Everything You Need to Know About the DoD 5220.22-M Disk Wiping Standard & Its Applications Today

MAY 09, 2022 BLOG ARTICLE

When vendors state that their solutions meet the DoD 5220.22-M "standard," it typically means that their software will write to all addressable hard drive locations with a character, its complement and a random character. It must then be followed by verification. This "3-pass" procedure is designed to prevent data from being recovered by commercially available processes.

But is the DoD 5220.22-M standard ((or, the longer DoD 5220.22-M ECE standard) the best wiping method for your organization?

Read more to learn about how the DoD data overwriting standard applies today.

Richard Stiennon

Security executive Richard Stiennon has previously held roles such as Chief Strategy Officer of Blancco Technology Group from 2016-2017 and Vice President of Research at Gartner Inc. from 2000 to 2004. Currently, Richard is a cyber security lecturer at Charles Sturt University in Australia and a strategic advisory member of the International Data Sanitization Consortium. His book, There Will Be Cyberwar, was named a Washington Post bestseller in April 2016. Richard is regularly featured in news publications such as Forbes, Dark Reading, Infosecurity Magazine, Network World and BetaNews, where he comments on data governance, data management, and cyber security.

What is the DoD Standard (DoD 5220.22-M)?

The "DoD standard," referring to DoD 5220.22-M, is a term often used in the data sanitization industry. But what does this "standard" mean for enterprises, government entities, ITADs, and data sanitization solution providers?

To effectively erase previously stored data, the simplest techniques overwrite hard disk drive storage areas with the same data everywhere—often using a pattern of all zeros. The DoD "standard" and others like it take overwriting a step further with prescribed random overwriting methods. At a minimum, such applications will prevent the data from being retrieved through standard data recovery methods.

A Brief History of the Standard

The DoD 5220.22-M method for data erasure first appeared in the early days of the data sanitization industry. When it was published by the U.S. Department of Defense (DoD) in the National Industrial Security Program Operating Manual (also known as "NISPOM," "NISP Operating Manual," or Department of Defense document #5220.22-M), it specified a process of overwriting hard disk drives (HDDs) with patterns of ones and zeros. The process required three secure overwriting passes and verification at the end of the final pass. This was in 1995, before the debut of smartphones and the widespread use of flash-based storage technologies.

Reflecting its original requirements, the DoD 5220.22-M data sanitization method, or the DoD 3-pass method, is usually implemented in the following way:

- **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.

Erasing an HDD using the DoD 5220.22-M data sanitization method will prevent all software-based file recovery methods, as well as hardware-based recovery methods, from recovering meaningful data from the drive.

In 2001, a DoD memo specified additional overwriting and verification methods that became accepted as part of the "standard." The DoD 5220.22-M ECE method is an extended (7-pass) version of the DoD 5220.22-M. It runs the DoD 5220.22-M twice, with an extra pass (DoD 5220.22-M (C) Standard) sandwiched in between.

However, the latest version of the DoD 5220.22-M "standard," hasn't **specified an overwriting pattern for erasing hard drives** since at least 2006, though the 3-pass method is still standard practice when implemented.

In the most recent update, which occurred in 2021, the NISP Operating Manual became effective as a federal rule. Referred to as the "NISPOM rule," it replaces the NISPOM previously issued as a DOD policy and, again, **never specifies a method of data sanitization.**

Instead, it refers contractors to other government organizations (Cognizant Security Agencies, or CSAs). See § 117.18 Information system security.

Despite the absence of a current data erasure specification, the older 3-pass DoD 5220.22-M sanitization method is still one of the most common sanitization methods used in data destruction software, and in general, is often perceived as an industry standard in the U.S.

Most data sanitization software, including Blancco Drive Eraser, supports multiple data sanitization methods, including both DoD 5220.22-M 3-pass and 7-pass methods. However, in most cases, this DoD technique is now less effective, more resource demanding, and less economical than more modern standards, so it has fallen out of recommended practice even at federal agencies. Yet because even historical Department

of Defense standards are held in high esteem and carry great credibility, organizations' internal policies and information security teams may still require it.

> **Today's organizations use both HDDs and SSDs. Enterprise data sanitization requires more than a DoD wipe:** Take A Look At Modern Best Practices.

The Truth Behind DoD 5220.22-M Sanitization Method

Today, DoD 522.22-M is readily available as a data wiping option, but has been superseded by other data sanitization standards such as those from the National Institute for Standards and Technology: *NIST 800-88 Clear* and *NIST 800-88 Purge* (Our best practice download, "Data Sanitization in the Modern Age: DoD or NIST?" delves into this more.)

There are several reasons for this, some of which may influence you to consider using a different data wiping standard for complete data erasure:

- DoD 5220.22-M processes are difficult to apply to solid-state drives (SSDs), which pose different issues when needing to completely and permanently erase stored data.
- The Department of Defense no longer references DoD 5220.22-M as a method for secure HDD erasure.
- In like fashion, regulations and certification programs (especially in the government sector) now cite NIST SP 800-88 media erasure guidelines—not the DoD "standard."
- The NISPOM does not define any U.S. government standard for data sanitization. Instead, the Cognizant Security Authority (CSA), a select group of U.S. government agencies, is permitted to establish sanitization standards.
- The CSA is responsible for data sanitization standards for their own respective agencies and agencies under their purview, but the DoD 5220.22-M method is no longer permitted for use by various CSA members.
- Multiple overwrite passes are not always necessary. Due to technological advances since the DoD 5220.22-M method was first published, one overwrite pass is often sufficient, reducing the time and energy resources needed for effective data sanitization.

- For its own classified data, the DoD requires a combination of wiping, degaussing and/or physical destruction.
- The three-pass sanitization provision in the 1995 edition of the National Industrial Security Program Operating Manual (DoD 5220.22-M) was removed in the 2001 memo mentioned earlier, and the three-pass method was never permitted for Top Secret media.
- "Approved by DoD" claims are misleading, though achieving the overwriting method outlined by the DoD "standard" is certainly possible.

In the IT asset disposition (ITAD) space, operators and customers often cite a "DoD certification," but the reality is that no such certification exists. Instead, the U.S. Department of Defense adheres to NIST 800-88 Guidelines for Media Sanitization. However, even this is a guideline, not a certification (To understand the importance of both data erasure certifications and third-party validations, see "Why are Data Erasure Certifications & 3rd Party Validations So Important?"). And, as previously mentioned, most government and other regulations and certification programs now cite NIST SP 800-88 media erasure guidelines—not DoD 5220.22-M.

A Focus on NIST

In the past few years, NIST Special Publication 800-88 has become the go-to data erasure standard in the United States. Originally issued in 2006 and revised in December 2014, this publication addresses flash-based storage and mobile devices, which weren't considered under the DoD process. It outlines the preferred methodologies for data

sanitization for hard drives, peripherals, magnetic and optical storage and other storage media under Minimum Sanitization Recommendations in Appendix A. These methods include overwriting and Secure Erase, which is a protocol built into a hard drive.

Our article, "What is NIST 800-88, and What Does "Media Sanitization" Really Mean?" goes into greater detail, but essentially, NIST describes three methods that can help ensure that data is not unintentionally accessed:

- **NIST Clear**. This method sanitizes data in all user-addressable storage locations using logical techniques. It is usually applied through the standard Read and Write commands to the storage device.
- **NIST Purge**. This method applies physical or logical techniques that prevent data recovery using advanced laboratory techniques.
- **NIST Destroy.** This method relies on physical destruction using state-of-the art techniques to prevent data recovery, but also prevents the media from being reused for data storage.

The NIST Special Publication 800-88 was published with the intent to provide guidelines for sanitizing electronic media, and the table, "Media Sanitization Decision Matrix" in Appendix A can be very helpful to enterprises and others weighing different options for data destruction. The document does not, however, provide standards, requirements or specifications.

What Does It Mean to Erase to the DoD Standard?

We've already noted that the latest version of the NISPOM (DoD 5220.22-M) does not specify a method for achieving secure erasure, so in no way is the manual actually a standard.

The guide does state, however, that "instructions on clearing, sanitization and release of IS [information system] media shall be issued by the accrediting CSA." Standards for data sanitization are the responsibility of the Cognizant Security Agencies. The CSAs are: Department of Defense, Department of Energy, Nuclear Regulatory Commission, Office of the Director of National Intelligence, and Department of Homeland Security.

When vendors state that their solutions meet the DoD 5220.22-M "standard," it typically means that their software will write to all addressable hard drive locations with a character, its complement and a random character. It must also then be followed by verification. The procedure is designed to prevent data from being recovered by any

commercially available process.

It's important to note that the U.S. National Security Agency (NSA Advisory LAA-006-2004) stated in fall 2004 that using just *one* overwrite using the DoD process is sufficient to achieve data sanitization. However, disk wiping software cannot sanitize hard drives that have physically failed or internal hard drives that are disconnected. Such software is also limited in reaching data in hidden sectors on solid state drives.

Physical Destruction vs. Data Erasure

If your drives are no longer required, another method to achieve data sanitization is physical destruction through melting, crushing, incineration or shredding.

Physical destruction is not ideal if you want to reuse your drives, as they'll be completely destroyed, but even this method isn't necessarily absolute. If any disk pieces remain large enough after destruction (especially on SSDs), they can still contain recoverable information. Data erasure software, however, doesn't leave information behind, and the disks can be reused after they're erased—preserving costs.

Whichever method you choose, whether it be physical destruction or data erasure software or both, your organization must first have policies in place to govern hard drive disposal and data sanitization for other IT assets, including servers, laptops and removable media. These policies should include training for employees so that they can take proven steps to keep data out of harm's way. The U.S. Federal Trade Commission's Fair and Accurate Credit Transactions Act (FACTA) rule is one of the many regulations that governs the proper storage and disposal of specific consumer information and requires that such information is disposed of properly.

The best way to ensure data removal—for the highest security environments—is to combine software-based data erasure with physical destruction. That way, there's absolutely no chance the data can be recovered from any fragments because it has been removed completely.

Which Data Destruction Method is Right for You?

The DoD method is no longer recommended best practice but can be effective in some instances. It can sometimes also be required by your organization's policies or other regulations. Increasingly, however, organizations are using NIST 800-88 sanitization methods to prevent unauthorized access of data and sanitize their data storage devices.

Private businesses and organizations within the U.S. are also adopting NIST sanitization standards and leaving the DoD three-pass method increasingly behind.

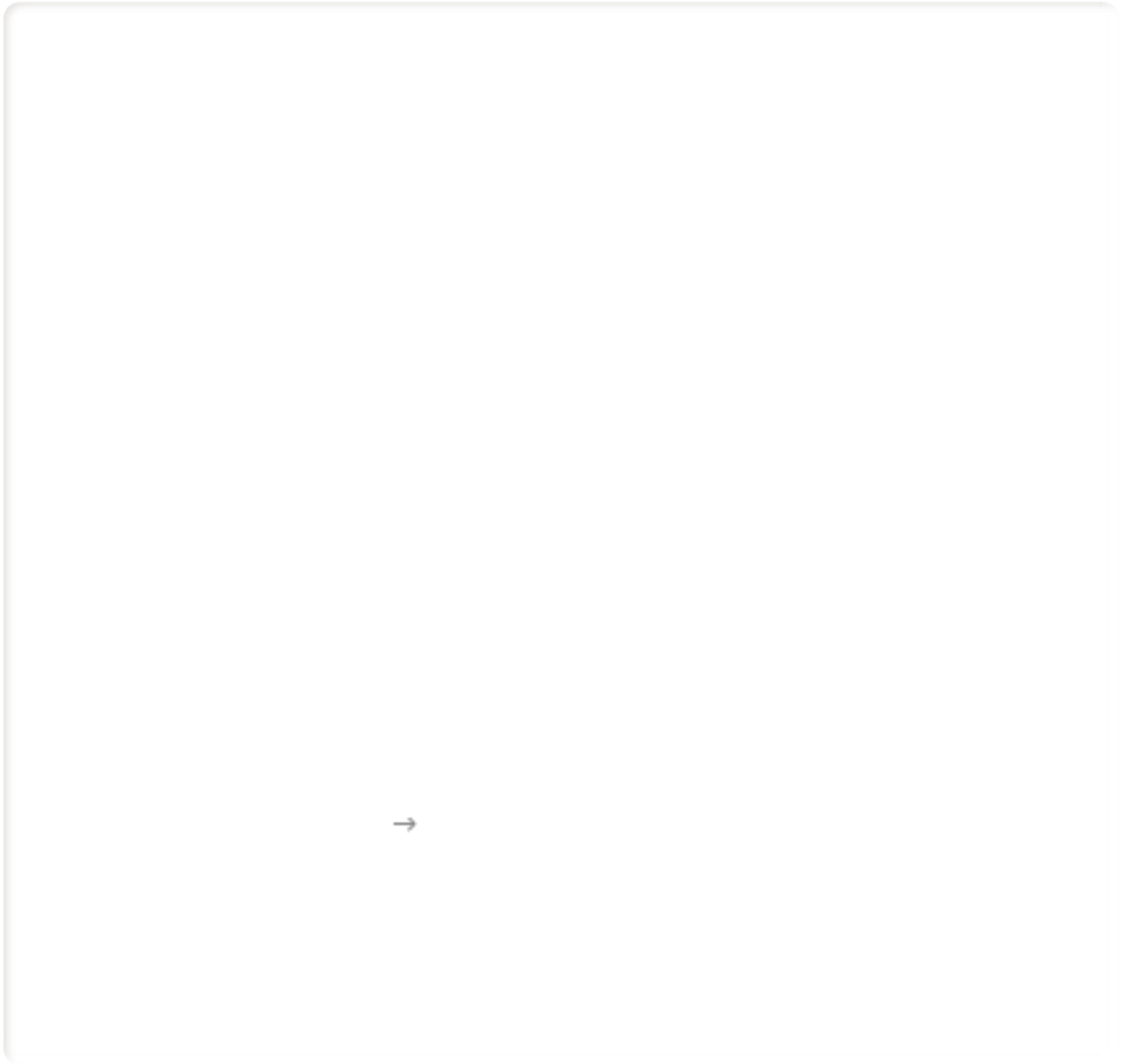
What is NIST 800-88, and What Does "Media Sanitization" Really Mean?

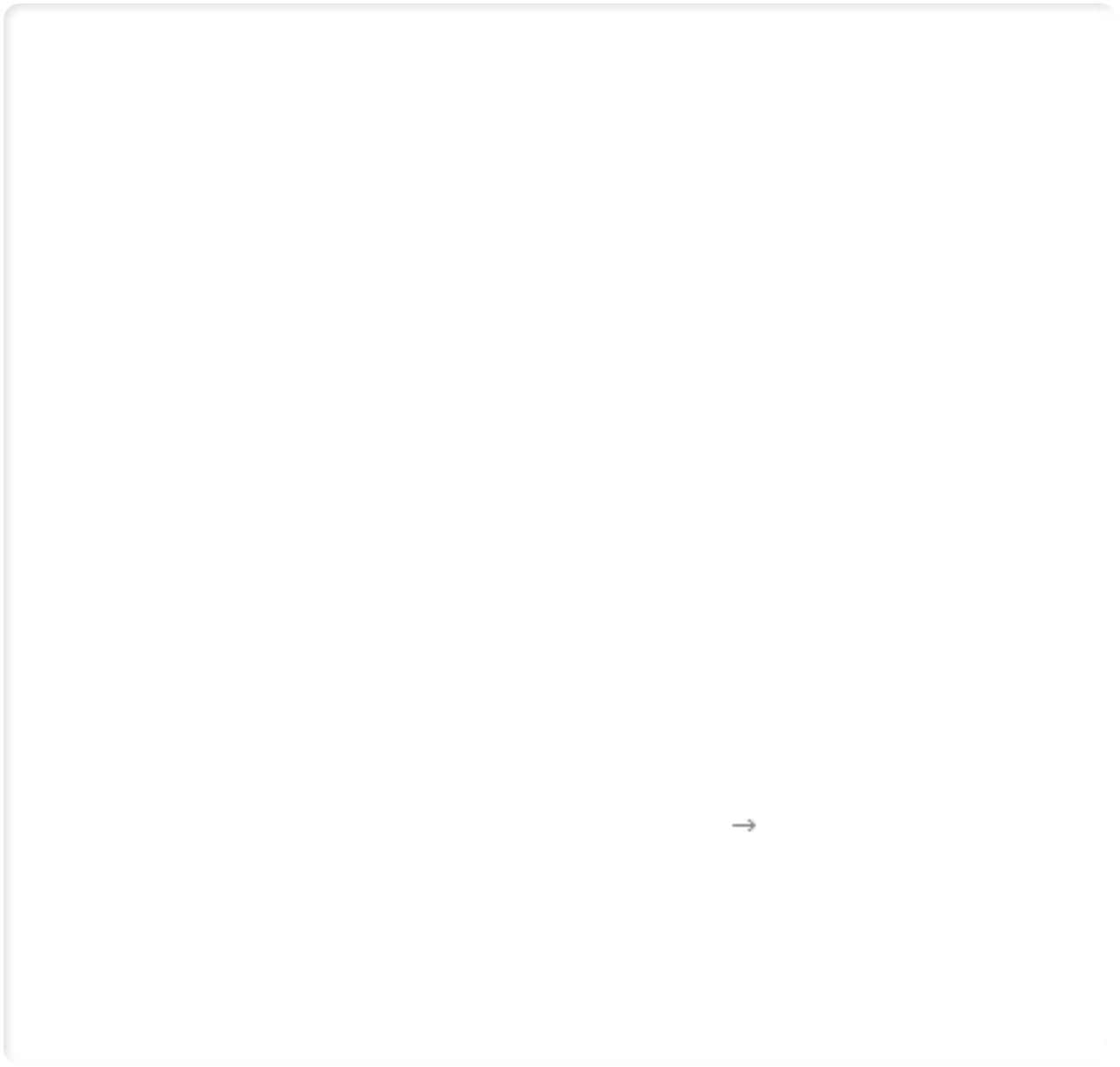
Whether you choose to use DoD, NIST, or other data sanitization methods, Blancco data erasure solutions carry more global certifications than any other data sanitization software and erase to more standards—ensuring no data remains behind on government or enterprise hard disk drives or solid-state drives.

Ensure Complete, Permanent Media Sanitization

Whether you choose DoD 5220.22-M, NIST 800-88 Clear or Purge, or another leading data sanitization method, see how Blancco ensures secure and compliant data erasure for virtually any government or business data storage device.

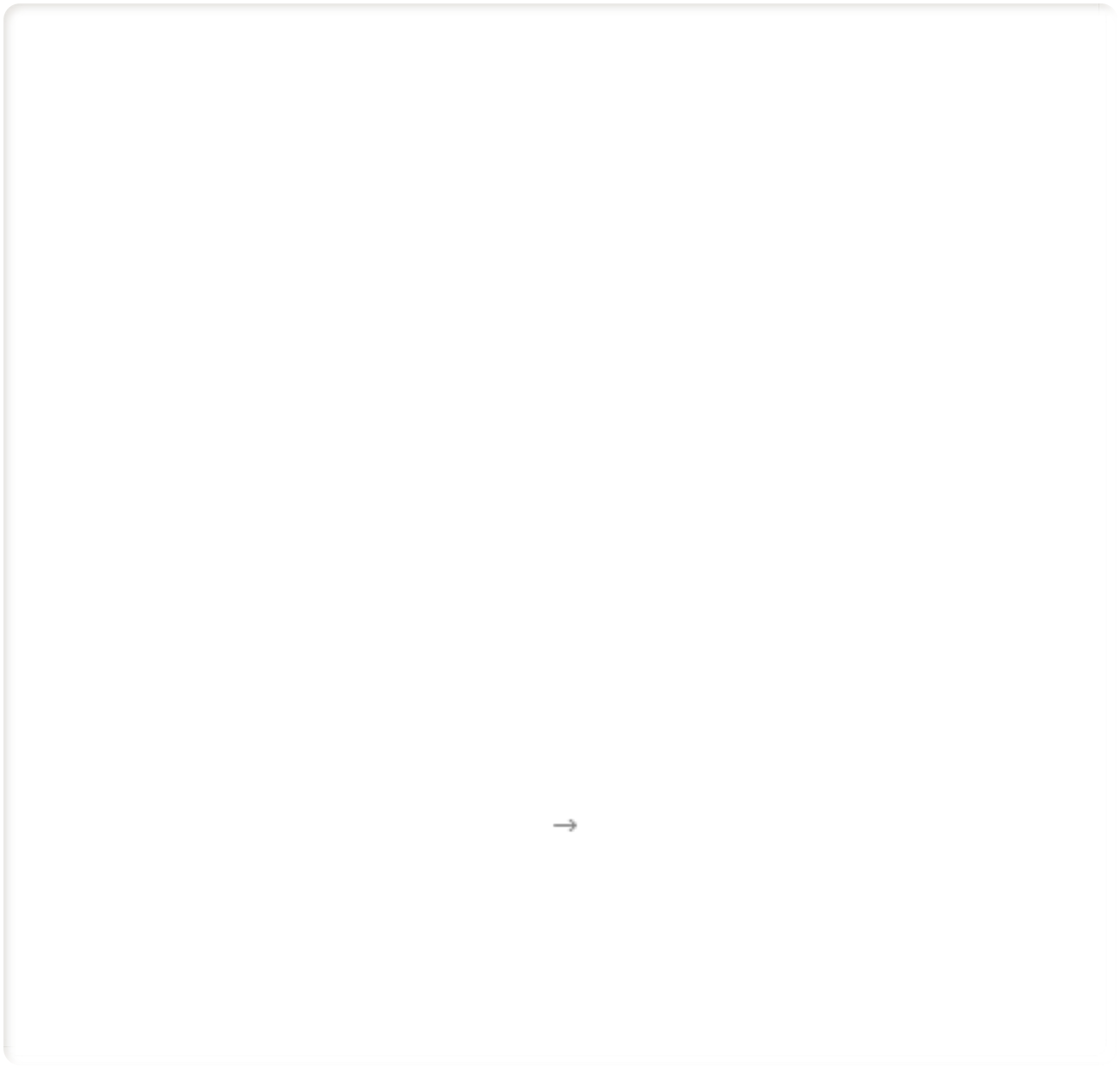
Originally published June 15, 2017, updated and expanded March 28, 2019, and updated most recently on May 9, 2021, with information on changes regarding the NISPOM Rule.





→

Survey of 1800 global IT leaders shows how organizations must leverage secure data erasure to manage data growth from cloud computing.



See all solutions

PORTALS

Cloud portal

Support portal

RESOURCES

Resource Hub

Case Studies

EVENTS

Event & Webinars

COMPANY

About Us

Certifications

Supported Standards

Our Team

News & Press

Careers

Sustainability

PARTNERS

Why Partner with Blancco

Blancco Technology Alliance Partners

Find a Partner

Partner Portal log in

INVESTORS

Investor Center

Investors Contact

STAY UP TO DATE

Email

Yes, I would like to receive information regarding Blancco products and service. I understand that I can opt-out at any time. Any personal data you provide is subject to Blancco's **Privacy Policy**

Subscribe

FOLLOW US

SEARCH

Search The Site

Privacy Policy Cookie Policy