The DoD 5220.22-M has long been an industry standard when it comes to data sanitization, but the tide is quickly changing. More and more organizations are seeing the advantages of switching to NIST 800-88 guidelines instead. Most regulatory bodies, including in government, now look to the NIST 800-88 as their standard because of new technology. WhiteCanyon Software recommends using the NIST single pass as standard practice for sanitizing hard drives.

THE ORIGIN OF DOD 3-PASS WIPE STANDARD

The idea that multiple wipe passes are required 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 in order to be rendered irrecoverable. 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. However, considering the pace of advancement in technology in the years since, this criteria is generally considered to be out of date.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 drive technologies are very precise and have eliminated this 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. WipeDrive’s “NIST 800-88r1 purge/clear” wipe pattern removes any device configuration that prevents access to the full drive, including Device Configuration Overlay (DCO), Host Protected Area (HPA), or Accessible Max Address. We use Firmware-based commands to then wipe all sectors of the drive. After the wipe, WipeDrive verifies 10%+ of the media (spanning the entire drive) to ensure that the wipe is successful.

WHY WE RECOMMEND NIST

Our NIST overwrite pattern uses the strongest wiping technique available to remove all data from a device (including DCO, HPA, etc.) to ensure that all sectors of the drive are securely wiped. This is a standard that is not always achieved with DoD 3-pass. DoD 3-pass was designed to address hardware that is no longer in use, whereas NIST 800-88 addresses the new technologies, including SSD, ATA and SCSI drives that are commonly used today.

In most cases a single pass, such as the NIST 800-88 pattern, is sufficient to make any data recovery impossible, even under laboratory conditions. Using multiple passes is time consuming, unnecessary and a drain on your productivity.

CONCLUSION

WhiteCanyon recommends our NIST 800-88 pattern as the best choice for all your data sanitization needs. Our clients have seen the benefits of decreased wipe time, increased efficiency, and better security when switching to the NIST pattern.
Overview

The DoD 5220.22-M has long been an industry standard when it comes to data sanitization, but the tide is quickly changing. More and more organizations are seeing the advantages of switching to NIST 800-88 guidelines instead. Most regulatory bodies, including in government, now look to the NIST 800-88 as their standard because of new technology. WhiteCanyon Software recommends using the NIST single pass as standard practice for sanitizing hard drives.

THE ORIGIN OF DOD 3-PASS WIPE STANDARD

The idea that multiple wipe passes are required 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 in order to be rendered irrecoverable. 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. However, considering the pace of advancement in technology in the years since, this criteria is generally considered to be 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 drive technologies are very precise and have eliminated this 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. WipeDrive’s “NIST 800-88r1 purge/clear” wipe pattern removes any device configuration that prevents access to the full drive, including Device Configuration Overlay (DCO), Host Protected Area (HPA), or Accessible Max Address. We use Firmware-based commands to then wipe all sectors of the drive. After the wipe, WipeDrive verifies 10%+ of the media (spanning the entire drive) to ensure that the wipe is successful.

WHY WE RECOMMEND NIST

Our NIST overwrite pattern uses the strongest wiping technique available to remove all data from a device (including DCO, HPA, etc.) to ensure that all sectors of the drive are securely wiped. This is a standard that is not always achieved with DoD 3-pass. DoD 3-pass was designed to address hardware that is no longer in use, whereas NIST 800-88 addresses the new technologies, including SSD, ATA and SCSI drives that are commonly used today.

In most cases a single pass, such as the NIST 800-88 pattern, is sufficient to make any data recovery impossible, even under laboratory conditions. Using multiple passes is time consuming, unnecessary and a drain on your productivity.

CONCLUSION

WhiteCanyon recommends our NIST 800-88 pattern as the best choice for all your data sanitization needs. Our clients have seen the benefits of decreased wipe time, increased efficiency, and better security when switching to the NIST pattern.
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. WipeDrive’s “NIST 800-88r1 purge/clear” wipe pattern removes any device configuration that prevents access to the full drive, including Device Configuration Overlay (DCO), Host Protected Area (HPA), or Accessible Max Address. We use Firmware-based commands to then wipe all sectors of the drive. After the wipe, WipeDrive verifies 10%+ of the media (spanning the entire drive) to ensure that the wipe is successful.

WHY WE RECOMMEND NIST

Our NIST overwrite pattern uses the strongest wiping technique available to remove all data from a device (including DCO, HPA, etc.) to ensure that all sectors of the drive are securely wiped. This is a standard that is not always achieved with DoD 3-pass. DoD 3-pass was designed to address hardware that is no longer in use, whereas NIST 800-88 addresses the new technologies, including SSD, ATA and SCSI drives that are commonly used today.

In most cases a single pass, such as the NIST 800-88 pattern, is sufficient to make any data recovery impossible, even under laboratory conditions. Using multiple passes is time consuming, unnecessary and a drain on your productivity.

CONCLUSION

WhiteCanyon recommends our NIST 800-88 pattern as the best choice for all your data sanitization needs. Our clients have seen the benefits of decreased wipe time, increased efficiency, and better security when switching to the NIST pattern.