An In-Depth Guide to Meeting Federal Data Destruction Regulatory Compliance

SEM®

Global Leader in High Security Information End-of-Life Solutions for Over 50 Years

Data security encompasses all aspects of information protection and has been an integral part of federal policy since the Social Security Act of 1934 made it illegal to disclose an individual's social security number and personally identifiable information (PII). Since then, numerous federal programs and processes specific to the privacy and security of personal, financial, health, and intelligence information have been instituted. Of these, the creation of the National Security Agency (NSA) in 1954 and the enactment of the Privacy Act of 1974 are two of the most pivotal.

Under the Director of National Intelligence, the NSA is an intelligence agency of the United States Department of Defense (DoD) and has responsibility for global monitoring, collection, and processing of information of foreign and domestic intelligence and counterintelligence purposes. In other words, all classified information falls under the jurisdiction of the NSA. The Privacy Act of 1974, based on the fact that privacy is a fundamental right protected by the Constitution of the United States, acknowledges that "The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information." Further, the Privacy Act of 1974 extended protections to any and all records, whether paper or digital, containing PII pertaining to an individual's education, financial, medical, criminal, or employment history as well as photographs, fingerprints, and voiceprints.

While many other data security regulations exist, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) for the healthcare sector and the Fair and Accurate Credit Transactions Act of 2003 (FACTA) for financial services, and numerous other U.S. state laws, the security regulations that matter the most to federal entities come from the NSA for classified and top secret information and the National Institute of Standards and Technology (NIST) for controlled unclassified information (CUI) in Executive branch agencies. Data destruction is an integral part of any comprehensive data security policy, including those governed by the NSA and NIST.

SEM®

Paper

While some people maintain that paper is going away, this simply is not the case at present or in the foreseeable future. Paper is and will continue to be the most important information-bearing media in the federal government and private sector, and often contains personal, confidential, or even classified and top secret data. As such, paper used in the federal government must be physically destroyed in order to maintain data security and privacy.

Classified and Top Secret

Paper bearing classified and top secret information must be destroyed to NSA specifications, currently a 1mm x 5mm (DIN 66399 P-7) final particle, in an NSA evaluated and approved device. Such devices are listed on the NSA's Evaluated Products Lists (EPLs) for Paper Shredders and for Paper Disintegrators. While both types of devices effectively destroy classified and top-secret information, they are distinctly different and are therefore used in specific applications.

Self-contained, portable, and compact, paper shredders are typically used in lower volume and/or office environments and the NSA rates these devices as low, medium, and high volume on the EPL for Paper Shredders. These devices are quiet, efficient, and often come equipped with standard 110V electrical. Paper shredders are convenient, reliable, and relatively inexpensive, but NSA listed paper shredders do have some drawbacks. First, they ONLY accept paper. Feeding optical media, ID cards, dog tags, or even staples

NSA listed high security paper shredders

and/or paper clips into an NSA listed paper shredder can potentially damage the device. Therefore, users must be conscientious when destroying classified documents in an NSA listed paper shredder in order to maintain the integrity of the machine. Second, NSA listed paper shredders are not intended for higher volumes. The highest volume paper shredders on the NSA EPL for Paper Shredders can accept a maximum of approximately 30 reams per hour. Thirdly, NSA listed paper shredders do not accept paper that is crumpled, bulky, or in booklet form. And finally, high security paper shredders do not provide any type of briquetting or compacting solution, meaning that the wastepaper must be traditionally discarded as recyclers typically do not accept shredded paper due to the bulk of the final particles. Therefore, NSA listed paper shredders should be used specifically for low and medium volumes of classified information as found in office environments.

The NSA mandates that classified paper be destroyed to a particle size of 1mm x 5mm or less (DIN P-7)

Centralized military high security destruction facility utilizes two disintegrators with briquettors

As an alternative to paper shredders, NSA listed paper disintegrators are ideal for high volumes of paper, but not for office environments, for several reasons. First, paper disintegrators are bulky devices powered by 3-phase electrical, often requiring large, dedicated spaces in which to operate. They are also fairly loud and dusty, which is why they are often installed with enclosures to minimize sound, odor, and errant dust particles. Additionally, disintegrators come at a much higher price point than NSA listed paper shredders.

But as far as classified paper destruction goes, the positives associated with disintegration over shredding far outweigh the negatives. NSA listed paper disintegrators accept media other than paper including classified CDs, paper clips, staples, and binder clips. They also accept bulk and crumpled paper, making them extremely convenient for high volume destruction of classified material. Although not recommended for office environments, paper disintegrators come with a variety of options, making them an ideal solution for any other type of classified paper destruction application. These options include sound proofing, feed conveyors, air evacuation systems, cart tippers, master control panels, air locks, air stands, and inline magnetic separators, as well as briquetting systems that produce 90 percent less waste than standalone disintegrators. Briquettes are fully recyclable, making disintegrators with briquettors a zero landfill, green solution — a feature that is critically important in all industry including the federal government. For example, the CIA incorporates numerous green initiatives that are led by the Directorate of Support through its Green Council, which was created in 2009 to consolidate Agency-existing sustainability efforts, advance energy and environmental initiatives,

and to meet federal government sustainability. Mollie Halpern from the FBI Office of Public Affairs has stated, "The FBI is committed to integrating earth-friendly practices into the way we carry out our law enforcement mission." And the U.S. military, who is the major institutional energy consumer in the United States, has long been committed to renewable energy and green solutions for both the safety of its troops as well as the health of the planet.

CUI

Controlled Unclassified Information (CUI) on paper has long been destroyed to less stringent standards, typically a 4mm x 40mm (DIN 66399 P-4) particle, but that has changed in recent years. All unclassified information throughout the Executive branch that requires any safeguarding or dissemination control is characterized as Controlled Unclassified Information (CUI) and includes nearly all government agencies. Further, unclassified data such as For Official Use Only (FOUO), Sensitive But Unclassified (SBU), Personally Identifiable Information (PII), as well as information relating to critical infrastructure, defense, export control, financial, immigration, intelligence, international agreements, law enforcement, legal, natural and cultural resources, NATO, nuclear, patent, privacy, procurement and acquisition, proprietary business information, provisional, statistical, tax, and transportation all fall under this requirement.

The ISOO CUI mandate covers nearly all government agencies

Executive Order 13556 "Controlled Unclassified Information" (the Order) establishes a program for managing CUI across the executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance. The Archivist of the United States delegated these responsibilities to the Information Security Oversight Office (ISOO). 32 CFR Part 2002 "Controlled Unclassified Information" was issued by ISOO to establish policy for agencies on designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI, self-inspection and oversight requirements, and other facets of the program.

Prior to the CUI Program, agencies often followed agency-specific policies and procedures to handle CUI, resulting in a patchwork approach of inconsistent and often insecure information management.

The ISOO CUI directive, which affects all Executive branch agencies, has very clear requirements for information end-of-life, mandating that all CUI information be destroyed to NIST 800-88 Guidelines for Media Sanitization specifications. Like the NSA, NIST 800-88 specifies that information-bearing paper be destroyed to a 1mm x 5mm particle, which is the same particle size as required for classified and top secret information. Therefore, all CUI paper must be destroyed using a high security shredder or disintegrator that produces a final particle size of 1mm x 5mm or less, such as those listed on the NSA EPL for classified paper destruction.

Non-Classified

DIN level P-4 particle (4mm x 40mm) is acceptable for sensitive and confidental non-classified paper

Non-classified paper is easier to destroy due to the increased number of available options. Not to be confused with CUI, which must be destroyed to NSA standards, non-classified material is typically found in commercial rather than federal operations and is governed by many different regulations. These include HIPAA for medical and health information, FACTA and GLBA for financial institutions, PCI DSS for payment card industries, FISMA for non-Executive branch federal information, Sarbanes-Oxley for public companies, and various state mandates for state and local agencies, to name a few. While these varying regulations have different requirements, a DIN P-4 final particle is acceptable for sensitive and confidential paper destruction.

Paper shredders are the best way to destroy non-classified paper. Unlike their classified counterparts, non-classified paper shredders are capable of accepting other types of media including optical media, plastic cards, paper clips, and staples. They also have higher throughputs and feed rates. Office environments with low to mid-volume will find a simple and inexpensive non-classified paper shredder to be effective. Higher volume applications are best-met with industrial paper shredders, which come with a variety of convenience options including feed conveyors, waste conveyors, feed hoppers that accept crumpled and bulk paper, and baling solutions. Industrial paper shredders are also available in a variety of final particle sizes.

Digital (IT) Media

In modern times, digital media houses the majority of classified, CUI, and non-classified information. Because digital media is so dense and can hold vast amounts of information, it is critical that it be properly sanitized at end-of-life. Of course, the appropriate sanitization method is entirely dependent on both type of digital media and regulatory requirement.

Rotational Hard Drives and Magnetic Media

A hard disk drive (HDD) is an electromechanical, platter-based data storage device while magnetic media is any storage medium that uses magnetic patterns to store information, such as tapes and floppy disks. HDDs are still the storage media of choice for both government and commercial applications as they are both reliable and affordable. The use of tape media, once considered almost obsolete, has been making a resurgence as technology has increased the storage capacity and reliability of tape media, which has always been a cost-effective solution for data storage.

Degaussing

The NSA has clear destruction requirements for classified information stored on any type of magnetic media, and it is a two-step process: degauss and destroy. Degaussing permanently erases data from magnetic media by rearranging or scrambling the magnetic field. Not to be confused with secure erasure, degaussing is permanent, rendering the drive inoperable. Degaussing is considered to be far more secure than any type of erasure, secure or otherwise, as erased drives still contain remnant data that could potentially be recovered with the right tools and time. Therefore, NSA requires that HDDs or magnetic media with classified or top secret data be degaussed in an NSA evaluated and listed degausser, after which the degaussed drive must be physically destroyed.

Crushing and Shredding

HDDs can be effectively destroyed by crushing and shredding, and the choice is entirely dependent on specific application. Hard drive crushers use force and an anvil to puncture and bend the rotational platter. For very low volume applications or in situations where access to electricity is an issue, a manual hard drive crusher is an acceptable solution. At the push of a button, automatic hard drive crushers mangle hard drives as effectively as manual crushers. Both manual and automatic hard drive crushers are highly portable, making them ideal for multi-office locations. Typically, crushers are used in lower volume applications of less than 100 drives per day.

Hard drive crushers are ideal for low volume office applications

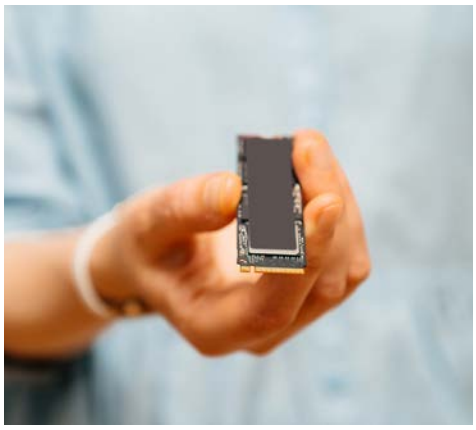
Standard final particle size for an HDD shredder is 1.5", while 1.0" and 0.75" options ar also available

Hard drive shredders are larger, faster machines that can be operated continuously over a long period of time, making them ideal for higher volume destruction applications. HDD shredders utilize sawtooth cutting blades to shred drives from 0.75" to 1.5" final particle size and come in a variety of sizes and configurations. Small machines with sound proofing and HEPA filtration destroy up to 250 drives per hour and are ideal for data centers. Large machines can destroy up to 3,500 drives per hour and come with customizable convenience features such as feed and waste conveyors, making them ideal for centralized destruction such as found in military and intelligence operations. Newer hard drives, also called enterprise drives, are constructed of heavy, solid components and are much denser than their predecessors. These industrial grade drives require a hard drive shredder specifically manufactured for the destruction of enterprise drives.

Best practices for the destruction of non-classified drives includes crushing or shredding. For most magnetic media, a crusher or shredder used on its own is acceptable. However, for drives containing highly sensitive or confidential information, drives should be degaussed prior to physical destruction, as mandated by the NSA. Most regulations outside of the NSA — such as HIPAA, FACTA, FISMA, PCI, Sarbanes-Oxley, and NIST 800-88 — require that CUI, sensitive, or personal data on rotational hard drives and magnetic media be unrecoverable, and the best way to accomplish this goal is with physical destruction.

HDDs that have been both degaussed and crushed are unrecoverable

Solid State Drives



Unlike HDDs that rely on rotating platters, solid state refers to any electronic device physically comprised of solid and non-moving components. Solid state components are engineered so that they can reverse and amplify electric current and they are typically constructed with semiconductors to manage the movement of positive and negative electric charges. Solid state technology is used in transistors, insulators, integrated circuits, memory, and storage equipment and includes solid state drives (SSDs), circuit boards, SIM cards, thumb drives, and flash memory.

Unlike rotational hard disk drives and other magnetic media, solid state drives and devices do not utilize magnetic fields and therefore cannot be degaussed. Rather, they are electronic devices, systems, and parts based entirely on the semiconductor. Therefore, the only acceptable means of SSD data destruction is physical destruction. And because SSDs store vast amounts of data on small flash memory chips, it is possible to recover data from even small fragments of SSDs as long as the chip is intact. To eliminate the possibility of data recovery from solid state devices, each and every chip must be destroyed. Therefore, SSDs should only be destroyed in devices specifically engineered to destroy solid state media, as rotational hard drive shredders produce a larger shred size, creating the possibility that some SSD chips could escape undamaged — leaving large amounts of data intact and recoverable.

Per the NSA, classified SSDs must be destroyed to a particle size of less than 2mm

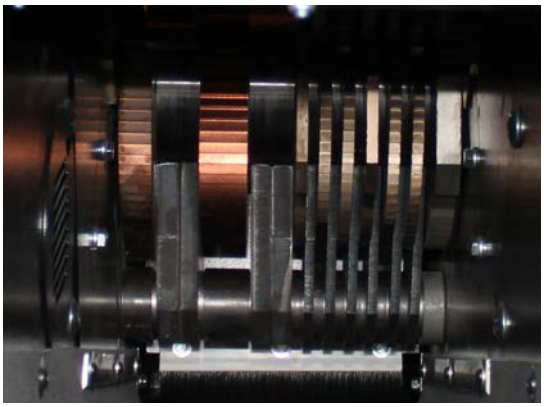
Classified

Classified and top secret data stored on solid state drives and devices must be destroyed to NSA standards, currently a particle size of less than 2mm. While this particle may seem exceedingly small and a bit of overkill, the NSA has instituted this standard due to the sophistication of technology available to hackers and criminals in today's world. Chips on solid state drives and devices are becoming increasingly dense, and even the smallest chip may still contain enough sensitive information to cause damage to the United States government and citizens if it made its way into the wrong hands.

The only NSA approved devices for destroying classified SSDs are disintegrators and incinerators, which provide the most complete chip destruction and the highest level of security. The NSA mandate for solid state incineration is that the device or drive must be turned to ash. Incinerators are considered problematic to the environment as they release toxins into the air. Additionally, turning a solid state drive or device to ash requires a tremendous amount of heat and energy. Therefore, disintegrators are the methodology of choice for most federal agencies.

While true disintegrators utilize rotary knife mill or granulator technology, the NSA has approved hammermills under the disintegrator umbrella. Hammermills destroy media in a grinding chamber where the material is struck repeatedly by hammers mounted on a horizontal, swiftly rotating shaft. The media is then continuously pulverized by hammer blows and by being forced against the walls of the grinding chamber until it is able to pass through a screen to create a uniform particle size, in this case less than 2mm. While hammermills are effective and efficient, they are also particularly dangerous. Due to the constant, high pressure battering of material, hammermills create airborne dust particles and are excessively loud. In addition, hammermills operate at high speeds under extreme pressure, friction, and high temperature, causing sparks and hot particles that can cause flash fires. There have been instances of hammermills causing combustible dust explosions due to a combination of the sparks and the airborne dust. For these reasons, hammermills should be used with caution.

Using heavy duty blades, SSD granulators (hereafter referred to as disintegrators) continuously cut SSDs until they are small enough to pass through a specified waste sizing screen, which for classified data is less than 2mm, making data recovery impossible. The challenge for NSA listed SSD disintegrators is throughput and durability. The smaller the particle, the slower the throughput on any device, including SSD disintegrators. Additionally, whether for paper, optical media, or SSDs, the smaller the screen size on a disintegrator, the more likely the screen is to blind — or clog — resulting in the need for more frequent device maintenance, including knife sharpening and replacement. Understanding the maintenance required on a disintegrator is critical to the longevity and continued productivity of the device. Finally, NSA listed SSD disintegrators are fairly expensive. Due to these reasons, SSD disintegration in an NSA listed disintegrator should be solely utilized for classified and top secret data-bearing SSDs. However, due to challenges associated with incinerators and hammermills, SSD disintegrators are certainly the best option for classified SSD destruction.



Combo shredders feature dual cutting heads and are capable of shredding both HDDs (left) and SSDs (right)

CUI and Non-Classified

Non-classified SSDs are most efficiently and cost-effectively destroyed by either crushing or shredding. Small, anvil-style solid state crushers are ideal for low volume (less than 100 drives per day) of SSDs but may be impractical for smaller solid state devices like thumb drives and compact flash. SEM's cabinet-style SSD crusher employs solid steel, rotational, toothed blades, making it a more versatile crusher style that is able to accept all types of solid state devices and drives, including IronKeys. Still, crushers — which are the lowest cost option for SSD destruction — tend to be best reserved for lower volume office applications, particularly when noise, dust, and portability are of concern. Also, NIST 800-88 notes that solid state drives and devices should be destroyed by shredding, disintegration, pulverization, or incineration by burning the device in a licensed incinerator. Therefore, CUI information should not be destroyed by crushing but rather by shredding or disintegration. Incineration should only be used in extreme circumstances due to its negative effect on the environment.

For medium and high-volume destruction of solid state devices, from SSDs to cell phones to compact flash to thumb drives, solid state shredders are the recommended solution. They produce final waste particles of 0.375", small enough to ensure that each and every flash storage chip is destroyed. Like their HDD counterparts, SSD shredders come in a variety of throughputs, sizes, and configurations to effectively meet any application. SSD shredders are the fastest, most durable, and most cost-effective solution for CUI and non-classified solid state destruction.

Optical Media

Optical media refers to storage media that is written and read by a laser. Typically flat and circular, the most common types of optical media include Compact Discs (CDs), Digital Video Discs (DVDs), and Blu-ray Discs (BDs). As technology has improved, so has the density of optical media storage, so that BDs store more information than DVDs, which store more information than CDs. Due to the storage density discrepancies among optical media, the NSA has two separate requirements for classified optical media destruction.

Classified

Until November of 2018, the NSA requirement for the destruction of CDs and DVDs was a final particle size of less than 5mm, while BDs could only be destroyed by incineration. The release of the updated EPLs in November of 2018 noted significant changes for optical media destruction.

While the CD destruction mandate remains the same, the new EPL for DVD and now BD destruction mandates that DVDs and BDs be physically destroyed to a particle size of less than 2mm. Typically, all optical media can be destroyed in an NSA listed solid state disintegrator, much like SSDs. However, due to their thin size, optical media can also be destroyed in an optical media shredder. These compact devices have CD/DVD/BD sized feed slots and shred one disc at a time. They are also capable of destroying other small solid state devices like SIM cards and Common Access Cards (CACs). There are a variety of shredder sizes and solutions on the NSA EPL for CD destruction. However, when it comes to DVD and BD destruction to the 2mm NSA particle, the options are very limited. And while NSA listed DVD/BD shredders have significantly less throughput than their disintegrator counterparts, they are also physically smaller and far less expensive, making them the recommended solution for low volume and office applications.

The 2018 NSA EPL mandates that classified DVDs and BDs be destroyed to a particle size of less than 2mm

CUI and Non-Classified

Unlike classified optical media, CUI and non-classified CDs, DVDs, and BDs can be sanitized in any IT disintegrator or non-classified paper shredder. NIST 800-88 specifies that optical mass storage media must be destroyed by pulverizing, cross-cut shredding, or burning. The most cost-effective, efficient, and environmentally-friendly way to destroy CUI and non-classified optical media is through shredding. Burning has significant environmental impact and pulverizing is slower and more costly than shredding. Any non-classified paper shredder or industrial paper shredder is an acceptable means of optical media destruction as long as it creates a cross-cut rather than strip cut particle. Best practices suggest a final particle size of DIN 66399 P-4, but this is not a requirement under NIST 800-88.

Conclusion

While there are countless data security and destruction regulations not only within the United States but also globally, the two that affect nearly all U.S. government entities are NSA and NIST standards. The data destruction mandates set forth by the NSA cover all Intelligence Operations and classified data, while those set forth by NIST cover all CUI data. Clearly, NSA and NIST are the hallmarks of federal data security for classified and CUI data, respectively. Having two mandates regulate nearly all federal information provides a simpler and more streamlined methodology by which to destroy sensitive data and greatly enhances federal data security, ensuring a safer and more secure America.

Security Engineered Machinery Co., Inc.
5 Walkup Drive | Westboro, MA 01581
800.225.9293 | 508.366.1488
contact@semshred.com
www.semshred.com