blancco

Data Sanitization in the Modern Age: DoD or NIST?

Any organization that handles sensitive customer information has a legal duty to dispose of said information fully and irretrievably when it is no longer in use or required for regulatory purposes. Today, customers have far greater autonomy over how businesses use and store their data, and with cybercrime accelerating, businesses need more comprehensive data protection and data erasure policies across the data lifecycle.

For organizations tasked with fully sanitizing data stored on IT assets, there are several "standards" that may be followed. The two most widely utilized in the US are from the US Department of Defense (DoD) and the National Institute for Standards and Technology (NIST). The DoD standard – DoD 5220.22-M – is 25 years old. The NIST standard – NIST 800-88 – accounts for more recent technologies and technical advancements.

The DoD three-pass standard was last updated in 2006, a time before many of today's technologies existed. This raises concerns for today's organizations, as the sanitization of SSDs and other recent storage technologies is not considered by the DoD standard. The most recent standard is the Special Publication 800-88 from NIST, which is the go-to data erasure standard for organizations in the United States.

The table below illustrates the key differences between the DoD standard and the NIST standard.

	DoD 5220.22-M or DoD 5220.22-M ECE	NIST 800-88
Number of overwriting passes	3 or 7	1
Standard last updated	February 2006	December 2014
Considers SSD erasure	No	Yes
Created for	Government	All organizations
Verifiably secure method of erasure	Yes (HDDs only)	Yes
Outlines specific data erasure methods	No	Yes

Useful Resources

How many passes is recommended for data to be unrecoverable?
Multiple overwrites are not necessary today, thanks to advances in technology. The DoD standard does not account for newer technologies and recommends a three-pass method. NIST, which does take these technologies into account, recommends a single, secure overwrite. One overwrite is adequate to erase data – nothing is gained by any additional passes.

Which method is more economic for businesses?
Overwriting data multiple times is costly in workforce hours and power. The NIST standard saves organizations time and money while increasing security.

blancco

Am I taking on any additional risk?
The NIST standard actively reduces risk. As a more recent data sanitization standard, it accounts for newer technologies and highlights the need to render data completely unrecoverable.

What is the difference between NIST Clear and NIST Purge?

NIST Clear	NIST Purge
"Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. 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." Degaussing of any hard drive assembly usually destroys the drive as the firmware that manages the device is also destroyed.

Blancco's Drive Eraser software is compliant with both NIST Clear & Purge; however, we also acknowledge that industry terminology is highly convoluted. Blancco uses data sanitization terminology as defined by the International Data Sanitization Consortium, including the term "data erasure." There are three steps included in data erasure:

1. The data is successfully and permanently removed from the storage device (via at least one overwrite wipe).
2. The data's removal has been verified.
3. The data's removal is certified via a tamper-proof report.

In this way, we both meet and achieve the data sanitization requirements put forth by NIST, as degaussing, Secure Erase and clearing all have their own data security limitations.

Access the complete NIST Guidelines for Media Sanitization here.

For more information on permanent erasure through Blancco Data Eraser solutions, visit our website.