DoD 5220.22-M Relevancy & the Evolution of Wipe Standards

www.WhiteCanyon.com | Sales@WhiteCanyon.com | 1 (801) 224-8900

Overview

Changes in technology and data storage devices have forced the DoD 5220.22-M erasure standard to be re-evaluated. The following document discusses the DoD 5220.22-M deletion standard, it's efficacy today and discover what organizations are using for their proven wipe method.

DOD 5220.22-M STANDARD

The DoD 5220.22-M data erasure standard was one of the earliest requirements for US military personnel on how to address data storage devices. Since this standard was one of the earliest, it became the ad hoc requirement for corporations, ITADs and data sanitization providers. This standard was incorporated in data erasure tools and became the pattern of choice for over a decade. But as new data storage technologies emerged, as we will discuss later, the DoD 5220.22-M standard became outdated and is no longer recommended by the DoD or other certification organizations.

The DoD 5220.22-M policy was first published in the National Industrial Security Program's Operating Manual in 1995 to address data erasure in hard drives. It also addressed the destruction of data in tapes and other media. The DoD standard specifically lays out how a hard drive should be overwritten with ones and zeroes.

The DoD 5220.22-M data sanitization method is implemented with the following overwrite pattern:

- Pass 1: Overwrite all addressable locations with binary zeroes.
- Pass 2: Overwrite all addressable locations with binary ones *(the compliment of the above).*
- Pass 3: Overwrite all addressable locations with a random bit pattern
- Verify the final overwrite pass.

The US Department of Defense 5220.22-M also addressed eradicating data from other media devices. See corresponding numbers below the following chart for the required process.

These methods of data eradication were adopted and used for the following decade. For data sanitization on hard drives, the DoD overwrite pattern would render all the data on a hard drive unrecoverable by software and hardware-based attacks.

DOD 5220.22-M DATA ERADICATION METHODS

MAGNETIC TAPE 1		
Media	Clear	Sanitize
Type I	1 or 2	1, 2, or 13
Type II	1 or 2	2, or 13
Type III	1 or 2	13

MAGNETIC DISK		
Media	Clear	Sanitize
Bernoullis	1, 2 or 3	13
USBs (floppys)	1, or 2	2, or 13
Non-Removable Rigid Disk	3	1, 2, 4, or 13
Removable Rigid Disk	1, 2 or 3	1, 2, 4, or 13

OPTICAL DISK		
Media	Clear	Sanitize
Read Many, Write Many	3	13
Read Only		13 or 14
Write Once, Read Many (Worm)		13 or 14

PRINTERS		
Media	Clear	Sanitize
Impact	7	16 then 7
Laser	7	15 then 7

MEMORY		
Media	Clear	Sanitize
Dynamic Random Access memory (DRAM	1, 2 or 3	13
Electronically Alterable PROM (EAPROM)	1, or 2	2, or 13
Electronically Erasable PROM (EEPROM)	3	1, 2, 4, or 13
Erasable Programmable (ROM (EPROM)	1, 2 or 3	1, 2, 4, or 13
Flash EPROM (FEPROM)	1, 2 or 3	13
Programmable ROM (PROM)	1, or 2	2, or 13
Magnetic Bubble Memory	3	1, 2, 4, or 13
Magnetic Core Memory	1, 2 or 3	1, 2, 4, or 13
Magnetic Plated Wire	1, 2 or 3	13
Magnetic Resistive Memory	1, or 2	2, or 13
Nonvolatile RAM (NOVRAM)	3	1, 2, 4, or 13
Read Only Memory ROM	1, 2 or 3	1, 2, 4, or 13
Static Random Access Memory (SRAM)	1, 2 or 3	13

EQUIPMENT		
Media	Clear	Sanitize
Cathode Ray Tube (CRT)	7	17

1. Degauss with a Type I degausser
2. Degauss with a Type II degausser.
3. Overwrite all addressable locations with a single character.
4. Overwrite all addressable locations with a character, its complement, then a random character and verify. THIS METHOD IS NOT APPROVED FOR SANITIZING MEDIA THAT CONTAINS TOP SECRET INFORMATION.
5. Overwrite all addressable locations with a character, its complement, then a random character.
6. Each overwrite must reside in memory for a period longer than the classified data resided.
7. Remove all power to include battery power.
8. Overwrite all locations with a random pattern, all locations with binary zeros, all locations with binary ones.
9. Perform a full chip erase as per manufacturer's data sheets.
10. Perform 9 above, then 3 above, a total of three times.
11. Perform an ultraviolet erase according to manufacturer's recommendation.
12. Perform 11 above, but increase time by a factor of three.
13. Destroy - Disintegrate, incinerate, pulverize, shred, or melt.
14. Destruction required only if classified information is contained.
15. Run five pages of unclassified text (font test acceptable).
16. Ribbons must be destroyed. Platens must be cleaned.
17. Inspect and/or test screen surface for evidence of burned-in information. If present, the cathode ray tube must be destroyed.

NISPOM

The DoD 5220.22-M document otherwise known as the NISP Operating Manual (National Industrial Security Program) received critical updates in 2001, 2004, and 2007.

The 2001 update added an extended overwrite pattern to the DoD-3 overwrite pattern. This new overwrite pattern was specified as DoD 5220.22-M ECE and soon became referred to as the DoD-7 pass. The DoD-7 pass data sanitization method is implemented with the following overwrite pattern:

- Pass 1: Overwrite all addressable locations with binary zeroes.
- Pass 2: Overwrite all addressable locations with binary ones (*the compliment of the above).*
- Pass 3: Overwrite all addressable locations with a random bit pattern
- Pass 4: Overwrite all addressable locations with binary zeroes.
- Pass 5: Overwrite all addressable locations with binary zeroes.
- Pass 6: Overwrite all addressable locations with binary ones *(the compliment of the above).*
- Pass 7: Overwrite all addressable locations with a random bit pattern
- Verify the final overwrite pass.

The 2004 provided limited addition to data sanitization methods and the 2007 update did not specify an overwrite pattern. After a decade of being the industry's principal overwrite pattern, the DoD 5220.22-M sanitization method started to cause issues that made the DoD and other organizations rethink their recommended data sanitization overwrite pattern.

Though the DoD-3 and DoD-7 overwrite patterns were on their way out in the military environment. Corporations and consumers were embracing the recommendation and continuing to adopt it as the recognized standard. This corporate requirement induced the majority of data sanitization software to include DoD 5220.22-M compliant overwrite patterns and the standard became universal in the industry.

TECHNOLOGICAL ADVANCES

For the past decade, the solid-state drive (SSD) has slowly become the storage device of choice over the hard drive. It is much faster, more reliable and has fewer mechanical failures, making it an optimum replacement as cost decreased. The SSD and other storage devices presented a major problem for the DoD standard. The standard was not created to address chip-based storage and the different mechanisms for handling the storage capacity.

This major issue, discovered by UCSD, caused a ripple effect in the industry and influenced NIST to release the NIST 800-88 Clear and NIST 800 88 Purge standards. The commercial space, including ITADs, have slowly accepted the new NIST standard but there are hold outs that still require a DoD overwrite pattern. (Please note, there is no certification for the DoD standard.) It is a requirement that organizations can be compliant to but not receive certification.

NIST ADDRESSES NEW TECHNOLOGY

NIST (the National Institute for Standards and Technology) functions to create commercial standards for materials and products. The agency first published a recommendation on data overwrites in 2006. The NIST 800-88r1 guideline provided methodology to address SSDs and other types of storage devices. This guideline was updated in 2012 with ATA commands and other recommendations for data sanitization. As with the DoD standard, there is no provided NIST certification for an organization or software tools. Organizations can only specify that they are NIST compliant when sanitizing electronic media.

The advances in technology have made the National Industrial Security Program DoD 5220.22-M Operating Manual overwrite standard obsolete. The DoD overwrite pattern was the proper method for over a decade. Since the standard was written new storage devices that are not correctly addressed by the DoD Standard have become widespread and the NIST standards were created to tackle the issues produced by these devices. As technology advances, we must assume that further standards will be created and adopted to address future storage techniques and hardware.

To learn more about the data erasure standards and methods WipeDrive supports, including DoD 5220.22-M, please contact us at 801.224.8900.