NIST 800-88 & DoD 5220.22-M

SGN Tech

OVERVIEW

The DoD 5220.22-M has long been an industry standard when it comes to data sanitization, but drive technology has changed drastically since the standard was last changed in 2006.

The more modern NIST 800.88 US government standard has taken the role as the primary erasure pattern for government, military and enterprise. Due to the necessary changes that arrived with SSD and newer drive technologies, Sipi Asset Recovery highly recommends using the current NIST 800.88 for sanitizing all drive types.

THE ORIGIN OF DOD 3-PASS WIPE STANDARD

The idea that multiple wipe passes are necessary to render data irrecoverable originates in part with a 1996 study published by Peter Gutmann who suggested that data should be wiped up to 35 times. He proposed that data could be recovered using magnetic force microscopy (MFM) and scanning tunneling microscopy (STM) techniques. Gutmann's study was widely cited and lead to the adoption of the DoD 3-pass wipe as a standard.

The Department of Defense 5220.22-M requires 3 overwrites passes (0's, 1's, Random) with a 100% verification pass. This standard was last updated in 2006 and in consideration of the pace of advancement in technology this criteria is significantly out of date.

Modern hard drives over the last 10-15 years have advanced in technology to the point where the MFM and STM techniques have become obsolete. Specifically, part of Gutmann's claim was that the head positioning system in hard drives was not precise enough to overwrite new data on top of the exact position of the old data, thus creating the possibility that the old data would remain intact. Today's hard drives are exponentially more precise and use radically different writing technologies eliminating this type of recovery as a potential vulnerability.

A BETTER STANDARD

NIST (the National Institute for Standards and Technology) Special Publication 800-88, originally released in 2006 and revised in 2012, takes into consideration the newer technologies in use today. The NIST Guideline provides an exhaustive overview of all the various storage media deployed today and offers recommendations for clearing, purging and/or destroying data on each one of them. Tools such as *WipeDrive's "NIST 800-88r1 purge/clear"** provide a wipe pattern that removes any device protection that prevents access to the full drive, including Device Configuration Overlay (DCO), Host Protected Area (HPA), Wear Leveling Areas or Accessible Max Address.

WHY WE RECOMMEND NIST

NIST overwrite pattern uses the strongest wiping techniques to remove all data from a device (including DCO, HPA, etc.) to ensure that all sectors of the drive are securely wiped. NIST 800-88 addresses the current state of drive technologies, including all types of Solid State memory drives that are commonly used today.

NIST is secure: In all cases the NIST 800-88 pattern prevents any data recovery, even under laboratory conditions. Using multiple passes is unnecessary and less secure than a single pass properly performed by a certified erasure tool.

NIST is better for the environment: As the time required to sanitize drives is shorter, *wiping hard drives per the NIST standard save energy ad electricity* and is thus more ecologically conservative.

NIST improves efficiency: A single overwrite pass provides improvements in process efficiencies, allowing assets to move through to final disposition sooner, while keeping risk down, compliance high and value recovery at maximum potential.

KEY DIFFERENCES

	DoD 5220.22-M	NIST 800-88 Rev. 1
Number of overwriting passes	3	1
Standard current date	Revised 2006	Revised 2012
Considers new technology (e.g.: SSD)	No	Yes
Sector created for	Government	All organizations
Outlines specific data erasure methods	No	Yes
Verifiable secure method of erasure	Yes (HDD only)	Yes
Maximum ecological conservation	No	Yes

*Wiping software produced by White Canyon.