zeros. 16 Systems initiated the contest to demonstrate recovering data from a zeroed hard drive was impossible and to dispel the "myth" that more passes were required.

The prize was never claimed.

Is DoD 5220.22M still the "gold standard" for drive erasure?

In a word: no.

Even though the DoD guidelines were initially developed for pre-2006 hard drives, you'll still find plenty of references around the web supporting a 3-pass process. Some sites even claim they "enforce" a 3- pass process as if it were a law, and claim it's "required" by the DoD. Aside from the fact the DoD never required private industry follow their standards, the simple truth is that the Department of Defense itself no longer references DoD 5220.22M.

What the DoD references now are new standards for data erasure from the National Institute of Standards and Technology, which are published in NIST SP 800-88. These newer standards rely on National Security Agency research which has confirmed that "one overwrite is good enough to sanitize most drives."

NIST SP 800-88 - Table 2.1 includes these relevant statements:

- Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. Clearing must not allow information to be retrieved by data, disk, or file recovery utilities. [...] Studies have shown that most of today's media can be effectively cleared by one overwrite.
- Purging information is a media sanitization process that protects the confidentiality of information against a laboratory attack. For some media, clearing media would not suffice for purging. However, for ATA disk drives manufactured after 2001 (over 15 GB) the terms clearing and purging have converged.

In practical terms, this means the majority of drives you have in service can be securely sanitized using a 1-pass process. ITAD providers automatically shred pre-2001 drives because they have no remarketing value, which is also true of drives with capacities under 15GB. (For that matter, ITAD providers would also shred any drive manufactured prior to 2013.) And looking further into NIST SP 800-88, Appendix 1 confirms that 1-pass overwriting is also valid for numerous non-ATA drive types.

The take-away: it's time to move to NIST SP 800-88

If you're still referencing DoD 5220.22M and specifying a 3-pass standard for data sanitization it's time to align your corporate requirements with current thinking and standards and move to NIST SP 800-88 when specifying drive sanitization requirements. Modern data sanitization utilities used by established ITAD providers not only ensure that data cannot be recovered after a 1-pass overwrite, they also generate drive-specific erasure reports that verify the overwrite procedure has completed properly. A report should always list the asset's inventory profile – including the hard drive serial number, model number, and asset tag number – to guarantee the link between the erasure and the hardware.

And be assured, if you retire a hard drive that's too old or low density to be sanitized with a 1-pass process – or one that can't be sanitized for any other reason - that drive was already headed to the shredder directly from product sort. Your ITAD partner is every bit as invested as you are in ensuring thorough data sanitization and data security.

About Ingram Micro's ITAD Services

Ingram Micro Lifecycle is a leading worldwide provider of enterprise IT asset disposition (ITAD), lifecycle support services, onsite data destruction, and e-waste recycling services that reduce the risk, cost, and complexity associated with securely managing IT assets throughout their lifecycle in compliance with environmental and data security regulations.

With the ability to provide service in a growing portfolio of over 80 countries, we manage the entire asset chain-of- custody seamlessly to provide secure and sustainable reverse logistics solutions for over 1,000 customer organizations.