Department of the Army
Pamphlet 25–2–3

Information Management: Army Cybersecurity

Reuse of Army Computer Hard Disk Drives

Headquarters
Department of the Army
Washington, DC
8 April 2019

UNCLASSIFIED

SUMMARY

DA PAM 25–2–3
Reuse of Army Computer Hard Disk Drives

This new Department of the Army pamphlet, dated 8 April 2019—

- Provides Army personnel (military, civilians, and contractors) with specific guidance and procedures for the purging or clearing of Army computer hard disk drives (throughout).

- Addresses the reuse of information technology hard disk drives owned by Army organizations, to include hard disk drive media used in tactical systems (throughout).

Headquarters
Department of the Army
Washington, DC
8 April 2019

Department of the Army Pamphlet 25–2–3

Information Management : Army Cybersecurity

Reuse of Army Computer Hard Disk Drives

By Order of the Secretary of the Army:

MARK A. MILLEY
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army

History. This publication is a new Department of the Army pamphlet.

Summary. This pamphlet implements aspects of AR 25–2 that provide Army personnel and contractors with procedures for the purging or clearing of hard disk drives before reuse.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Proponent and exception authority. The proponent of this pamphlet is the Chief Information Officer/G–6. The proponent has the authority to approve exceptions or waivers to this pamphlet that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency, in the grade of colonel or the civilian equivalent. Activities may request a waiver to this pamphlet by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific guidance.

Suggested improvements. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to the Office of the Chief Information Officer/G–6 (SAIS–PRG), 107 Army Pentagon, Washington, DC 20310–0107.

Distribution. This pamphlet is available in electronic media only and is intended for the Regular Army, the Army National Guard/Army National Guard of the United States, and the U. S. Army Reserve.

Contents (Listed by paragraph and page number)

Contents—Continued

Appendixes

Figure List

Glossary

Chapter 1
Introduction

1–1. Purpose
This publication provides Army personnel and contractors with specific implementation guidance and procedures for the purging or clearing, as appropriate, of hard disk drives (HDDs) before reuse in the same environment or in a different environment, with a different classification level of data, or with a different need-to-know authorization of users or for reuse in the same environment. This pamphlet only addresses HDDs; DA Pam 25–2–8 addresses other types of media.

1–2. References and forms
See appendix A.

1–3. Explanation of abbreviations and terms
See the glossary.

1–4. Applicability
a. The scope of this guidance includes—

(1) HDDs owned by Army organizations (to include media used in tactical systems).

(2) HDDs on loan to the Army for test or evaluation purposes.

b. This guidance does not apply to—

(1) Information technology (IT) equipment items with an embedded National Security Agency (NSA) cryptographic module managed within the communications security (COMSEC) Material Control System or designated as a controlled cryptographic item and accounted for in the unit property book. Sanitize these excepted items following procedures issued by NSA. Sanitization procedures for COMSEC items are device specific and may require return of the entire item, or specific circuit boards to the COMSEC depot via secure means. Consult the COMSEC account manager for specific sanitization instructions.

(2) HDD media used in special access programs, for systems or media used under the purview of the NSA, Defense Intelligence Agency, or other environments where the Army does not have the authority to establish cybersecurity procedures.

(3) DA Pam 25–2–8 covers the other types of media.

Chapter 2
Hard Disk Drive Sanitization and Reuse

2–1. Background
Information systems security managers (ISSMs) will ensure the procedures in this publication are followed for HDD sanitization and reuse. It provides guidance in implementing key aspects of the AR 25–2 policy requirement to “use, mark, and protect authorized removable media in accordance with relevant DOD and Army guidance,” as NIST SP 800–53, Revision 4 requirements. Organization heads, to include commanders and directors, will ensure their appointed ISSMs are implementing this aspect of the organization’s cybersecurity program as they would for any other cybersecurity requirement. The procedures in this chapter are consistent with DODM 5200.01, Volumes 1 through 4, and are based on techniques and procedures defined in NIST SP 800–88, Revision 1. DOD has established the requirement to sanitize HDDs prior to disposal, release from organizational control, or release for reuse in accordance with DODM 5200.01, Volumes 1 through 4, or for reuse with a different need-to-know authorization of users, employing techniques and procedures in accordance with NIST SP 800–88, Revision 1.

2–2. Sanitization and reuse decision
a. The first action is to determine the access sensitivity or security category of the data on the HDD to determine whether the device can be sanitized for reuse and, if the device can be sanitized for reuse, what method is required to perform the procedure correctly (see fig 2–1). Ensure compliance with Army records retention policies before data is eliminated, since purging data without authority is a violation of U.S. law and Army policy. ISSMs will ensure personnel under their purview coordinate with the unit records manager before allowing media to be purged. This is a key step in meeting the security requirement identified in NIST SP 800–53, Revision 4 MP–6.

b. A key decision with respect to HDD sanitization for reuse is whether the HDD is intended for reuse within the organization or if it will be transferred outside of the owning organization's control, either permanently or for a temporary period of time (such as shipment to or from a theater or even a distant exercise location). If the media will not or cannot be reused within the DOD due to damage to the media or for other reasons, the ISSM approved destruction method will be used. The organization ISSM will develop a method that is consistent with the guidance outlined in this pamphlet.

c. The relatively low cost of media does not justify the risk of compromising Army data by allowing HDD storage devices to leave DOD's control where an adversary could obtain it and subject it to an advanced technical exploitation of data. New means of exploiting data remnant on media are continually being developed such that any sanitization method could potentially be compromised if media leaves the control of DOD. Physical destruction may not provide absolute assurance in all cases. However, proper physical destruction of media will provide the highest level of assurance given the feasible alternatives. Therefore, organizational heads, authorizing officials (AOs), and their ISSMs will consider these constraints in their planning and resourcing actions.

d. This pamphlet does not address leased HDDs. Please refer to DA Pam 25–2–8 for these cases and for other types of media. This pamphlet focuses on sanitizing and/or clearing HDDs, their reuse in Army organizations, transfer to other DOD components, or disposal.

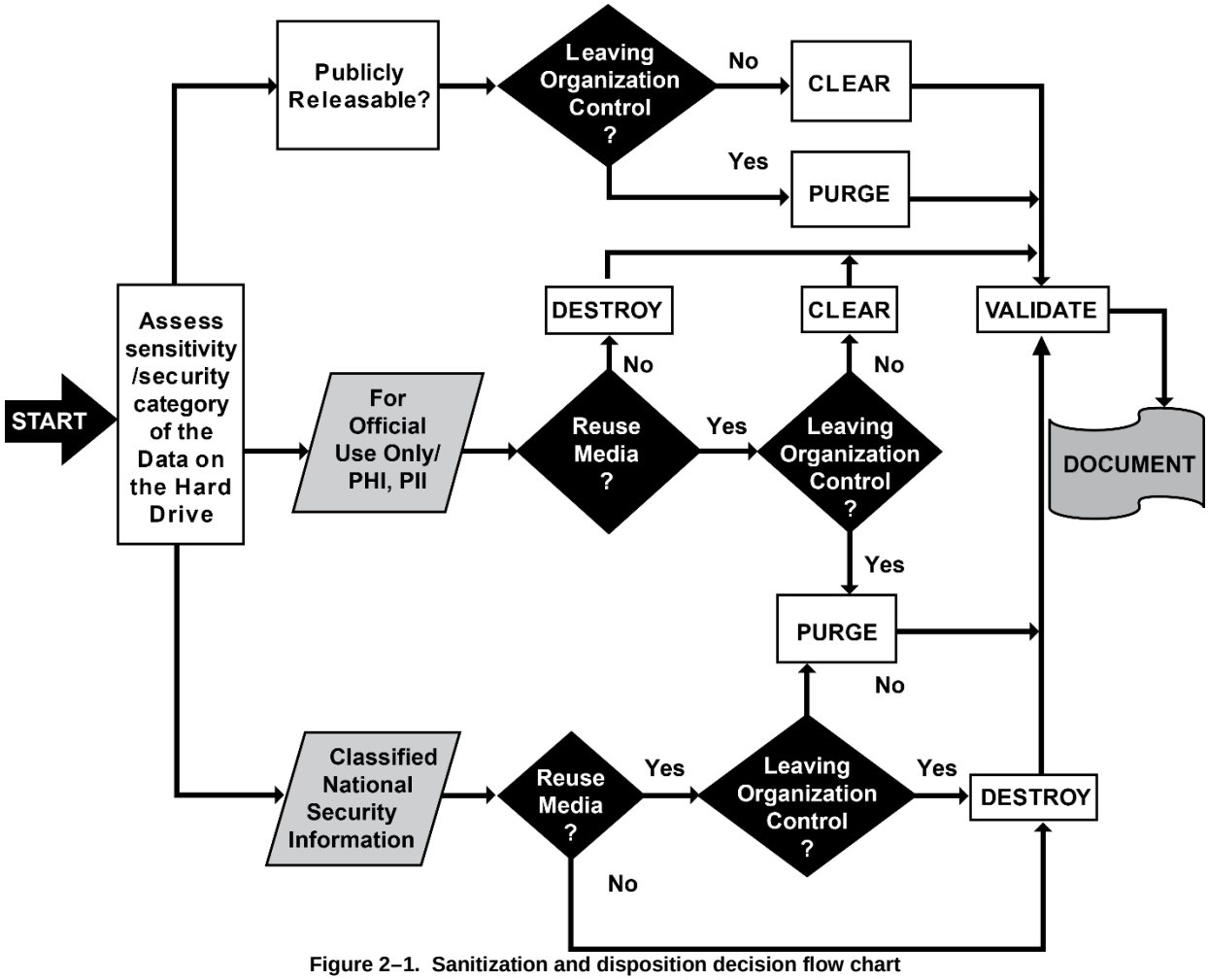

Figure 2–1. Sanitization and disposition decision flow chart

2–3. Sanitization procedures

All Army organizations will sanitize HDDs prior to disposal or reuse in accordance with the following procedures:

a. The information owner, in coordination with the system owner, is responsible for establishing appropriate controls for sanitization and disposal of HDDs. The organizational ISSM is required to know what these controls are for their systems to ensure personnel under their purview implement the established controls.

b. Army organizations will document the sanitization process (as noted below) for all dispositions of HDDs.

c. Certified "sanitized" HDD media will be verified on a random basis by two trained individuals, not including the person who performed the overwrite process. Personnel performing the sanitization will use the verification processes identified in NIST SP 800–88, Revision 1. System owners and project managers will use NIST SP 800–88, Revision 1 and this Army publication to develop their system and site-specific verification procedures. System owners will document these procedures in the system documentation that is made available to users.

d. Sanitize HDDs to ensure information has been removed in a manner that assures the information cannot be recovered. Before the sanitization process begins, disconnect the computer from any network to prevent accidental damage to the network operating system or other files on the network.

e. There are two acceptable methods to sanitize and reuse HDD in the Army:

(1) Purging (overwriting).

(2) Degaussing (see chap 3).

Note. Physical destruction is a sanitization method but is not a sanitization method for reuse since it makes it physically impossible to access data for reusing. Physical destruction is mandatory before disposal if the drive cannot be properly purged or degaussed (see chap 3).

f. The method used for protecting data and disposition of HDDs depends upon whether—

(1) The operable HDD media that will be reused must be overwritten or properly degaussed prior to disposition.

(2) The HDD is inoperable, will not be reused, or has reached the end of its useful life; it must be physically destroyed or degaussed.

g. Overwriting is an approved method for sanitization of HDDs for reuse in most cases. Overwriting of data means replacing data stored on electronic storage media with a predetermined pattern of meaningless information; this effectively renders the data unrecoverable. All software products and applications used for the overwriting process must meet Army requirements for overwriting the data on HDDs and should meet the requirements of CNSSP 11 and FIPS 140–2, when applicable. For example, software used for purging will be signed with a hash or controlled tightly in the supply chain so users of that overwriting software know it is an authentic copy of the overwriting software wiping tool.

(1) The universal purge tool (UPT) is available to Army organizations from Army Materiel Command, Communications–Electronics Command as a government-vetted and provided tool. The UPT was developed to meet the needs of tactical units, and has been tested to meet the criteria for overwrite and reuse of HDD within the Army, provided the procedures outlined in this pamphlet and the user's manual for the UPT are followed. Request the UPT by following the instructions at the UPT on Army Knowledge Online site, https://www.us.army.mil/suite/files/41013884, or use the official version of the UPT from the Program Executive Office Command, Control, and Communications Tactical Mission Command Project Management Office provided with their type accredited tactical systems. In either case, the unit level ISSM who employs the UPT must ensure users of the tool have signed and abide by the UPT Acceptable Use Policy. UPT is controlled and only organizational ISSM approved cybersecurity workforce personnel are allowed to access UPT, including the UPT capability when fielded as part of a type accredited tactical system. If there are any issues obtaining the UPT, users may contact the Software Engineering Command customer service via email at usarmy.apg.cecom.mbx.customer-relationship-management-project@mail.mil.

(2) New HDD storage technologies, such as some implementations of magnetic media interface specification Advanced Technology Attachment (ATA) HDDs, may render existing approved purge tools and the traditional overwriting process ineffective. Army personnel tasked with sanitizing HDD equipment must be technically qualified so that they are capable of properly using the purge tool and capable of understanding not only the capabilities and limitations of the purge tools they use, but the technology employed by the storage device.

(3) Guidance for Army users for ATA HDDs is available. Please note that NIST SP 800–88, Revision 1 provides various options that are not permitted by this guidance; the Army information requires a higher level of assurance. The storage device may not clearly indicate the type of media being used for data storage. Army personnel performing sanitization procedures must accurately determine the media type and then apply the appropriate sanitization procedure; for this reason, ISSMs must ensure personnel performing sanitization procedures are properly trained. For ATA HDDs use one of the following ATA sanitize device feature set commands, if supported, to perform a sanitize operation. One or more of the following options may be used:

(a) The OVERWRITE EXT command. Apply one write pass of a fixed pattern across the media surface. The Army requires the use of three total write passes of a pseudo-random pattern, leveraging the invert option so that the second write pass is the inverted version of the pattern specified.

(b) Use the cryptographic erase (CRYPTO SCRAMBLE EXT) only if the device supports encryption and the technical specifications detailed in NIST SP 800–88, Revision 1. Optionally, after cryptographic erase is successfully applied to a device, use the overwrite command (if supported) to write one pass of zeros or a pseudo-random pattern across the media. If the overwrite command is not supported, the secure erase or the clear procedure will be applied following cryptographic erase. Before cryptographic erase may be used; the following criteria must be met:

1. AO approved risk analysis for use of the technique on each individual piece of equipment where it will be employed.
2. The device must support the technical requirements stated in NIST SP 800–88, Revision 1.
3. The device must be capable of encryption.
4. The personnel performing the task must be properly trained and certified to perform crypto erase.

(c) Use the ATA security feature set SECURE ERASE UNIT command, if supported, in enhanced erase mode. Use the ATA sanitize device feature set commands, unless the ATA security feature set SECURITY ERASE UNIT command is the only option available for a particular HDD. In these cases the ISSM needs to weigh the risk involved.

(d) External HDDs consist of an HDD inside a durable housing, and usually connects to a computer through a universal serial bus or Firewire cable. These may be wiped for the purpose of purging and sanitization, as noted in paragraphs 2–3*g*(3)(*a*) and 2–3*g*(3)(*b*), provided that the entire HDD is wiped by software running off of a live bootable external media operating system with no write-back capability (such as the UPT). If the external drive has any means of swapping or exchanging data with an internal disk of the computer running the wiping software during the wiping process, then the purge and sanitization is rendered ineffective and invalid. The use of a type accredited purpose built system which prevents write-back to the host operating system significantly reduces the risk when purging multiple HDDs simultaneously.

h. Type accredited system AOs will ensure use of overwrite and other sanitization tools is addressed in their type accredited system's Risk Management Framework (RMF) authorization package. Authorization packages should address the capability they use for HDD wiping in the Enterprise Mission Assurance Support Service (eMASS). NIST SP 800–53, Revision 4 MP–6, along with its associated sub-controls (1) through (3) are applicable to media sanitization and purging practices.

2–4. Self-encrypting drives

Self-encrypting drives offer the potential of easily and quickly rendering access to any information stored in encrypted form on the drive infeasible by deleting (cryptographic erase) the encryption key. NIST SP 800–88, Revision 1 outlines how cryptographic erase leverages the encryption of target data by enabling sanitization of the target data's encryption key. This leaves only the ciphertext remaining on the media, effectively sanitizing the data by preventing read-access. Army organizations desiring to use cryptographic erase must meet all the conditions outlined in NIST SP 800–88, Revision 1 and must perform a risk analysis that is approved by the AO of the systems involved before employing it. Cryptographic erase is not an acceptable means of sanitization for HDDs that will be transferred outside of DOD control, or that are going to be processed for disposal. NIST SP 800–53, Revision 4; controls identified in CNSSI 1253 as MP–6; along with the associated sub-controls (1) through (3) are addressed by this guidance.

2–5. Declassification and disposal

a. Declassification is an administrative decision/action, based on a consideration of risk by the data owner, whereby the classification of a properly sanitized storage device is downgraded to unclassified. Therefore the AO, in coordination with the data owner, must approve the method employed for declassification of storage devices used with their systems. The risks associated with purge and declassification of media used in a particular system should be included in the risk assessments that are part of system authorization packages (under the RMF process) for systems fielded to using units by program managers so users in the field are provided a clear decision on how HDDs are to be handled for a particular system.

b. System owners will ensure the appropriate actions are executed when disposing of HDDs containing DOD classified and sensitive information. (See NIST SP 800–88, Revision 1.)

c. Army personnel maintain all records in a mixed system of records as if all the records in such a system are subject to Section 552a, Title 5, United States Code (5 USC 552a), known as the Privacy Act of 1974. Therefore, as with other forms of sensitive information, when HDD media is sanitized, all portions of the media containing the sensitive information must be completely sanitized.

2–6. Loaned equipment

a. Sanitize all HDDs before they are returned to the lending organization, such as at the end of a test period. Depending on the sensitivity or classification of the information and the technology employed by the device to store information, the drive unit or the entire device may have to be destroyed.

b. The terms of the loan agreement must stipulate that the Army unit using the HDD has the right to—

(1) Sanitize all information stored on the device.

(2) Destroy the device if classified information has been stored or spilled onto the device while being tested or evaluated, unless the HDD is to be used in the same environment and at the same classification level of the loaning organization.

c. ISSMs will review existing organization level procedures and policies with respect to loaned HDD equipment to make sure they are consistent with this implementation guidance.

2–7. Clearing

a. Clearing is not an authorized method of sanitization for an HDD, but it may be acceptable for reuse in the same environment when the sensitivity level and classification level is the same (for example, when reusing HDDs in a tactical system for a new mission at the same classification level). Implement clearing by applying logical techniques to remove data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques.

b. Clearing is typically applied through the standard read and write commands to the HDD, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported). Clearing data (deleting files) removes information from electronic storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data. However, because the clearing process does not prevent data from being recovered by advanced technical means, its use is limited to those situations where the HDD will be reused within the same owning organization and the person the device is re-issued to will have the same information access privileges. Clearing is not an acceptable method of sanitizing HDDs for end-of-life cycle disposal.

Chapter 3
Degaussing and Physical Destruction for Sanitization

3–1. General

Degaussing and physical destruction are often the most economical means of ensuring Army data is not remnant on HDDs before disposing of them, or before they leave DOD control. If an HDD cannot or will not be reused, then the guidance in this chapter applies. Compliance with this pamphlet meets the disposal requirements of the NIST SP 800–53, Revision 4 MP–6(1) for HDDs.

3–2. Degaussing cautions

a. Degaussing (demagnetizing) is a process that erases the magnetic media (for example, returned to a zero state). Users of this pamphlet must consider that HDDs are seldom useable after degaussing. Employ the degaussing method when the HDD and other electronic storage media are inoperable and will not be used for further service. Only use a degausser selected from the NSA Evaluated Products List. Refer to and apply the NSA Media Destruction Guidance obtained from their site at https://www.nsa.gov.

b. Use extreme care when operating degaussers, since this equipment can cause extreme damage to nearby telephones, monitors, and other electronic equipment. The use of a degausser does not guarantee all data on the HDD will be destroyed. Audit degaussing efforts periodically to detect equipment or procedure failures. There is no guarantee the data on the drives will be sanitized if the degausser is not operating within its manufacturer's specification, if the equipment is used improperly, or is used on the wrong type of media. This means there is a high risk that the procedure will fail and Army data will be at risk for compromise if procedures are improperly performed.

c. Adhere to the following standards and procedures when HDDs and other magnetic storage media are degaussed:

(1) Follow the product manufacturer’s directions carefully. It is essential to determine the appropriate rate of coercivity for degaussing, as many newer drives have coercivity ratings that exceed the capability of old degaussers.

(2) Shielding materials (for example, cabinets and mounting brackets), which may interfere with the degausser’s magnetic field, must be removed from the HDD before degaussing.

(3) Hard disk platters must be in a horizontal position during the degaussing process.

3–3. Physical destruction for sanitization

a. HDDs will be destroyed when they are defective, cannot be economically repaired or purged for reuse, or have outlived their usefulness. As an added security measure, operable HDDs no longer deemed economically viable will be degaussed before destruction. Physical destruction must be accomplished to an extent that precludes any possible further use of the HDD. Guidance for destruction of HDD storage media is as follows:

(1) Personnel performing the destruction of operable HDDs will hold a security clearance equal to or greater than the HDD being destroyed.

(2) Perform destruction at an approved metal destruction facility (that is, smelting, disintegration, or pulverization) or using an NSA-approved device as the preferred solution. Refer to the NSA/Central Security Service (CSS) Evaluated Products List for Hard Drive Destruction Devices at https://www.nsa.gov/resources/everyone/media-destruction/.

(3) For physical destruction/impairment beyond reasonable use, remove the HDD from the chassis or cabinet. Remove any shielding materials, mounting brackets, and cut any electrical connection to the HDD unit. In a suitable facility with individuals wearing appropriate safety equipment, subject the degaussed HDD to physical force (for example, pounding with a sledgehammer or drilling holes in the HDD) that will disfigure, bend, mangle, or otherwise mutilate the HDD so that it cannot be re-inserted into a functioning computer. Sufficient force should be used directly on top of the HDD unit to cause shock or damage to the disk surfaces. In addition, any connectors that interface into the computer must be mangled, bent, or otherwise damaged to the point that the HDD could not be reconnected without significant rework.

(4) The physical destruction techniques employed in paragraph 3–3*a*(3) must generate surface deformations throughout the disk surface in excess of 0.001 inch and preclude reading through a disk head. When bending, bend the disk platters to an internal angle of at least five degrees; an abrupt bend is preferred. When drilling, holes should be drilled through the platters; the drilling should produce holes greater than 0.25 inch. Penetrate the outer tracks and most of the remaining tracks. When cutting, the cuts must penetrate all tracks of the disk surface and may be accomplished by physical or thermal means. When shredding, shred to a chip size less than 1.5 inches. When using thermal destruction techniques, heat to a temperature where the substrate melts (for example, aluminum or titanium alloys) or fractures (for example, glass and ceramics).

(5) The ISSM, after obtaining unit safety officer guidance and with commander or director approval, may permit the process of the application of acid activator Dubais Race A (national stock number (NSN) 8010–181–7171) and stripper Dubais Race B (NSN 9010–181–7170) to a magnetic drum recording surface. Technical acetone (NSN 6810–184–4796) should then be applied to remove residue from the drum surface. The above should be done in a well-ventilated area and personnel must wear eye protection.

Note. Extreme caution must be observed when handling acid solutions as they are extremely caustic. The application of chemical substances to remove data should be accomplished only by qualified and approved personnel. Units will ensure the local safety officer approves the use of this procedure in their unit.

(6) Affix a signed label to the computer indicating the date of removal of all drives and to certify destruction of the HDDs. See figure 4–1.

(7) The certifier will maintain a separate document recording the same information of a minimum of 5 years. See figure 4–1.

(8) NSA/CSS Policy Manual 9–12 provides media sanitization guidance, to include approved products lists and techniques for sanitizing HDDs. The methods prescribed in this NSA guidance for sanitization of HDDs results in destruction such that the device cannot be reused. When implementing the procedure described in this paragraph, unit level personnel will review the NSA guidance and the instructions that are provided with the degaussers. Refer to https://www.nsa.gov. NSA guidance does not address sanitization for release or reuse of information system storage devices, such as HDDs. Additionally, U. S. Army Cyber Command (ARCYBER) operations orders and directives will be reviewed for applicability when applying this guidance, such as the ARCYBER Operations Order 2017–009.

b. When destroying media, ISSMs executing their responsibilities must consider the safety of personnel and security. NSA-approved destruction devices provide the safest and most secure means of physical destruction. Therefore, the preferred method of destruction is through the use of NSA-approved devices and guidance for use of those devices when going through the steps outlined in this paragraph.

c. Careful consideration and diligent application of destruction procedures for HDDs are required to ensure a low risk that data is recoverable after destruction and to ensure personnel safety and protection of the environment. HDDs that will be disposed of must comply with local policy for proper disposition of hazardous waste from IT products, as well as local command safety and operations security regulations. Units will incorporate or cite the procedures in this pamphlet into their emergency destruction and contingency plans and obtain their commander or director's approval for these local procedures as appropriate.

Chapter 4
Mandatory Certification and Disposition

4–1. Accountability
The procedures in this chapter are mandatory. Proper certification of HDD disposition is required for all Army HDDs. Failure to control and properly account for media has resulted in issues that introduced unnecessary high risk to Army operations in the past. The procedures in this chapter address NIST SP 800–53, Revision 4 MP–6(1).

4–2. Certification of sanitization
a. Army components must maintain documentation of all sanitization procedures. DA Form 7770 (Certificate of Sanitization) is required for each sanitization action. ISSMs will document sanitization procedures, upload the procedures for systems under their purview to eMASS, and retain completed DA Form 7770s for 5 years as part of the unit's records; the form shall be completed in accordance with the publication for sanitization of media.

b. Affix a locally produced and signed "Certificate of Hard Drive Disposition" label (see figure 4–1) to the electronic storage media, computer housing, or other appropriate surface. The label should contain the required information indicated in figure 4–1. ISSMs will also maintain a file of "Certificates of Hard Drive Disposition" for all media under their purview. The Certificate of Hard Drive Disposition or a local major command approved form with all the required information, such as DLA Form 2500 (Certification of Hard Drive Disposition), must be maintained for 5 years from date of sanitization and validation. If the local major command requires the use of another authoritative form, such as the Defense Logistics Agency (DLA) prescribing use of their DLA Form 2500, that form may be used as long as the required information is captured on the form. The unit procedures outlining how the form is to be used must still be documented and the form must be treated as an official record that is maintained and available for inspection for 5 years. Again, the HDD disposition forms and records should not contain classified information.

c. The organization ISSM is responsible for making sure that the label is consistent with Army marking policy for sensitive items, to include the policy outlined in AR 380–5 and related DOD implementation guidance.

Note. If an HDD is destroyed, it obviously cannot be labeled; nevertheless, a formal record of destruction will be created and maintained for 5 years by the organization ISSM. The record will contain the information outlined in paragraph 4-1b of this pamphlet. The Certification of Sanitization that is found in NIST SP 800–88, Revision 1 may be also used to maintain a disposition record of sanitization/destruction.

4–3. Disposition
a. For disposition outside the custody of the Army components and DOD, affix an adhesive label to the HDD case to record the sanitization process before transfer. The Certificate of Hard Drive Disposition should not contain classified information or details except in special circumstances where a program ISSM, with commander or director approval, sets up special procedures because of a mission need to capture classified information on disposition records. This must be well thought out and should be a rare exception to the rule.

Certificate of Hard Drive Disposition

This certifies Hard Drive
Serial Number: [serial number printed on the drive]
Make and Model: [make and model printed on the drive]
was purged for reuse in accordance with Army implementation guidance and system or site level guidance of all [classification] data on [date].
The purge was performed using:
[Tool manufacturer, product name, version]
This drive can now be handled as [classification] media. Electronic media ever used in a classified environment can never be released outside of DOD and will be destroyed at the end of their usefulness.
The Certification of Sanitization for this item is on file with

[Printed Name, Position Title (example: ISSM 2nd BDE, 1st INF),
Office Symbol, and telephone number]

Signature [of person performing the procedure] [Date]

Note. This form is to be locally produced or produced by the system owner or by the project management office so as to fit the item being processed for re-use or disposal and is in addition to proper media markings and labels as outlined in AR 380-5. Because there are so many types, sizes, and shapes of media used in Army systems, it is not possible to design a universal label, however, the key information noted here is what is essential. Also note that a destroyed HHD needs to be properly recorded and verified in a log which the ISSM ensures is maintained for 5 years.

Figure 4–1. Certificate of Hard Drive Disposition

b. These sanitization procedures, when used in conjunction with an HDD that is to be sent in for maintenance, meet the NIST SP 800–53, Revision 4 MA–2 requirement for sanitizing equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs. ISSMs are required to address the system-specific application of these procedures in their unit procedures. Do this by referencing this pamphlet and then adding concise statements in user security manuals or user standing operating procedures. Program managers for programs of record, that is systems delivered and sustained as part of an Army acquisition effort, will address these procedures in their system user security manuals/user security procedures provided to the using units with their system.

4–4. Training

a. Train personnel selected to sanitize or destroy HDD media on the proper use of available software applications and hardware equipment. Such training may be available through software and hardware vendors. ISSMs must ensure—

(1) Personnel performing sanitization or destruction procedures are properly trained and certified.

(2) Training records are captured in the Army Training and Certification Tracking System (ATCTS). The minimum acceptable level of training and certification are a Technical Level II DOD baseline certification and a computing environment training certificate on the tool, device, or operating that will be used to perform the operation. Record this training on an on-the-job training (OJT) record or as a certificate that is uploaded to ATCTS by the organization ISSM. Units can use the checklist in paragraph 4–5*b* as a way to record that the person was trained in the proper procedures.

b. ISSMs must review the training and ensure their people are properly trained, screened (that is have the proper security clearance), and are certified consistent with AR 25–2, DODD 8140.01, and associated implementation guidance before they are permitted to perform the procedures in this pamphlet, deployment to the field, or forward deployed environment.

c. In particular, the ISSM records in an employee's OJT record verification that they can properly perform the tasks outlined in this pamphlet; the checklist in paragraph 4–5*b* may be used for the OJT certificate. The level of supervision, at a minimum, must include observing the person doing the procedures in this pamphlet to standard and then documenting performance on their OJT record with periodic follow-ups to check on their work. If this level of training is not possible

given emergency field conditions, the senior commander or civilian director equivalent on the ground may authorize those variations necessary to protect Army information and ensure personnel safety. This risk decision should be documented in a memorandum for record and be reviewed by the next higher command headquarters as soon as time permits.

4–5. Purging checklist

a. Units will use the checklist in paragraph 4–5*b* to ensure steps are not overlooked in the purging process. Storage media will be physically controlled and safeguarded in the manner prescribed for the most sensitive designation, or the highest classification level, and category of data ever recorded on the media until purged (and declassified), degaussed, or destroyed using approved procedures.

b. Purging is the process of removing the data from the media before reusing the media in an environment that does not provide an acceptable level of protection for the data that was on the media before purging. Purging is not synonymous with declassification. Declassification is the separate administrative process resulting in a determination that given media no longer requires protection as classified information. Declassification is required after purging prior to reuse at a lower classification level. Units may use the following steps to make locally reproducible forms as needed. Personnel performing this procedure will contact their ISSM to make sure they meet local guidance and any additional steps required by local conditions, laws, regulations, procedures, or policy:

(1) Determine if the HDD needs to be cleared, purged, degaussed, or destroyed.

(2) Disconnect the computer from the network.

(3) Using one of the Army's approved purge tools, purge the HDD. Complete the purge in accordance with the published instruction provided by the manufacturer. The software must be set to perform a minimum of three cycles of data patterns on all sectors, to include bad sectors, blocks, tracks, and slack or unused disk space on the entire HDD medium.

(4) Verify all data has been removed from the entire HDD by printing the report generated by the purge tool and view purge pattern.

(5) Complete and affix a signed label verifying that the drive has been purged to the HDD and external housing (see fig 4–1).

(6) Complete and file separately a document recording the purge information for a minimum of 5 years (see para 4–2*b*).

(7) Have a trained person, other than the person who performed the purge, randomly verify the purge process has been successfully completed. Complete the declassification paperwork, as appropriate (see para 4–3).

(8) Notify and provide the proper paperwork to security personnel (see para 4–1).

(9) Notify and provide the proper paperwork to the property book officer.

Note. If this checklist is used as an OJT form, then add initials of the qualified testing officer/manager/administrator in each step and add the statement, "I [name of person administering the hands on test] verify that [name of person being tested] successfully demonstrated to me their ability to perform the procedures above on [date]".

Appendix A

References

Section I

Required Publications

The following publications are available on the Army Publishing Directorate website (https://armypubs.army.mil) unless otherwise stated. DOD publications are available at the Office of the Secretary of Defense website (http://www.esd.whs.mil/dd/).

AR 25–2
Army Cybersecurity (Cited on *title page.*)

AR 380–5
Department of the Army Information Security Program (Cited in para 4–2*c*.)

DODD 8140.01
Cyberspace Workforce Management (Cited in para 4–4*b*.)

NIST SP 800–53, Revision 4
Security and Privacy Controls for Federal Information Systems and Organizations (Cited in para 2–1.) (Available at https://csrc.nist.gov/publications/sp.)

NIST SP 800–88, Revision 1
Guidelines for Media Sanitization (Cited in para 2–1.) (Available at https://csrc.nist.gov/publications/sp.)

NSA/CSS Policy Manual 9–12
NSA/CSS Storage Device Declassification Manual (Cited in para 3–3*a*(8).) (Available at https://www.nsa.gov/resources/everyone/media-destruction/.)

Section II

Related Publications

A related publication is a source of additional information. The user does not have to read it to understand this publication. Unless otherwise indicated, Department of the Army publications are available on the Army Publishing Directorate website (https://armypubs.army.mil). DOD publications are available at the Office of the Secretary of Defense website (http://www.esd.whs.mil/dd/).

AR 25–1
Army Information Technology

AR 25–30
Army Publishing Program

CNSSI 1253
Security Categorization and Control Selection for National Security Systems (Available at https://www.cnss.gov/cnss/issuances/instructions.cfm.)

CNSSI 4009
Committee on National Security Systems (CNSS) Glossary (Available at https://www.cnss.gov/cnss/issuances/instructions.cfm.)

CNSSP 11
Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products (Available at https://www.cnss.gov/cnss/issuances/policies.cfm.)

DA Pam 25–2–8
Cybersecurity: Sanitization of Media

DOD 6025.18–R
DOD Health Information Privacy Regulation

DODD 5400.11
DOD Privacy Program

DODM 5200.01, Volumes 1 through 4
DOD Information Security Program

FIPS 140–2
Security Requirements for Cryptographic Modules (Available at http://csrc.nist.gov/groups/stm/cmvp/standards.html.)

NIST SP 800–53, Revision 4 MA–2
Controlled Maintenance (Available at https://nvd.nist.gov/800–53/rev4/control/ma-2.)

NIST SP 800–53, Revision 4 MP–6
Media Sanitation (Available at https://nvd.nist.gov/800–53/rev4/control/mp-6.)

NIST SP 800–53, Revision 4 MP–6(1)
Review/Approve/Track/Document/Verify (Available at https://nvd.nist.gov/800–53/rev4/control/mp-6.)

NIST SP 800–57 Part 1 Revision 4
Recommendation for Key Management: General (Available at https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-57pt1r4.pdf.)

NIST SP 800–60, Volume 1:
Guide for Mapping Types of Information and Information Systems to Security Categories (Available at https://csrc.nist.gov/publications/sp.)

NSA/CSS Media Destruction Guidance
NSA/CSS Evaluated Product List for Hard Drive Destruction Devices (Available at https://www.nsa.gov/resources/everyone/media-destruction/.)

US Army Cyber Command and ARCYBER Operations Order 2017–009
Removable Media Use Within Army Networks (U//FOUO)

5 USC 552a
Records maintained on individuals (Also known as the Privacy Act of 1974.) (Available at https://www.govinfo.gov/.)

Section III

Prescribed Forms

This section contains no entries.

Section IV

Referenced Forms

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website (https://armypubs.army.mil/).

DA Form 2028
Recommended Changes to Publications and Blank Forms

DA Form 7770
Certificate of Sanitization

DLA Form 2500
Certification of Hard Drive Disposition (Available at http://www.dla.mil/dispositionservices/offers/disposal/turnin/forms.aspx.)

Glossary

Section I

Abbreviations

AO
authorizing official

AR
Army regulation

ARCYBER
U. S. Army Cyber Command

ATA
Advanced Technology Attachment

ATCTS
Army Training and Certification Tracking System

BIOS
basic input/output system

CNSSI
Committee on National Security Systems instruction

CNSSP
Committee on National Security Systems policy

COMSEC
communications security

CSS
Central Security Service

DA Form
Department of the Army form

DLA
Defense Logistics Agency

DOD
Department of Defense

DODD
Department of Defense directive

DODM
Department of Defense manual

eMASS
Enterprise Mission Assurance Support Service

FIPS
Federal Information Processing Standard

HDD
hard disk drive

ISSM
information systems security manager

IT
information technology

MA
maintenance

MP
media protection

NIST SP
National Institute of Standards and Technology Special Publication

NSA
National Security Agency

NSN
national stock number

OJT
on-the-job training

RMF
Risk Management Framework

UPT
universal purge tool

Section II

Terms

Bend
The use of a mechanical process to physically transform storage media to alter its shape and make reading the media difficult or infeasible using state of the art laboratory techniques.

Ciphertext
Data in its encrypted form. See NIST SP 800–57 Part 1 Revision 4.

Clear
A method of sanitization by applying logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques using the same interface available to the user. Typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported). Clearing is typically applied through the standard read and write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported). Clearing data (deleting files) removes information from electronic storage media in a manner that renders it unreadable unless special utility software or techniques are used to recover the cleared data.

Coercivity
For ferromagnetic material the coercivity is the intensity of the applied magnetic field required to reduce the magnetization of that material to zero after the magnetization of the sample has been driven to saturation. Thus, coercivity measures the resistance of a ferromagnetic material to becoming demagnetized.

Cryptographic erase
A method of sanitization in which the Media Encryption Key for the encrypted target data (or the key encryption key) is sanitized, making recovery of the decrypted target data infeasible.

Cut
The use of a tool or physical technique to cause a break in the surface of the electronic storage media, potentially breaking the media into two or more pieces and making it difficult or infeasible to recover the data using state of the art laboratory techniques.

Declassification
An administrative decision/action, based on a consideration of risk by the owner, whereby the classification of a properly sanitized storage device is downgraded to unclassified (see NSA/CSS Policy Manual 9–12). ISSMs must ensure that the system AO has accepted the risk for sanitization methods used for media associated with their systems. AOs should ensure that this publication is referenced as the approved method for sanitization of for their systems in their system RMF packages in eMASS.

Degausser
An electrical device or permanent magnet assembly which generates a coercive magnetic force for the purpose of degaussing magnetic storage devices or other magnetic material.

Degaussing (or Demagnetizing)
Process for reducing the magnetization of a storage device to zero by applying a reverse (coercive) magnetizing force, rendering any previously stored data unreadable and unintelligible, and ensuring that it cannot be recovered by any technology known to exist.

Hard disk drive
An HDD is a hard disk, hard drive, or fixed disk data storage device used for storing and retrieving digital information using one or more rigid ("hard") rapidly rotating disks (platters) coated with magnetic material. The platters are paired with magnetic heads arranged on a moving actuator arm, which read and write data to the platter surfaces. Data is accessed in a random-access manner, meaning that individual blocks of data can be stored or retrieved in any order and not only sequentially. HDDs are a type of non-volatile memory, retaining stored data even when powered off.

Information system storage devices
The physical storage devices used by an information system upon which data is recorded.

Overwriting
A technique that is an approved method for sanitization of electronic storage media and IT equipment. Overwriting of data means replacing previously stored data on electronic storage media with a predetermined pattern of meaningless information. This effectively renders the data unrecoverable. All software products and applications used for the overwriting process must meet the following specifications:
a. The data must be properly overwritten with a pattern, and then its complement, and finally with a random pattern of 1's and 0's (for example, overwrite first with "00110101," followed by "11001010," then "10010111").
b. Sanitization is not complete until all six passes of the three overwrite cycles are verified as completed.
c. The software must have the capability to overwrite the entire HDD, independent of any basic input/output system (BIOS) or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data.
d. The software must have the capability to overwrite using a minimum of three cycles (six passes) of data patterns on all sectors, blocks, tracks, and any unused disk space on the entire hard disk.
e. The software must have a method to verify that all data has been removed.
f. Media sectors that are not overwritten must be identified.

Sanitization
The removal of information from the storage device such that data recovery using any known technique or analysis is prevented. Sanitization includes the removal of data from the storage device, as well as the removal of all labels, markings, and activity logs. The method of sanitization varies depending upon the storage device in question, and may include degaussing, incineration, shredding, grinding, embossing, and so on.