Department of the Army
Pamphlet 25–2–8

Information Management: Army Cybersecurity

Cybersecurity: Sanitization of Media

Headquarters
Department of the Army
Washington, DC
10 April 2019

UNCLASSIFIED

SUMMARY of CHANGE

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

This administrative revision, dated 14 February 2023—

- Changes proponency from CIO/G-6 to Deputy Chief of Staff, G–6 (title page).

This new Department of the Army pamphlet, dated 10 April 2019—

- Provides Army personnel (military, civilians, and contractors) with specific implementation guidance and procedures to ensure proper disposition and sanitization of any item of information technology equipment containing electronic storage media prior to reuse, transfer within Army, or permanent removal from Army custody (chaps 1-5).

- Addresses information technology equipment owned by Army organizations, to include media used in tactical systems, information technology equipment on loan to the Army for test or evaluation purposes, information technology equipment leased by Army organizations, and authorized employee-owned information technology equipment (chap 2).

- Requires that a cost-benefit analysis be performed to determine the most cost-effective sanitization process (para 2–1*c*).

Headquarters
Department of the Army
Washington, DC
10 April 2019

*Department of the Army Pamphlet 25–2–8

Information Management

Cybersecurity: Sanitization of Media

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 an administrative revision. The portions affected by this administrative revision are listed in the summary of change.

Summary. This pamphlet provides implementation guidance for the sanitization and disposal of electronic storage media and information technology equipment except for standard hard drives that are addressed in a separate Department of the Army pamphlet.

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, unless otherwise stated.

Proponent and exception authority. The proponent for this pamphlet is the Deputy Chief of Staff, 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) via email to usarmy.pentagon.hqda-dcs-g-6.mbx.publications-management@army.mil.

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)

UNCLASSIFIED

Contents—Continued

Chapter 1
Introduction

1–1. Purpose

This Department of the Army (DA) pamphlet (DA Pam) provides Army personnel and contractors with specific implementation guidance and procedures to ensure disposition and sanitization of any item of information technology (IT) equipment containing electronic storage media prior to reuse, transfer within Army, or permanent removal from Army custody. This DA Pam does not address the reuse of hard disk drives (HDD) that is covered in separate DA Pam. When IT equipment containing storage media is transferred, becomes obsolete, or is no longer usable or required by an information system, responsible personnel will ensure that residual magnetic, optical, electrical, or other representation of data stored on the device is processed so the information cannot be retrieved and reconstructed, reducing the risk of compromise to Army data.

1–2. References

See appendix A.

1–3. Explanation of abbreviations and terms

See the glossary.

1–4. Applicability

a. The scope of this implementation guidance includes—

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

(2) IT equipment on loan to the Army for test or evaluation purposes (see para 2–5).

(3) IT equipment leased by Army organizations (see para 2–5).

(4) Authorized employee-owned IT equipment.

b. This guidance does not apply to—

(1) 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 your COMSEC account manager for specific sanitization instructions.

(2) 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) Magnetic media interface specification (ATA) hard drives or HDD that are addressed in a DA Pam dedicated to purging and sanitization of this traditional storage media. The Army has made a conscious decision to dedicate a DA Pam to the purge and re-use ATA hard drives because this type of media is more traditional and well understood. Having two DA Pams, one to deal with ATA hard drives, and this DA Pam that deals with all types of media, also keeps the process more readily understood for Army users in the field.

Chapter 2
Media Sanitization and Disposition Decision Process

The procedures in this chapter establish the requirement to sanitize all media prior to disposal, release out of organizational control, or release for reuse in accordance with Department of Defense Manual (DODM) 5200.01 Vol. 1–4 using techniques and procedures in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800–88 (the full citation for this publication is in appendix A of this DA Pam. When media is sanitized, all portions of the media containing DOD information must be completely sanitized. Partial wiping or clearing of media does not meet Army or DOD security standards. Responsible personnel, to include commanders, directors, and information system security managers (ISSM) will ensure the appropriate actions are executed when disposing of IT equipment and electronic storage media containing any DOD information. This responsibility includes making sure that contracts address the requirements and guidance outlined in this DA Pam by working with procurement contracting officers to ensure that sanitization is addressed properly in all contracts involving the use of electronic media. This responsibility also includes compliance with the Army Regulation (AR) 25–400–2, and environmental laws and regulations pertaining to the disposal and handling of hazardous IT waste.

2–1. Sanitization decision

a. The first step is to identify the confidentiality (sensitivity or classification) of the information that has been stored on the information storage media. It is important to remember in this step that only in rare circumstances, is all the information on a particular piece of media publically releasable because the majority of storage devices in individual computers and on unclassified networks will, during their service life, have some form of controlled unclassified information stored on them. This may range from "for official use only" information with protection requirements, to personally identifiable information required to be protected under 5 USC 552a (The Privacy Act), or protected health information that must be protected under Public Law 104–191 (The Health Insurance Portability and Accountability Act). Army personnel must 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 that 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 Special Publication 800–53 Revision 4, MP–6, which covers media sanitization. After this first step, go to figure 2–1, which shows the sanitization and disposition decision flow chart and go through the other steps in subparagraphs *b*, *c*, *d*, and e, below.

b. The next step in the decision process, as shown in figure 2–1, is to determine whether the media is intended for reuse within the organization or transfer outside of the owning organization's control. The transfer could be permanent or temporary (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—consistent with guidance in NSA/Central Security Service (CSS) Policy Manual 9–12—will be used. Procurement contracting officers and commanders will make provisions for this policy in contracts and other agreements.

c. As part of this second step in the decision process, perform a cost-benefit analysis to determine the most cost-effective sanitization process that meets the DOD and Army requirements for protecting DOD and Army information. The cost-benefit analysis will include the cost of labor to sanitize the media, especially with large terabyte media storage devices, to verify that the sanitization process was effective, and the costs in physical labor to examine the media to ensure the process worked correctly. When these costs are included, physical destruction, rather than sanitization is often the most economical and effective approach that properly manages risk. Since the cost benefit analysis and risk assessment for this area requires significant time and resources to complete, the system owner or project manager should develop an analysis to address the standard use case for their site or system and use that as the basis for a site or system level policy for media reuse and disposal for their site or system. System owners and project managers will ensure that user security manuals, standing operating procedures (SOPs) or other guides are readily available to their users so as to provide detailed site and/or system specific procedures that are based on an authorizing official (AO) approved risk decision that is based on a risk assessment. ISSMs will ensure that the guidance in NSA/CSS Policy Manual 9–12, dated 15 December 2014, is appropriately applied when storage media will be transferred outside of Army organizational control, or when media are going to be processed for disposal. Costs involved with local or system specific procedures should also be considered so that the provisions of this guidance are carried out in a cost-effective manner. See the U.S. Army cost benefit analysis guide at https://www.asafm.army.mil/.

d. Given the relatively low cost of media and all the considerations presented above, the economics of the situation usually does not justify the risk of compromising Army data by allowing media 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 remnants on media are continually being developed, such that any sanitization method could potentially be compromised if media leaves DOD control and then is recovered by an adversary, who can then subject it to an exotic advanced laboratory attack. 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 in most cases. Therefore, Army leaders and AOs will consider these constraints in their planning and resourcing actions for their systems. AOs for programs of record and other accredited systems that are fielded to using units will ensure that system-specific procedures for sanitization of media associated with their systems are provided with the systems they field and sustain.

e. The third step is to finally decide on the course of action and to execute the decision using the procedures in paragraph 2–2.

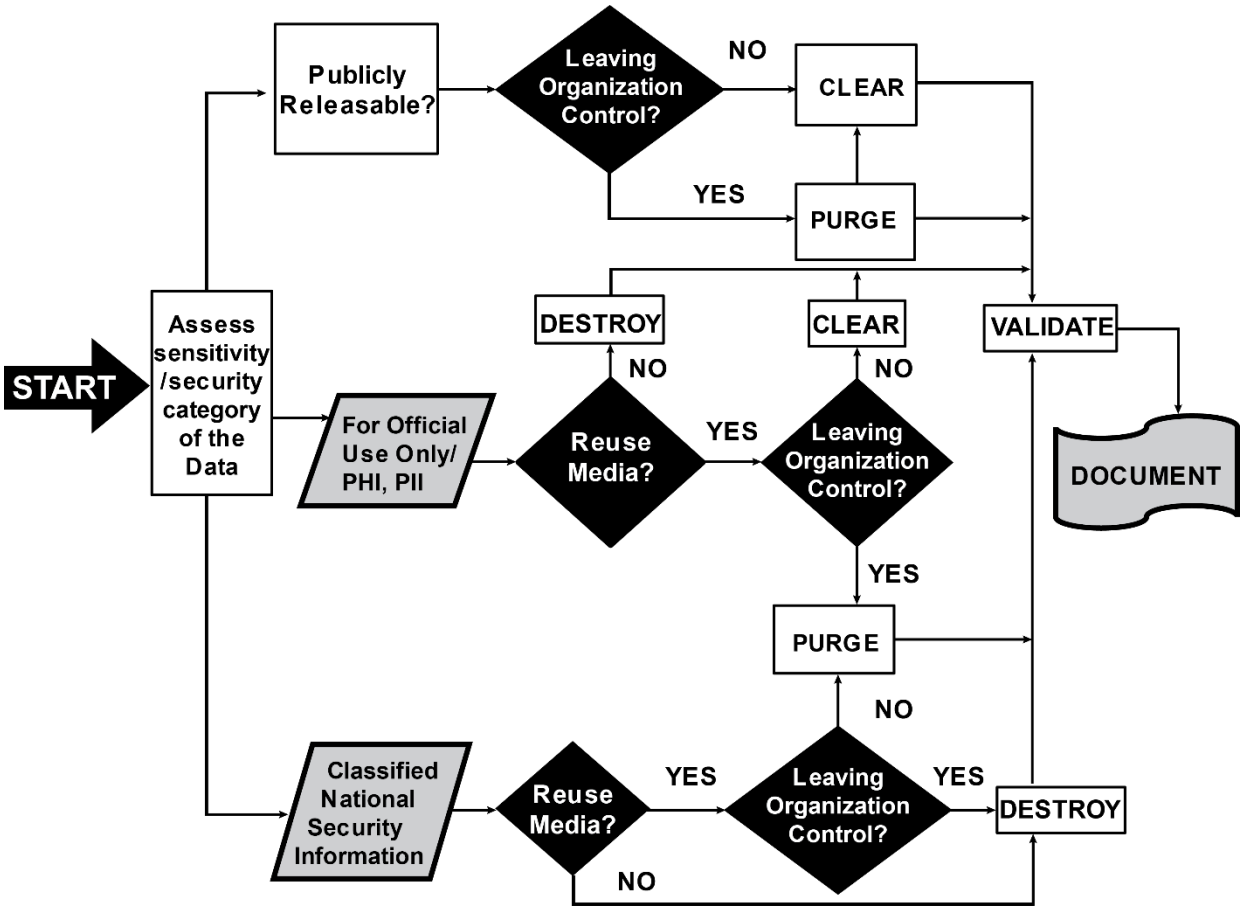

Figure 2–1. Sanitization and disposition decision flow chart

2–2. Procedures

All Army components will sanitize IT equipment and electronic storage media prior to disposal or reuse in accordance with the following procedures—

a. The information owner, in coordination with the system(s) owner(s) involved, is responsible for establishing appropriate controls for disposal. As noted above, system AOs will ensure that system-specific guidance is provided for implementation of controls associated with sanitization of media used with their systems.

b. Army organizations executing these procedures will document the sanitization process (as noted below) for **all** dispositions of electronic storage media and IT equipment.

c. Certified overwritten electronic storage media will be verified on a random basis by two trained individuals, not including the person who performed the overwriting process. Personnel performing the sanitization will use the verification processes identified in NIST SP 800–88. System owners and project managers will use NIST SP 800–88 and this Army guidance to develop their system and site specific verification procedures for their systems and will document these procedures in their system documentation that is made available to users.

d. Sanitize electronic storage media and IT equipment to ensure that information is removed from the electronic storage media 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 for the sanitization of electronic storage media and IT equipment:

(1) Purging (overwriting).

(2) Degaussing (see chap 3).

Note. Physical destruction is a sanitization method but is not a sanitization method for re-use of media since it makes it physically impossible to access data for reusing the storage media. Physical destruction is mandatory before disposal if the electronic media cannot be properly purged or degaussed.

f. The method used for sanitization depends upon the operability of the electronic storage media and IT equipment:

(1) Operable electronic storage media and IT equipment that will be reused must be overwritten prior to disposition. If the operable electronic storage media and IT equipment is to be removed from service completely, it must be physically destroyed or degaussed.

(2) If the electronic storage media and IT equipment is inoperable or has reached the end of its useful life, it must be physically destroyed or degaussed.

g. Clearing is not an authorized method of sanitization in the Army except in very special cases that are approved for certain devices, on a case by case basis, by the AO having authority over the system involved with Army security control assessor concurrence. Clearing is implemented by applying logical techniques to remove data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques. 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. 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 IT device 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 electronic storage media or IT equipment for end of life cycle disposal.

h. Overwriting 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 specifications in Section III of the glossary, in this DA Pam, under the special term "overwriting."

(1) The universal purge tool (UPT) is available to Army organizations from the Army Materiel Command's CECOM Life Cycle Management 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 overwriting and reuse.

(2) Request the UPT by following the instructions on the UPT site on Army Knowledge Online, at https://www.us.army.mil/suite/files/41013884 or use the official version of the UPT provided through the Program Executive Officer (PEO) Command, Control, and Communications Tactical (PEO C3T) Mission Command Project Management Office that is provided with their type accredited tactical systems. UPT is controlled and only organizational ISSM approved cybersecurity workforce personnel are allowed to have access to UPT and this includes the UPT capability when fielded as part of a type accredited tactical system. If you have any issues with UPT please contact the Software Engineering Center (SEC) customer service at email: usarmy.apg.cecom.mbx.customer-relationship-management-project @mail.mil.

i. For SCSI SSSDs, this includes parallel SCSI, serial attached SCSI (SAS), fibre channel, USB attached storage (UAS), and SCSI express. Use one of the following methods:

(1) Apply the SCSI SANITIZE command, if supported. Use the cryptographic erase (CRYPTO SCRAMBLE EXT) only if the device supports encryption and is designed in a manner that is consistent with the technical specifications detailed in NIST SP 800–88. After cryptographic erase is successfully applied to a device, the person performing the sanitization will use the block erase command (if supported) to block erase the media. If the block erase command is not supported, then use the overwriting procedure in paragraph *h*, following the cryptographic erase.

(2) A cryptographic erase through the trusted computing group (TCG), storage work group, Opal security subsystem class (SSC) (TCG Opal SSC), or enterprise security subsystem class (SSC) interface, by issuing commands as necessary to cause all media encryption keys (MEKs) to be changed, may be used provided the following requirements are met:

(a) AO-approved risk analysis for use of the technique on each INDIVIDUAL piece of equipment where it will be employed.

(b) The device must support the technical requirements stated in NIST 800–88.

(c) The device must be capable of encryption.

(d) The personnel performing the task must be properly trained and certified to perform crypto erase.

(e) After cryptographic erase is successfully applied to a device, the block erase command is used (if supported) to block erase the media or if the block erase command is not supported, then the overwriting procedure in noted above is used following the cryptographic erase. Refer to the TCG and vendors shipping TCG Opal or enterprise storage devices for more information.

2–3. Procedures for sanitization of other computer related storage media

Storage media are a rapidly advancing technology and there will always be emerging considerations for special types of media that are not addressed in this implementation guidance.

a. Solid state memory components will be sanitized before disposal or release. Memory components reside on boards, modules, and sub-assemblies. A board can be a module, or may consist of several modules and sub-assemblies.

b. Unlike magnetic media sanitization, clearing may be an acceptable method of sanitizing some types of memory components for release. Personnel performing sanitization should refer to NIST Special Publication 800–88, Revision 1, dated December 2014, and NSA/CSS Policy Manual 9–12, NSA/CSS for the proper procedures for media that are not explicitly addressed in this DA Pam. Memory components are categorized as volatile or nonvolatile, as described below. Sanitization procedures should be followed as specified below:

(1) Volatile memory components do not retain data after removal of all electrical power sources, and when re-inserted into a similarly configured system do not contain residual data (for example, static random access memory and dynamic random access memory).

(2) Nonvolatile memory components do retain data when all power sources are discontinued. Nonvolatile memory components include read only memory, programmable read only memory, or erasable programmable read only memory, and their variants. Memory components that have been programmed at the vendor's commercial manufacturing facility and are considered unalterable in the field may be released. Otherwise, DOD sanitization procedures must be followed.

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 Special Publication 800–88, Revision 1 outlines how cryptographic erase (CE) 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 CE must meet all the conditions outlined in NIST SP 800–88. The risk analysis for Army systems under the risk management framework (RMF) process will address the employment of sanitization for their system's media consistent with NIST Special Publication 800–53, Revision 4, controls identified in Committee on National Security Systems (CNSS) Instruction No. 1253, identified as MP–6, along with the associated sub-controls (1)-(3).

2–5. Leased and loaned equipment

a. Leased equipment. Army organizations frequently enter into contractual arrangements with commercial firms to lease IT hardware. In general, these lease agreements require the Army to return the leased equipment back to the lessor at the end of the lease period. Any computer system, server, printer, copy machine, router, switch, or other multi-functional device that has had sensitive or classified Army information stored on an internal storage device (hard magnetic drive or solid state drive), that storage device must be destroyed before the system is returned to the lessor.

b. Loaned equipment. On occasion, vendors may loan IT equipment to Army organizations for a limited period for test or evaluation purposes, with the understanding that the equipment will be returned at the end of the test period. Sanitize all such equipment before it is returned to the vendor at the end of the 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. The terms of the loan agreement must stipulate that the Army has the right to sanitize all information stored on the device, or to destroy the device if classified information has been stored or spilled onto the device while being tested or evaluated by the Army.

c. Processing and storage. There are occasions when arrangements are made with commercial firms where the processing and storage of Army information is performed on the vendor's hardware in the vendor's facilities. Contract termination clauses must address the sanitization of sensitive or classified Army information from any storage media used by the vendor during the period of the contract.

d. Information system security managers (ISSMs) and contracting officials at all levels will review existing and new IT service and lease agreements to ensure that sanitization requirements are included within the contract.

Chapter 3
Degaussing and Physical Destruction

As noted above, degaussing and physical destruction are often the most economical means of ensuring Army data is not remnant on media before disposing of it or before it leaves DOD control. The procedures in this chapter meet the requirements identified in NIST SP 800–53, version 4, for control DM–2.

3–1. Degaussing cautions

a. Degaussing (demagnetizing) is a process that erases the magnetic media (for example, returned to a zero state). Hard drives and other electronic storage media are seldom useable after degaussing. Employ the degaussing method only when

the hard drive and other electronic storage media are inoperable and will not be used for further service. Use only the NSA degausser evaluated products list; refer to 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 that all data on the hard drive will be destroyed. Degaussing efforts will be audited periodically to detect equipment or procedure failures. If the degausser is not operating within its manufacturer's specification, there is guarantee significant risk that the data on the drives will not be sanitized. It the equipment is used improperly or on the wrong type of media there is a high risk that the procedure will fail and that Army data will be at risk for compromise.

c. Adhere to the following standards and procedures when hard drives 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. Special care will be taken to make sure the degausser actually works on the type of media involved. In the past there have been incidents caused by using a degausser for sanitizing media that the degausser was incapable of removing data from the device such as an optical disk.

(2) Shielding materials (cabinets, mounting brackets), which may interfere with the degausser's magnetic field, must be removed from the hard drive before degaussing.

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

3–2. Physical destruction

a. The NSA provides media destruction guidance on their online site at https://www.nsa.gov/resources/everyone/media-destruction/. The NSA/CSS Policy Manual 9–12, dated 15 December 2014, provides guidance for sanitization of information system (IS) storage. When destroying media, commanders and civilian directors 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. The use of other appropriate or alternate means is permissible when an NSA-approved destruction device is not available because of extenuating circumstances, such as for forward deployed units when procuring or providing the proper environment or power source for these types of devices is not possible. However, other appropriate or alternative solutions require a field commander's or civilian equivalent's proper risk assessment and explicit approval based on the method being consistent with NIST Special Publication 800–88 or AR 380–5. Refer to https://www.nsa.gov for more information. See DA Pam 25–2–3 for additional information about hard drive types of devices that are not covered in this DA Pam.

b. The destruction procedure for floppy disks, tapes, CDs, DVDs, optical disks, and other forms of expendable media is to use in order of preference NSA-approved devices and procedures, NIST Special Publication 800–88, or to use procedures in AR 380–5 if and when they apply to a specific type of media. In the Army, units follow NSA recommendations to use an NSA/CSS-evaluated optical storage device shredder, or disintegrator, so as to reduce CD and DVD storage devices into particles that have nominal edge dimensions of 5 millimeters or less and a surface area of 25 square millimeters or less whenever feasible. Solid state memory components (for example SD cards) will be disintegrated into particles that are nominally 2 millimeter edge length in size using an NSA/CSS-evaluated high security disintegrator whenever feasible. AOs are solely responsible for determining when these procedures are not feasible for systems and sites under their purview and in those cases where procedures in this DA Pam are determined by the AO to not be feasible for systems under their purview that they field or support, the AO will make sure the alternative solution is covered in their site and/or system type accreditation packages along with a risk assessment that shows the alternate means they approve manages the risk to an acceptable level. For details refer to NSA's storage device sanitization site at https://www.nsa.gov/resources/everyone/media-destruction/. Use of other appropriate/alternate means are permissible in a situation which requires the emergency destruction. In either situation, forward deployed unit or emergency destruction, alternative solutions require proper risk assessment and explicit approval by the commanding officer or civilian equivalent. At a minimum, the method of destruction must meet in principle the basic requirements outlined above such that an adversary is not likely to be able to reconstruct the data and use it against Friendly Forces. Army system owners and site commanders are required develop emergency destruction procedures to address this requirement as part of their system and site accreditation packages.

Chapter 4
Final Disposition of Media

Proper certification of sanitization and/or destruction is required for all Army storage media. Failure to control and properly account for media has resulted in issues that introduced unnecessary risk to Army operations in the past. Therefore, the

procedures in this section are mandatory. The implementation of procedures in this chapter meet the requirements of NIST SP 800–53 controls, MA–2(d), and MP–6(1).

4–1. Certification of sanitization

a. Army Components must maintain documentation of all sanitization procedures, using DA Form 7770 (Certificate of Sanitization). The use of the certification of sanitization that is found in NIST SP 800–88 may be also used to maintain a disposition record of sanitization or destruction. ISSMs will ensure that sanitization procedures are documented in their system's procedures, uploaded to Enterprise Mission Assurance Support Service (eMASS), and will retain completed certifications of sanitization for 5 years. The names of the persons involved in the sanitization or destruction action must be recorded in accordance with this paragraph. *Items marked with an asterisk are mandatory entries on the form.

b. When fully completed, the certificate should record at least the following details:

(1) Manufacturer.*
(2) Model.*
(3) Serial number.*
(4) Organizationally assigned media or property number (if applicable).
(5) Media type (magnetic, flash, hybrid, and so forth).*
(6) Media source (user or computer the media came from).*
(7) Pre-sanitization confidentiality level.*
(8) Sanitization description (clear, purge, damage, destroy).*
(9) Method used (degauss, overwriting, block erase, crypto erase, and so forth).*
(10) Tool used (including version).*
(11) Verification method (full, quick sampling, and so forth).*
(12) Post-sanitization confidentiality level.*
(13) If known, post-sanitization destination.

c. For both sanitization and validation:*

(1) Name of person.*
(2) Position or title of person.*
(3) Date.*
(4) Location.*
(5) Phone or other contact information.*
(6) Signature.*

d. Optionally, an organization may choose to record the information in an AO-approved database, provided that the system can authoritatively prove who created the record, audit entries into the record, provide for ongoing independent review of the records for correctness and completeness, retain records for 5 years, and the data is backed up daily to an alternate location. The records for purge or destruction must provide a method to hold users accountable for their purge or destruction actions, such as digital signatures using approved DOD mechanisms on the forms or records.

e. Affix a locally produced and signed "certificate of media disposition" label (see fig 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 of this document, and will include a reference to where the media record is stored in the organization, along with a the device serial number recorded on DA Form 7770. ISSMs will maintain a file of certificate media disposition forms, DA Form 7770**,** for all media under their purview and the records will be maintained for 5 years. 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 DL2500, 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.

Certificate of Media Disposition (Example)*

This certifies this [type of media, e.g. hard drive],

Serial Number: [serial number printed on drive],

Make and Model: [make and model printed on drive],

Was purged 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 media can now be handled as [classification, e.g. Unclassified, FOUO, Classified SECRET] media.

Electronic media that was ever used in a classified environment can *never* be released outside of DoD and will be destroyed at the end of their usefulness.

The Certificate of Sanitization for this item is on file with:

[Printed name, position title, Office symbol, telephone number of certificate holder]

[Printed name, position title, Office symbol, telephone number of certificate holder]

Signature of [Person performing purge procedure] on [date].

* Note that this label is to be locally produced or produced by the system owner or by the project management office and is in addition to proper media markings 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.

Figure 4–1. Example of a certificate of media disposition

4–2. Defense Reutilization Marketing Office

The DRMO requires that a copy of the proof of sanitization accompany all hard drives earmarked for disposal. This proof may be a copy of the entire "certificate of sanitization" form. In instances where attaching the paper form to the equipment is not suitable, a label containing the required information may be affixed to the hard drive(s), equipment case (for example, a central processing unit box), or appropriate surface. The label must contain the name and signature of the person performing the sanitization, equipment identification, and sanitization method used. Equipment serial and inventory numbers must match those on the unit inventory.

4–3. Disposition

a. For disposition outside the custody of the Army Components and DOD, an adhesive label must be affixed to the equipment case to record the sanitization process before transfer. For any remaining questions about leased equipment and equipment maintained through a service agreement, contact your ISSM.

b. These sanitization procedures – when used in conjunction with equipment that is to be sent in for maintenance – address the NIST SP 800–53 controlled maintenance requirement MA–2(d) for sanitizing equipment, to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs. ISSMs

must make sure that the system-specific application of these procedures is addressed in their system RMF packages in eMASS. Do this by referencing this DA Pam and then adding concise statements in their users' security manuals, or users' standing operating procedures, that are uploaded to eMASS and that relate to how these procedures are applied for their system.

Chapter 5
Training

5–1. Individual training standard and records

Army personnel tasked with sanitizing IT equipment must be technically qualified so that they are capable of properly using the purge tool and of understanding the capabilities and limitations of the purge tools they use as well as the specific technology employed by the storage device being purged. Unit level ISSOs will make sure this training is properly documented in the training records of persons authorized by their organization's commander, or in civilian organizations their director, to perform the tasks in this DA Pam. Completion of relevant training will be included in the training record in ATCTS for all personnel involved in sanitization operations. Organization ISSMs must review the training and ensure that their people are properly trained and screened, that is, ensure they have the proper security clearance, and are certified consistent with AR 25–2, and DODD 8140.01, using the associated implementation guidance for these directives and regulations. This includes ensuring that the person doing the work has a baseline certification or meets the military occupational specialty (MOS) requirements of 25B, 25U, or other cyber workforce related MOS, provided they are supervised by a fully qualified ISSM and their organization ISSM records in their on-the-job training record as having been verified that they can properly perform the tasks outlined in this DA Pam to the Army and unit standard. The checklist outlined in paragraph 5–3, below may be used to create an on-the-job training form.

5–2. Site- and system-specific procedures

The implementation guidelines in this DA Pam, or any other enterprise level document, cannot cover all the detailed system- and site-specific, low-level, step-by-step procedures needed to do the work of sanitization for the full range of electronic storage media used in the Army today. This is because the number of tools available, types of media, and systems involved in sanitization ranges into the thousands of variations. For this reason, system owners and site commanders and directors will develop user security manuals (USMs) or SOPs using the guidance in this DA Pam to cover their particular sites and systems. For example, the universal purge tool (UPT) noted above has a USM to cover cases where the unit or organization decides to use that tool.

5–3. Sanitization checklist

a. Units will use the checklist below to ensure steps are not overlooked in the process. Storage media must 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 that 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.

c. Units may use the steps below 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 electronic storage media needs to be cleared, purged, degaussed, or destroyed.

(2) Disconnect the computer from the network.

(3) Using one of the Army's or NSA's approved purge tools, purge the electronic storage media. Complete the purge in accordance with the published instruction provided by the manufacturer and the procedures outlined in this DA Pam. For example, if the UPT is used, then the user's security manual provided by CECOM SEC will be used to perform the step by step procedures.

(4) Verify that all data has been removed from the entire electronic storage media 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 4–1*a*).

(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 your security personnel (see para 4–1).

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

Note: If this checklist is used as an OJT form, then add initials of the qualified testing officer, manager, or 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

AR 25–2
Army Cybersecurity (cited in para 5–1.)

DODD 8140.01
Cyberspace Workforce Management (Cited in para 5–1.) (Available at https://www.esd.whs.mil/.)

NIST Special Publication 800–53, Rev. 4
Security Controls and Assessment Procedures for Federal Information Systems and Organizations: media protection level 6 (MP-6) (Cited in para 2–1*a*.) (Available at http://www.nist.gov/publication-portal.cfm.)

NIST Special Publication 800–60, Vol. 1
Guide for Mapping Types of Information and Information Systems to Security Category (Cited in Glossary under "DOD Information") (Available at http://csrc.nist.gov/publications/nistpubs/800–60-rev1/sp800-60_vol1-rev1.pdf.)

NIST Special Publication 800–88
Guidelines for Media Sanitization (Cited in para 2–3*b*.) (Available at http://www.nist.gov/publication-portal.cfm.)

NSA/CSS Policy Manual 9–12
National Security Agency (NSA)/Central Security service (CSS) Storage Device Sanitization Manual (Cited in para 2–1*c*.) (Available at https://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml.)

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, Army publications are available on the Army Publishing Directorate website (https://armypubs.army.mil); CNSS publications are available on the Committee on National Security Systems website (https://www.cnss.gov); and DOD publications are available on the Defense Department website (https://www.esd.whs.mil).

AR 25–1
Army Information Technology

AR 25–30
Army Publishing Program

AR 25–400–2
The Army Records Information Management System (ARIMS)

CNSS Policy No. 11
National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products, 10 June 2013

CNSSI No. 1253
Security Categorization and Control Selection for National Security Systems

CNSSI No. 4009
Committee on National Security Systems (CNSS) Glossary

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

DODD 5400.11
DOD Health Information Privacy Regulation

DODM 6025.18
Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DOD Health Care Programs

DODM 5200.01 Vol. 1
DOD Information Security Program: Overview, Classification, and Declassification

DODM 5200.01 Vol. 2
DOD Information Security Program: Marking of Classified Information

DODM 5200.01 Vol. 3
DOD Information Security Program: Protection of Classified Information

DODM 5200.01 Vol. 4
DOD Information Security Program: Controlled Unclassified Information (CUI)

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

NSA/CSS Policy Manual 9–12
Storage Device Sanitization Manual (Available at https://www.nsa.gov/.)

PL 104–191
The Health Insurance Portability and Accountability Act (Available at https://www.govinfo.gov/.)

5 USC 552a
Records maintained on individuals

Section III

Prescribed Forms

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

DA Form 7770
Certificate of Sanitization (Prescribed in para 4–1*a*.)

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

Glossary

Section I

Abbreviations

AO
authorizing official

ATA
magnetic media interface specification. Also known as “IDE” – integrated drive electronics

ATCTS
Army Training and Certification Tracking System

CD
compact disc

CE
cryptographic erase

CNSS
Committee on National Security Systems

CNSSI
Committee on National Security Systems instruction

COMSEC
communications security

CSS
Central Security Service

DA
Department of the Army

DLA
Defense Logistics Agency

DOD
Department of Defense

DRMO
Defense Reutilization Marketing Office

eMASS
Enterprise Mission Assurance Support Service

HDD
hard disk drives

IS
information system

ISSM
information system security managers

ISSO
information systems security officer

IT
information technology

MEKs
media encryption keys

MOS
military occupational specialty

NIST
National Institute of Standards and Technology

NSA
National Security Agency

PEO
Program Executive Officer Command

RMF
risk management framework

SAS
serial attached SCSI

SCSI
small computer system interface

SD
secure digital

SEC
Software Engineering Center

SIF
selective identification feature

SOPs
standing operating procedures

SP
special publication

SSC
security subsystem class

SSDs
solid state drives

TCG
trusted computing group

UAS
USB attached storage

UPT
universal purge tool

USB
universal serial bus

USM
user security manual

Section II

Terms

Bend
The use of a mechanical process to physically transform the 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. Source: NIST SP 800–57 Part 1 Rev 3.

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.

Cryptographic erase
A method of sanitization in which the media encryption key (MEK) for the encrypted target data, or the key encryption key (KEK) 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 (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 DA Pam is referenced as the approved method for sanitization of for their systems in their system RMF packages in Enterprise Mission Assurance Support Service (eMass).

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.

DOD information
DODI 8500.01 states that DOD information is any information that has not been cleared for public release in accordance with DODD 5230.09, dated August 22, 2008, and that has been collected, developed, received, transmitted, used, or stored by DOD, or by a non-DOD entity in support of an official DOD activity. DOD information is categorized and classified based on the sensitivity of the information. Refer to the National Institute of Standards and Technology Special Publication 800–60 volume I; and Department of Defense Manual 5200.01, volumes 1 through 4, dated 24 February 2012, incorporating change 2, 19 March 2013. Personally identifiable information and protected health information are forms of DOD sensitive information. Refer to DODD 5400.11, 29 October 2014; and DOD 6025.18–R, 24 January 2003. Policy requires that DOD personnel maintain all records in a mixed system of records as if all the records in such a system are subject to The Privacy Act. For example, an Army hospital has a contract with a firm that provides medical radiological consulting services. X-ray images of military personnel are digitized and transmitted via the internet to a radiology consulting firm that examines the images and provides expert medical advice. These files contain personally identifiable information and protected health information that must be protected. As stated in DODI 8500.01, all DOD information in electronic format will be given an appropriate level of confidentiality, integrity, and availability that reflects the importance of both information sharing and protection.

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

Recycling
End state for IS storage devices processed in such a way as to make them ready for reuse, to adapt them to a new use, or to reclaim constituent materials of value.

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 forth.

Section III

Special Abbreviations and Terms

Burn–In
A tendency for an image that is shown on a display over a long period of time to become permanently fixed on the display. This is sometimes seen in emissive displays such as cathode ray tube and plasma, because chemical changes can occur in the phosphors when exposed repeatedly to the same electrical signals.

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.

Opal Storage Specification
The Opal Storage Specification is a set of specifications for features of data storage devices (such as disk drives) that enhance their security. For example, it defines a way of encrypting the stored data so that an unauthorized person who gains possession of the device cannot see the data. That is, it is a specification for self-encrypting drives (SED). Reference https://trustedcomputinggroup.org/storage-work-group-storage-security-subsystem-class-opal/.

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:
-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, overwriting first with "00110101," followed by "11001010," then "10010111").
-Sanitization is not complete until all six passes of the three overwrite cycles are verified as completed.
-The software must have the capability of overwriting the entire hard disk drive, independent of any BIOS or firmware capacity limitation that the system may have, making it impossible to recover any meaningful data.
-The software must have the capability of overwriting 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.
-The software must have a method to verify that all data has been removed.
-Media sectors that are not overwritten must be identified.

Security Subsystem Class (SSC)
The trusted storage architecture core specification developed in the Storage Work Group provides a comprehensive definition of TCG-related functions for a TCG trusted storage device. However, trusted storage devices use cases may not require all core specification functionality. There are multiple "classes" of core specification compliance called security subsystem classes (SSCs). SSCs explicitly define the minimum acceptable core specification capabilities of a storage device in a specific "class." Reference: http://www.trustedcomputinggroup.org/storage-work-group-storage-security-subsystem-class-enterprise-faqs/

Trusted Computing Group (TCG)
Through open standards and specifications, the Trusted Computing Group (TCG) enables secure computing. Benefits of TCG technologies include protection of business-critical data and systems, secure authentication and strong protection of user identities, and the establishment of strong machine identity and network integrity. Trusted hardware and applications reduce enterprise total cost of ownership and support regulatory compliance. Reference http://www.trustedcomputinggroup.org/about/