NIST 800.53
Media Sanitization

WHITE CANYON™
SOFTWARE

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

NIST 800.53 Media Sanitization

Media Sanitization recommendations for US Federal information systems.

NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems. The guidelines in 800.53 were developed in collaboration with industry, government, and academic organizations to decrease vulnerabilities to data threats and risks, “including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks”.

The evolution of media storage and use in organizations has grown exponentially and will continue to be a component of federal information systems. Media storage is low cost, easy to transfer data and is the backbone of most systems. It has many vulnerabilities, as well, which has necessitated recommendations for which sanitization methods to employ and when sanitization should be performed. NIST 800:53 recommends media sanitization prior to:

- Disposal
- Release out of Organizational Control
- Release for Reuse

The recommendation to wipe data prior to disposal is not a new suggestion. NIST has recommended data erasure as part of the disposal process since 2006.

NIST

National Institute of
Standards and Technology

The National Institute for Standards and Technology (NIST) is an organization that creates commercial standards for materials and products. NIST standards are common in many industries and NIST first released standards to address the sanitization of data on media devices in 2006.

An increase concern in security has caused the recommendation of sanitization on devices when they are released from organizational control and reuse. HIPAA and other regulations have made all parties liable when there is a data breach. This has initiated the need for erasure in-house before IT assets are transferred to an ITAD, 3rd party service provider, leasor or other entity.

Even when reusing media within an organization, there is a chance of a data spill or breach. When a computer is reassigned to another employee in the same organization there is a possibility that data on the device remains and is at risk. NIST 800:53 recommends these devices are wiped prior to reassignment.

The stages in the IT asset lifecycle when a device is recommended for wiping is increasing and will continue to be required at different points in an asset's lifespan.

TYPES OF MEDIA DEVICES

The media sanitization recommendation applies to all media, including but not limited to scanners, copiers, printers, notebook computers, workstations, network components, mobile devices, and non-digital media, even if the media is not removable. These devices all store data in some capacity and should be sanitized following the recommendations above.

Portable storage devices (USBs) have been the culprit of many data breaches, ransomware attacks and other hacks. These devices can contain malicious code that can be accidentally or purposely introduced into an organizations internal network. NIST 800:53 recommends scanning these storage devices and wiping them prior to use. This will decrease an organizations vulnerability to a USB-based attack.

METHOD FOR SANITIZATION

Media sanitization techniques include clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction. Organizations should determine their level of sanitization depending on the data's significance and consequence of a data breach. The Federal agencies should still follow NSA standards and policies to control the sanitization of 'classified' information and the National Archives and Records Administration (NARA) policies to control unclassified information. Data software tools, like WipeDrive, perform clearing, purging and cryptographic erasure and provide certificates of destruction for future audits.

IMPLEMENTATION

Each organization should follow their data security and record retention policies when sanitizing media storage. All sanitization efforts should be tracked and documented; this includes the following:

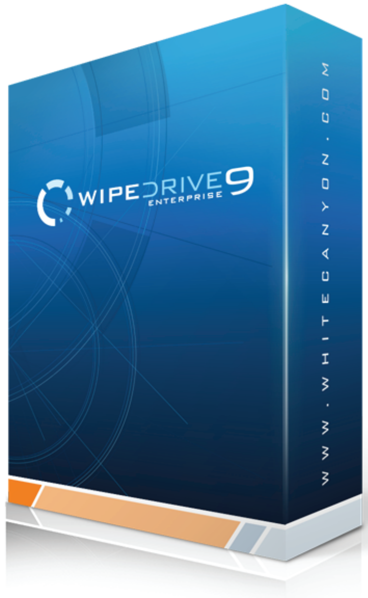
- Listing personnel who reviewed and approved sanitization and disposal actions
- Types of media sanitized
- Files stored on the media
- Sanitization methods used

- Date and time of the sanitization actions
- Personnel who performed the sanitization
- Verification actions taken and personnel who performed the verification
- Disposal actions taken

Personnel that perform that media sanitization should be technically qualified individuals and possess sufficient skills and expertise to determine if the proposed sanitization reflects applicable federal and organizational standards, policies, and procedures. NIST 800:53 recommends that organizations have two individuals perform the wipe to ensure that sanitization occurs as intended, protecting against errors and false claims of having performed the sanitization actions. To reduce the risk of collusion, organizations consider rotating dual authorization duties to other individuals.

Erasure records are vital in the case of litigation or discovering the source of a data breach. It is the organizations responsibility to ensure data is not sanitized prior to when it can be, according to the record retention policies and is securely wiped prior to leaving the facility for disposal.

When implementing remote wiping of information, NIST 800:53 recommends strong authentication to prevent unauthorized individuals from purging or wiping the system, component, or device. Remotely wiped devices should be overwritten, or the encryption key destroyed. The device is then purged and able to leave the facility.



These recommendations made by NIST will ensure your organization sanitizes media correctly and help reduce the vulnerability of a data breach. WipeDrive Enterprise is a proven software-based erasure tool that meets NIST 800:53 requirements when sanitizing your media storage. Request a trial today or contact our Sales Team at 801.224.8900.