



Headquarters
Department of the Army
Washington, DC
18 October 2022

***Army Regulation**
25-400-2
Effective 18 November 2022

Information Management Army Records Management Program

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
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.

Authorities. This regulation implements Title 44, United States Code: outlines the role of public printing and documents in the United States Code; Chapter 31, Records Management by Federal Agencies, Sections 3101-3107; Chapter 33, Disposal of Records, Sections 3301-3314; Chapter 35, Coordination of Federal Information Policy, Sections 3501-3515; DoDI 5015.02; and Public Law 113-187 implements the Presidential and Federal Records Act.

Applicability. This regulation 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. It also applies to Department of the Army Civilians and contractors who perform recordkeeping duties, unless otherwise stated. This regulation applies during partial and full mobilization.

Proponent and exception authority. The proponent of this regulation is the Chief Information Officer. The proponent has the authority to approve exceptions or waivers to this regulation 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 regulation 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 requirements.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11-2 and identifies key internal controls that must be evaluated (see appendix B).

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-cio.mbx.policy-inbox@army.mil.

Distribution. This regulation 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, as well as Army Civilians who perform recordkeeping duties.

*This regulation supersedes AR 25-400-2, dated 2 October 2007 and DA Memorandum 25-51, dated 29 March 2017.

Contents (Listed by chapter and page number)

Chapter 1

Introduction, *page 1*

Chapter 2

Responsibilities, *page 2*

Chapter 3

Record Definitions, *page 5*

Chapter 4

Recordkeeping, *page 7*

Chapter 5

Records Retention, *page 9*

Chapter 6

Disposition of Records, *page 9*

Chapter 7

Wartime and Contingency Operations Records, *page 10*

Appendixes

A. References, *page 11*

B. Internal Control Evaluation, *page 13*

Glossary of Terms

Summary of Change

Chapter 1 Introduction

1–1. Purpose

This regulation ensures the Army Records Management Program is compliant with various elements of Title 36 Code of Federal Regulations (CFR) Chapter XII, Subchapter B and the Federal Records Act (see Title 44, United States Code, Chapters 21–35 (44 USC Chapters 21–35)). Failure to manage records in a compliant manner increases the risk that records will not be readily accessible for normal business operations, for program development, and for accountability to Congress and the public. It also increases the risk of loss of Federal data and records, which raises the possibility that permanent records may not be retained for eventual transfer to the National Archives, as required by 44 USC 3101.

1–2. References, forms, and explanation of abbreviations

See appendix A. The abbreviations, brevity codes, and acronyms (ABCAs) used in this electronic publication are defined when you hover over them. All ABCAs are listed in the ABCA database located at <https://armypubs.army.mil/abca/>.

1–3. Associated publications

Procedures associated with this regulation are found in DA Pam 25–403.

1–4. Responsibilities

See section II of this chapter.

1–5. Records management (recordkeeping) requirements

The records management requirement for all record numbers, associated forms, and reports required by this regulation are addressed in the Records Retention Schedule–Army (RRS–A) and/or new Army Records Disposition Schedule. Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS–A at <https://www.arims.army.mil>. If any record numbers, forms, or reports are not current, addressed, and/or published correctly in ARIMS/RRS–A (see DA Pam 25–403 for guidance).

1–6. Statutory authority

a. The Federal Records Act of 1950, as amended, and codified at 44 USC Chapter 29, 44 USC Chapter 31, and 44 USC Chapter 33, contains the statutory authority for the Army Records Management Program. The Federal Records Act was further amended by Public Law 113–187. The National Archives and Records Administration (NARA) has Government-wide responsibility for Federal recordkeeping, which is implemented through 36 CFR Chapter XII, Subchapter B. These statutes are, in turn, implemented by Army.

b. 44 USC 3301–3314 establishes the legal basis for the disposal of records of the Government. In coordination with Army organizations, the Army Records Management Directorate (ARMD), develops retention and disposal authorizations that meet Army needs and obtains approval from the Archivist of the United States. Approval by the Archivist is the only legal authority for the retention and disposal of all Army records.

c. The criminal penalties for the unlawful, deliberate, or accidental removal, defacing, alteration, or destruction of Federal records or the attempt to do so, may include the following:

- (1) A fine, imprisonment, or both (see 18 USC 641 and 18 USC 2071).
- (2) Removal from office (see 18 USC 2071).
- (3) Disqualification from holding any other office in the Government (see 18 USC 2071).

d. 44 USC Chapter 35 establishes the legal basis for minimizing the cost of creation, collection, maintenance, use, dissemination, and disposition of information.

e. 36 CFR 1220.34(f) provides general training requirements for agency records management training programs. NARA Bulletin 2017–01 supplements general training requirements outlined in 36 CFR 1220.34.

Chapter 2 Responsibilities

2-1. The Secretary of the Army

In accordance with Title 36 Chapter XII, Subchapter B, Code of Federal Regulations, and Title 44, United States Code, the Secretary of the Army will—

- a. Establish, sufficiently resource and maintain an Army Records Management Program.
- b. Appoint a Senior Agency Official for Records Management (SAORM) as identified in the Office of Management and Budget (OMB) NARA M-12-18.

2-2. Headquarters, Department of the Army principal officials, Army commands, Army service component commands, and direct reporting units

HQDA principal officials, ACOMs, ASCCs, and DRUs, in accordance with 36 CFR 1220, will—

- a. Use the most economical, efficient, and reliable means to create, maintain and use, dispose of, and preserve Army records in any media as directed in Office of Management Budget Circular A-130.
- b. Implement records management controls and accountability standards necessary to capture, manage, and preserve Army records, including electronic records and electronic messages and their attachments, using internal controls in accordance with DoDI 5010.40.
- c. Establish an essential records program to identify and preserve essential records (formerly vital records). The essential records program will ensure essential records are maintained, revised and, where appropriate, available after an event that disrupts normal business.
- d. Ensure any information system or electronic collection service developed, acquired, or provided by the Army, that contains records are managed and scheduled. Register the information system or electronic collection or information technology (IT) service in the Army Portfolio Management System and populate and maintain the records management data elements.
- e. Ensure prompt retirement or disposal of temporary records and the timely transfer of permanent records to NARA for preservation under NARA-approved records schedules. Transfer permanent records to NARA in digital or electronic form to the greatest extent possible.
- f. Safeguard all personal data within records, in accordance with DoDI 5400.11. Protect all personal data within health-related records in accordance with DoDI 6025.18.
- g. Ensure requests for removal of non-record materials outside of DoD be reviewed by the proper Army authority. Unclassified documents, including email, are not automatically publicly releasable and must be reviewed for release to departing officials or employees.
- h. Maintain accountability of records when they are loaned and transferred to other DoD Components or federal agencies, and accept possession and management responsibility when loaned records are returned to the Army. Continue lifecycle management of the records in accordance with NARA-approved records disposition schedules.
- i. Issue a records management policy memorandum within their agencies/commands. At a minimum, the policy memorandum will ensure all Department of the Army (DA) military, civilians, contractors, and foreign nationals are aware—
 - (1) There are criminal penalties for the unlawful removal or destruction of Federal records.
 - (2) Of their responsibilities pertaining to the management of records within their organization.
- j. In accordance with NARA Bulletin 2017-01, ensure all personnel with email accounts or IT network resource access, complete Records Management training within 60 days of employment and refresher training, annually. Additionally ensure records management training is provided to command personnel that create, receive, access, or use Army records, regardless of whether those individuals have email accounts or IT network access. The above training requirements apply to any personnel that create, receive, access, or use Army records.
- k. Prepare written contingency plans that include records in accordance with DA Pam 25-1-2.
- l. Ensure records retention and disposition requirements are clear, accurate, essential, current, and contained in the publications of their functional areas.
- m. Close all records holding areas (RHAs) and transition recordkeeping repositories to a fully electronic environment in accordance with OMB Memorandum M-19-21.
- n. Appoint records management officials (RMOs) at each level of command, in writing, and ensure registration in the ARIMS. RMOs within the organization will receive records management training annually, on the Army Learning Management System website (available at <https://www.lms.army.mil/>) and ARIMS

training via ARMD. RMOs (in hierarchical order) are records administrators (RAs), records managers (RMs), RHA managers and records coordinators. See mandatory procedures prescribed in DA Pam 25–403 for the list of duties and responsibilities for RMOs.

2–3. Assistant Secretary of the Army (Acquisition, Logistics and Technology)

The ASA (ALT) will—

- a. Include records management requirements when acquiring new technologies for the Army.
- b. Direct contractors performing DoD program functions to create and maintain records to document these functions. Contracts must specify the delivery to the United States Government of all the data required for adequate documentation of the contractor-operated program in accordance 41 CFR.

2–4. General Counsel

The GC will—

- a. Coordinate legal and policy advice to the Army Records Management Program and determine the DA position on legal questions or procedures related to records management.
- b. Ensure records related to matters involved in administrative or legal proceedings are retained until authorized resumption of normal disposition.

2–5. Chief Information Officer

The CIO, in accordance with 44 USC, will—

- a. Develop and establish Army policy and standards to implement the Army Records Management Program, including the life cycle management of records in all media including the capability to identify, retrieve, and retain records for as long as they are needed.
- b. Develop sound records management principles in Army business processes such as:
 - (1) Identifying and linking records management requirements to their implementing technologies as described in DoD 5015.02–STD.
 - (2) Integrating records management requirements into Army IT governance processes for portfolio management, risk management, capital planning, enterprise architecture, business process design and system development.
- c. Oversee the incorporation of records management and preservation considerations in the acquisition, development, and enhancement of information systems or electronic collection and IT services and the management of these records in accordance with NARA-approved records disposition schedules.
 - (1) For new information systems or electronic collections and IT services, records will be managed electronically by recordkeeping functionality provided by the information system or electronic collection or IT service, or by transferring records to an electronic recordkeeping repository, such as a records management solution that is compliant with DoD 5015.02–STD.
 - (2) For existing information systems or electronic collections and IT services, records will be managed electronically, manually, or a combination of both. To manage records electronically, recordkeeping functionality will be provided by the information system or electronic collection or IT service, or records will be transferred to an electronic recordkeeping repository, such as a records management solution that is compliant with DoD 5015.02–STD.
- d. Develop and issue policy on information systems or electronic collections and IT services where data is shared or transferred to another federal agency such as the Department of Veterans Affairs or NARA. Metadata, standards, or mediation will be used in accordance with DoDI 8320.02.
- e. Develop and issue policy on records management practices for those instances in which the Army is designated the executive agent in multi-agency efforts with records management responsibilities.
- f. Serve as the SAORM.
- g. Appoint the Army records officer in accordance with OMB and NARA M–12–18.
- h. Cultivate an Army records management community of interest by encouraging use of collaborative tools and technologies to distribute and evaluate the best practices and lessons learned in records and information management.

2–6. Director of the Army Staff

The DAS will serve as the principal official for all records management responsibilities necessary to conduct business in the Office of the Chief of Staff of the Army.

2-7. Deputy Chief of Staff, G-6

The DCS, G-6 will—

- a. Incorporate and implement records management requirements throughout the Army.
- b. Support records management requirements by immediately informing CIO when new technologies emerge containing record data.
- c. Include records management in any governance framework boards.
- d. In conjunction with the CIO, develop technical solutions to ensure that electronic records can be located, retrieved, presented, interpreted, and accessioned to NARA when scheduled.

2-8. The Judge Advocate General

On behalf of TJAG, the U.S. Army Legal Services Agency will—

- a. Concur with resuming destruction actions on all records subject to litigation hold and record freeze, as appropriate.
- b. Notify ARMD of the requirement to suspend dispositions. ARMD notifies NARA (as appropriate), HQDA principals officials and RMOs of ACOMs, ASCCs, and DRUs, to suspend regular disposition of the affected records and when a freeze or moratorium is lifted. Each command will notify its subordinate installations and activities to the lowest echelon to impose or remove the records freeze.

2-9. Senior agency official for records management

The SAORM will—

- a. Oversee the Army Records Management Program.
- b. Advise senior leaders of their records management responsibilities within the first 30 days of assumption of duties. Provide out-briefings to senior leaders to ensure capture of the records generated during their tenure.
- c. Ensure the establishment of a records management solution that is compliant with DoD 5015.02-STD to manage unstructured electronic records.
- d. Inform the DoD SAORM of any actual, impending, or threatened unlawful removal, defacing, alteration, corruption, deletion, erasure, or other destruction of permanent or long-term records in the custody of the Army that impacts more than one Component, or attracts interest or scrutiny from other agencies, Congress, or the public.
- e. Advise the DoD SAORM of records management issues that could have broad implication across DoD or between DoD and other government agencies, and fully cooperate with the DoD CIO in resolving these issues.
- f. Work with the DoD SAORM to coordinate responses to existing, new, or changing records management requirements.

2-10. Army records officer

The ARMD, Records Management Division Chief, is the Army records officer. The Army records officer will—

- a. Administer the Army Records Management Program and ensure compliance with DoD standards and guidance.
- b. Provide records management training for the staff responsible for the Army's records management program and operations.
- c. Oversee prompt retirement or disposal of temporary records and the timely transfer of permanent records to NARA for preservation under NARA-approved records schedules. Transfer permanent records to NARA in digital or electronic form to the greatest extent possible.
- d. Notify the Archivist of the United States of any actual, impending, or threatened unlawful removal, defacing, alteration, corruption, deletion, erasure, or other destruction of records in the custody of the Army.
- e. Monitor the Army compliance with the Army Records Management Program and implement corrective actions when necessary.
- f. Oversee requests for removal of non-record materials outside of the Army control be reviewed by the proper Army authority, as designated by the Army. .
- g. Oversee accountability of records when they are loaned and transferred to the other DoD Components or federal agencies, and accept possession and management responsibility when the loaned records are returned to the Army.

h. Complete the NARA Certificate of Federal Records Management Training within 1 year of assuming the position in accordance with OMB and NARA M–12–18.

Chapter 3 Record Definitions

3–1. Records management

a. Records management is the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transaction of the Federal Government and effective and economical management of Army operations.

b. Records management significantly contributes to the smooth operation of the Army's programs by making information readily available when needed for effective decision-making. Additionally, records management—

- (1) Safeguards the rights and interests of the Army and its Soldiers and DA Civilians.
- (2) Protects records from inappropriate and unauthorized access.
- (3) Provides continuity in the event of a disaster.

3–2. Records

a. Army records can be found in all media formats: paper, email, instant messaging, chat and text messages, telephone messages, voice mail messages, presentations, websites, social media, word processing documents, spreadsheets, and information systems. If the information is not a record, then such information would be categorized as either a non-record or personal paper (see paras 3–2 and 3–4).

b. As defined in the Federal Records Act of 1950, as amended, the term "records" includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government, or because of the informational value of data in them.

(1) The term "records" does not include library, archival, and museum material made or acquired and preserved solely for reference or exhibition purposes.

(2) The term "recorded information" includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

c. Determining whether a document is a record does not depend on whether it is an original or a copy. Several copies of a single document may each be a record copy because of the following:

- (1) Each serves a separate administrative purpose.
- (2) Each is maintained separately with other relevant records.

d. A record may be active or inactive.

(1) *Active records.* Active records are necessary to conduct the current business of an office and are used on a daily or monthly basis. Active records are generally maintained in the current file area.

(2) *Inactive records.* Inactive records are no longer used in the day-to-day course of business, but may be preserved and occasionally used for legal, historical, or operational purposes. Inactive records must be identified and filed separately from active records.

e. Records may be temporary or permanent.

(1) *Temporary records (all records other than permanent).* Temporary records may be destroyed after a fixed period of time or after the occurrence of an event in accordance with a NARA-approved schedule. The vast majority of the Army's records are temporary.

(2) *Permanent records.* Permanent records are any Federal record that has been determined by NARA to have sufficient value to warrant its preservation in the National Archives of the United States, even while it remains in Army custody. Permanent records are those for which the disposition is permanent and must never be destroyed. They require special care and handling and must be transferred to NARA's ownership to preserve forever once they are no longer needed for business purposes.

f. Whether a record is temporary or permanent determines what eventually happens to it in the records life cycle (see DA Pam 25–403).

3-3. Non-records

a. Non-records are those Federally-owned materials that do not meet the statutory definition of records or that have been excluded from coverage by the definition. Non-record material has no real evidential or informational value. Excluded materials are extra copies of documents kept only for reference, stocks of publications and processed documents, and library or museum materials intended solely for reference or exhibit. Non-records will be identified and filed separately from records and personal papers (see DA Pam 25-403 for examples).

b. When in doubt, treat the information as a record. More information on non-records can be found in DA Pam 25-403.

3-4. Personal papers

a. Personal papers and/or files are excluded from the definition of Federal records and are not owned by the Government. Personal papers are documentary materials belonging to an individual that are not used to conduct agency business. Personal papers must be filed separately from Army records (see DA Pam 25-403 for examples).

b. Consult with your organization's RMO if there are question as to whether materials are personal or Federal records.

3-5. Essential records

An essential record, also known as a vital record, is an Army record that is needed to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records). The Essential Records Program contains information the Army may need to conduct business under emergency operating conditions or to protect the legal and financial rights of the Federal Government and the people it serves. See DA Pam 25-403 for elaboration on essential records and procedural guidance outlining the entire process for creating an essential records program.

3-6. Unscheduled records

Unscheduled records are Federal records whose final disposition has not been approved by NARA on a SF 115 (Request for Records Disposition Authority). Such records must be treated as permanent until a final disposition is approved. Records not identified or described in the RRS-A should be brought to the attention of the RMO who will assist in obtaining a valid record number (see DA Pam 25-403).

3-7. Contract records

a. The contracting officer representative responsible for administering contracts must safeguard records created, processed, or in the possession of a contractor or a non-Federal entity by taking the following steps: (1) Contractors performing Army functions create and maintain records that document these activities. (2) Contracts must specify in the contract Government ownership and the delivery to the Government of all records necessary for the adequate and proper documentation of contractor-operated Army activities and programs in accordance with the requirements of the Federal Acquisition Regulation. (See Office of Federal Procurement Policy Act of 1974 (Public Law 93-400), as amended by Public Law 96-83 and 41 USC), and, where applicable, the Defense Federal Acquisition Regulation Supplement (see 48 CFR 200-299).

(1) Records management oversight of contract records is necessary to ensure that all recordkeeping needs are met. All records created for Government use and delivered to, or under the legal control of, the Government must be managed in accordance with Federal law. In addition, electronic records and background electronic data specified for delivery to the contracting agency must be accompanied by sufficient technical documentation to permit understanding and use of the records and data.

(2) Contracts that require the creation of data for the Government's use must specify, in addition to the final product, delivery of background supporting data or other records that may have reuse value to the Government. To determine what background supporting data or other records that contractors must deliver, program and contracting officials must consult with Army records officials and historians and, when appropriate, with other Government agencies to ensure that all Government needs are met, especially when the data deliverables support a new agency mission or a new Government program.

(3) Deferred ordering and delivery-of-data clauses and rights-in-data clauses must be included in contracts whenever necessary to ensure adequate and proper documentation or because the data have re-use value to the Government.

b. All data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 USC Chapters 21, 29, 31, and 33, the Freedom of Information Act (see 5 USC 552), as amended, and the Privacy Act of 1974 (see 5 USC 552a), as amended, and must be managed and scheduled for disposition only as provided in 36 CFR, Chapter XII, Subchapter B.

c. Establish the appropriate authority for retention of classified materials has been granted to contractors or non-Government entities participating in the National Industrial Security Program, established under Executive Order 12829, as amended, or a successor order.

3–8. Social media records

Social media refers to the various activities integrating web technology, social interaction, and user-generated content including social networks, photo libraries, and video sharing sites. Social media is used internally and externally to share information, support business processes, and connect people to Government. Social media, when used in the conduct of Army business, may result in the creation of official record information, and managed in compliance with records management laws, regulations, and policies. When social media content is determined to be official record material, RRS–A disposition instructions must be applied, and the records managed throughout their life cycle. Organizations will take necessary actions to capture such content and prevent its unauthorized destruction. If an appropriate retention period has not been designated, the records will be maintained as permanent until a schedule is approved by NARA.

3–9. Unlawful or accidental removal, defacing, alteration, or destruction of records

a. The unlawful or accidental removal, defacing, alteration, or destruction of records must be prevented. Records must not be destroyed except under the provisions of NARA-approved Army records schedules or the general records schedules (GRS) by NARA.

b. All employees and contractors must be informed of the provisions of the law relating to unauthorized destruction, removal, alteration, or defacement of records.

c. Policies and procedures must be implemented and disseminated to ensure that records are protected against unlawful or accidental removal, defacing, alteration, and destruction.

d. Any unauthorized removal, defacing, alteration, or destruction must be reported to NARA. See reporting requirements and procedures in DA Pam 25–403.

3–10. Records inspection

a. In accordance with 44 USC 2904(c)(7) and 44 USC 2906, Army records are subject to inspection to ensure compliance with Federal statutes and regulations; to assess the proper management of Army records in all media; to protect the rights of individuals; to assure Government accountability; and to preserve and make available records of permanent value. (See DA Pam 25–403 for RMOs duties.)

b. ARMD is responsible for conducting formal evaluations to measure the effectiveness of records management programs and practice throughout the Army.

Chapter 4 Recordkeeping

4–1. Overview

Army records, regardless of medium, must follow the disposition instructions identified in the RRS–A for guidance and comply with the security requirements of AR 25–2. Any information generated by or contained in an information system or other IT source created or received during the conduct of business must be preserved according to those instructions. If this requirement has not been met, records are considered unscheduled. Unscheduled records carry a disposition of permanent until the appropriate disposition schedule has been approved by NARA. This includes information contained on Government-owned machines in information systems, command or installation unique systems, email systems, systems maintained in the office environment, shared drives, collaboration tools, websites, instant messaging, texting,

and social media sites. Unscheduled records should not be transferred to a Federal Records Center (FRC). The procedures for saving electronic records should be determined as early as possible in the life cycle of a system.

4-2. Office of Management Budget/National Archives and Records Administration Memorandum M-19-21

a. Federal agencies must ensure the retention, protection, and accessibility of the electronic records comply with OMB Memorandum, M-19-21. Federal agencies will manage all temporary and permanent records in an electronic format with appropriate metadata.

b. OMB Memorandum M-19-21 requires agencies to transition recordkeeping to a fully electronic environment consistent with Federal records management regulations, develop plans to close their storage facilities (also called RHAs), and transfer analog records to FRCs operated by NARA or to commercial storage facilities. The Army Electronic Archive (AEA) modification allows the Army to electronically store and maintain records with a disposition of more than 1 year within ARIMS.

4-3. Maintaining Information System

An information system is an automated system that contains and provides access to Federal records and other information. This information may be administrative or programmatic and whose functions include collecting, storing, assembling, processing, transmitting, and disseminating information electronically according to defined procedures.

4-4. Electronic records management controls

a. Army is required to manage its electronic records in accordance with 36 CFR 1236.10. The following types of records management controls are needed to ensure that Federal records in information systems provide adequate and proper documentation of Army business. These controls must be incorporated into the information system or integrated into a recordkeeping system that is external to the information system itself. These controls are as follows:

(1) Reliability—controls to ensure a full and accurate representation of the transactions, activities, or facts to which they attest and can be depended on during subsequent transactions or activities.

(2) Authenticity—controls to protect against unauthorized addition, deletion, alteration, use, and concealment.

(3) Integrity—controls, such as audit trails, to ensure that records are complete and unaltered.

(4) Usability—mechanisms to ensure that records can be located, retrieved, presented, interpreted, and accessioned to NARA when applicable.

(5) Content—mechanisms to preserve the information contained within the record itself that was produced by the creator of the records.

(6) Context—mechanisms to implement cross-references to related records that show the organizational, functional, and operational circumstances about the record, which will vary depending on the business, legal, and regulatory requirements of the business activity.

(7) Structure—controls to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

b. The records management controls must be planned and implemented in the system as part of the capital planning and systems development life cycle processes.

c. All records in the system must be retrievable and usable for as long as the NARA-approved retention period dictates. If the records will need to be retained beyond the planned life of the system in which the records are originally created or captured, the migration of records and their associated metadata to new storage media or formats must be completed by the system owner, in order to avoid loss due to media decay or technological obsolescence. See NARA Universal Electronic Records Management available at <https://www.archives.gov/>.

Chapter 5 Records Retention

5–1. Records Retention Schedule

a. A records retention schedule (also known as a disposition schedule, or simply, a schedule), is a document that provides instructions for what to do with records no longer needed for current Government business.

b. In accordance with 44 USC 3301–44 USC 3314, the Army is required by law to develop agency records schedules that cover all Army records that are not covered by the GRS. The GRS is issued by the Archivist of the United States to provide disposition authorization for records common to several or all agencies of the Federal Government. The GRS—

- (1) Does not cover all records such as program-specific records of an agency.
- (2) Does not apply to most or all permanent records (there are currently five dispositions contained in the GRS).
- (3) Does not apply to records related to military pay and military personnel.

Note: These records are covered under Army specific schedules.

5–2. The Records Retention Schedule-Army

The RRS–A is the records retention schedule approved by NARA and the only legal authority for destroying non-permanent Army information. Record information will be identified and managed in ARIMS, according to either short term or long term, based on their value to the business process.

- a. Application and other details of RRS–A are enumerated in DA Pam 25–403.
- b. Classified electronic records up through secret can be managed on the ARIMS-Classified website.
- c. Disposition of all records, including classified and unclassified, is prescribed in DA Pam 25–403.

5–3. The Army Records Information Management System

ARIMS is the official records repository for all Army records.

a. It lists and details all records with their appropriate record number and disposition schedule instructions.

b. ARIMS is a web-based tool used to identify, arrange, manage, store, retrieve, and apply dispositions to Army record material. It is a portal to the RRS–A, the Army Consolidated Records Schedule (ACRS) framework, the AEA, and a software suite of tools to manage Army record information. Functionality is based on the role of the user. ARIMS has an unclassified site and a classified site. The links for both sites are for unclassified at <https://www.arims.army.mil> and classified <https://www.arims.army.smil.mil>.

c. All Army records should be stored in accordance with applicable records management policies and directives (that is, system examples include Defense Travel System, Defense Civilian Personnel Data System or Automated Time Attendance and Production System). If organizations are storing their records in an information system outside of ARIMS, they must ensure that the system has the ability to maintain the records throughout their life cycle according to its scheduled disposition. For more details and training see AR 25–1, DA Pam 25–403, and the ARIMS user guide.

Chapter 6 Disposition of Records

6–1. Disposition

The final phase of the records life cycle is disposition. Disposition is the actions taken regarding records no longer needed for the conduct of the regular current business of the Army. Records disposition includes transfer to the AEA, retirement to FRCs, disposal of temporary records and accession of permanent records to NARA. Temporary records are disposed of in accordance with the disposition instructions that were developed when the records were scheduled. Requests for deviation in disposition instructions must be sent through records management channels to be approved by the Archivist of the United States. See 36 CFR 1226.26 for direct donations to NARA. Litigation holds and record freezes related to legal actions may require changes to normal disposition and must be coordinated with the appropriate legal counsel. Destruction after a litigation hold or record freeze will only be resumed with the concurrence of

the legal office that ordered the hold or freeze. Procedures for disposition of Army records are prescribed in DA Pam 25–403.

6–2. Transfer and retirement

a. OMB Memorandum, M–19–21, has directed that no later than 31 December 2022, all temporary agency records will be managed electronically to the greatest extent possible. By this date, all Army RHAs must be closed, and all inactive, temporary analog records must be transferred to FRCs or commercial storage facilities that meet NARA records storage requirements. Originating offices or units will send electronic temporary (1+) and permanent records to ARIMS for storage in the AEA as soon as they are complete. If the records must be kept onsite longer than the completion date, a request for exception will be forwarded to ARMD. Legacy hardcopy or analog records will be prepared for transfer or retirement by the appropriate RM or records coordinator. The procedures for records transfer and retirement are prescribed in DA Pam 25–403.

b. FRCs are establishments maintained and operated by NARA used to store federal records. Commercial Records Storage Facilities or Centers are maintained and operated by a private commercial entity used to store federal records. Until permanent closure of RHAs, Army installations and activities not serviced by an installation RHA (such as, HQDA principal officials and any Army organization not residing on an Army installation) will coordinate with ARMD prior to sending an electronic Standard Form (SF) 135 (Records Transmittal and Receipt) through Archives and Records Centers Information System directly to a FRC.

Chapter 7 Wartime and Contingency Operations Records

7–1. General

Recordkeeping requirements during wartime and contingency operations (CONOPS) are governed by the same statutes, laws, and regulations as recordkeeping during peacetime or while in garrison, except that wartime and CONOPS records are permanent records. The nature of a wartime and CONOPS environment requires sound management of record information. Inadequate documentation puts the Army at risk for losing important segments of its history, limits its ability to formulate lessons learned, and could potentially lead to a failure on the part of the Army to protect the rights and interests of Soldiers and DA Civilians deployed during wartime and/or CONOPS.

7–2. Preservation and transfer

Army commanders at all levels will ensure wartime and CONOPS records are created and preserved throughout the Army. Wartime and CONOPS records are permanent records and must be transferred to the Archives with appropriate metadata. See NARA website for applicable formats for transfer. During an international armed conflict, records in the custody of the Army outside the territorial limits of the continental United States may only be destroyed if appropriate as determined by the combatant command or ASCC. See DA Pam 25–403 for instructions.

Appendix A

References

Section I

Required Publications

Army publications are available on the Army Publishing Directorate website available at <https://armypubs.army.mil/>. CFRs are available at <https://www.ecfr.gov/>. DoD publications are available at <https://www.esd.whs.mil/>. USCS are available at <https://uscode.house.gov/>.

AR 25–2

Army Cybersecurity (Cited in para 4–1.)

DA Pam 25–1–2

Information Technology Contingency Planning (Cited in para 2–2k.)

DA Pam 25–403

Army Guide to Recordkeeping (Cited in para 1–3.)

DoD 5015.02–STD

Electronic Records Management Software Applications Design Criteria Standard (Cited in para 2–5b(1).)

DoDI 5010.40

Managers' Internal Control Program Procedures (Cited in para 2–2b.)

DoDI 5015.02

DoD Records Management Program (Cited in the title page.)

DoDI 5400.11

DoD Privacy and Civil Liberties Programs (Cited in para 2–2f.)

DoDI 6025.18

Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs (Cited in para 2–2f.)

DoDI 8320.02

Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense (Cited in para 2–5d.)

Executive Order 12829

National Industrial Security Program (Cited in para 3–7c.) (Available at <https://www.archives.gov/>.)

NARA Bulletin 2017–01

Agency Records Management Training Requirements (Cited in para 1–6e.) (Available at <https://www.archives.gov/>.)

OMB Circular A–130

Managing Information as a Strategic Resource (Cited in para 2–2a.) (Available at <https://www.cio.gov/policies-and-priorities/>.)

OMB Memorandum M–12–18

Managing Government Records Directive (Cited in para 2–1b.) (Available at <https://www.archives.gov/>.)

OMB Memorandum M–19–21

Transition to Electronic Records (Cited in para 2–2m.) (Available at <https://www.archives.gov/>.)

PL 93–400

Office of Federal Procurement Policy Act (Cited in para 3–7a.) (Available at <https://www.congress.gov/>.)

PL 113–187

Presidential and Federal Records Act Amendments of 2014 (Cited in title page.) (Available at <https://www.congress.gov/>.)

36 CFR, Chapter XII, Subchapter B

National Archives and Records Administration, Records Management (Cited in para 1–6a.)

36 CFR 1220.34

What must an agency do to carry out its records management responsibilities? (Cited in para 1–6e.)

36 CFR 1226.26

How do agencies donate temporary records (Cited in para 6–1.)

36 CFR 1236.10

What records management controls must agencies establish for records in electronic information systems? (Cited in para 4–4a.)

48 CFR 200–299

Defense Acquisition Regulations System Department of Defense (Cited in para 3–7a.)

5 USC 552

Freedom of Information Act (Cited in para 3–7b.)

5 USC 552a

Privacy Act of 1974 (Cited in para 3–7b.)

18 USC 641

Public money, property or records (Cited in para 1–6c(1).)

18 USC 2071

Concealment, removal, or mutilation generally (Cited in para 1–6c(1).)

41 USC

Public Contracts (Cited in para 3–7a.)

44 USC Chapter 29

Records Management by the Archivist of the United States and by the Administrator of General Services (Cited in para 1–6a.)

44 USC Chapter 31

Records Management by Federal Agencies (Cited in para 1–6a.)

44 USC Chapter 33

Disposal of Records (Cited in para 1–6a.)

44 USC Chapter 35

Coordination of Federal Information Policy (Cited in para 1–6d.)

44 USC Chapters 21–35

Federal Records Act (Cited in para 1–1.)

44 USC 2904(c)(7)

General responsibilities for records management (Cited in para 3–10a.)

44 USC 2906

Inspection of agency records (Cited in para 3–10a.)

44 USC 3101

Records management by agency heads; general duties (Cited in para 1–1.)

44 USC 3301–44 USC 3314

Disposal of Records (Cited in title page.)

Section II

Prescribed Forms

Unless otherwise indicated, DA Forms are available on the Army Publishing Directorate website available at (<https://armypubs.army.mil/>). Standard Forms and Optional Forms are on the General Service Administration website available at (<https://www.gsa.gov/>).

SF 135

Records Transmittal and Receipt (Prescribed in para 6–2b.)

Appendix B

Internal Control Evaluation

B–1. Function

This internal control evaluation assesses the execution of the Army Records Management Program.

B–2. Purpose

The purpose of this evaluation is to assist HQDA, ACOMs, ASCCs, DRUs, and installations in evaluating the key internal controls listed in paragraph B–4. It is intended as a guide and does not cover all controls.

B–3. Instructions

Answers must be based on the actual testing of internal controls (for example, document analysis, direct observation, sampling, or other). Answers that indicate deficiencies must be explained and corrective action indicated in supporting documentation. These key internal controls must be formally evaluated at least once every 5 years. Certification that this evaluation has been conducted must be accomplished on DA Form 11–2 (Internal Control Evaluation Certification).

B–4. Test questions

- a. Is a records management program established in your organization?
- b. Has a RA or RM been appointed in writing to manage the internal records of the organization and its sub-elements?
- c. Are all personnel within the organizational scope receiving records management training annually?
- d. Have RMOs received specialized records management training within 90 days of their appointment?
- e. Does the RA survey and evaluate the command or agency records management program at least once every 2 years and send the report to ARMD?
- f. Does the RM survey and evaluate the organization at least once every 2 years to the office or unit level and forward the report to the servicing RA?
- g. Does the RA or RM participate in the planning process for new or replacement IT systems?
- h. Have instructions been issued specifying the degree of protection to be afforded record information (including email) stored and used electronically in accordance with classification requirements, release ability, accessibility, and sensitivity, such as the Freedom of Information Act, personally identifiable information, and other types of sensitive records?
- i. Are controls being used to capture and prevent the unauthorized alteration or deletion of electronic records including email, instant messages, and other communication media?
- j. Are procedures in place to ensure electronic record information is readable throughout its retention period, in accordance with OMB Memorandum M–19–21 and this regulation?

B–5. Supersession

This evaluation replaces the evaluation previously published in AR 25–400–2, dated 2 October 2007.

B–6. Comments

Help to make this a better tool for evaluating internal controls. Submit comments to the Army records officer via the email address specified at usarmy.belvoir.hqda-rmda.mbx.rmda-certification@army.mil or via U.S. Mail to the Army Records Management Directorate, 9301 Chapek Road, Building 1458, Fort Belvoir, VA 22060–5605.

Glossary of Terms

Access

The ability or permission to locate, use, or retrieve record information. Security measures must be used to limit access to sensitive or classified electronic and hardcopy record information.

Accession

The act and procedures involved in transferring legal title and physical custody of records from DA to NARA. This action is done by ARMD through a formal offer of the records to NARA.

Army Consolidated Records Schedule

ACRS is a large aggregation schedule crosswalk or framework that organizes the RRS–A record numbers according to functionally related records series and subseries.

Army Electronic Archives

Stores electronic documents that makeup a record.

Army Records Information Management System

ARIMS is the IT system for identifying, arranging, managing, storing (electronic records), retrieving, and applying dispositions to Army record material. The system is accessed via the ARIMS website (<https://www.arims.army.mil>). The web-site contains the RRS–A, the ACRS framework, the AEA, and a software suite of tools to manage Army record information.

Army Records Management Program

Governs the capture, maintenance, and disposition of Army information.

Army records officer

A NARA requirement. All federal agencies will appoint a records officer who is responsible for leading, planning, and managing the Army Records Management Program for both core mission and administrative records, regardless of medium or format.

Cloud computing

As defined by NARA, a technology that allows users to access and use shared data and computing services via the Internet or a virtual private network. It gives users access to resources without having to build infrastructure to support these resources within their own environments or networks.

Copy

A reproduction or duplication of an original record. Copies are often identified by their functions, such as action copy, file or record copy, information or reference copy, and official copy.

Disposition

The actions taken with noncurrent records. These include transfer to the AEA, a RHA, retirement to an FRC, authorized donations, destruction, and accessioning into NARA.

Disposition instructions

Precise instructions specifying the time and/or event for transfer, retirement, or destruction of record information.

Electronic discovery

Electronic discovery involves identifying and collecting electronically stored information (record and non-record) that may be potentially responsive to a particular lawsuit.

File

An accumulation of records maintained in a predetermined physical or electronic arrangement or to place documents in a predetermined location according to an overall plan of classification.

Information management

Activities required to coordinate, plan, organize, analyze, integrate, evaluate, and control information resources effectively throughout their life cycle.

Information system

A set of information resources organized for the collection, processing, use, sharing, storage, maintenance, transmission, dissemination, and disposition of information in accordance with defined procedures, whether automated or manual.

Litigation hold

Litigation refers to any legal action involving a court of law. Because of ongoing litigation, an agency's counsel's office may periodically issue litigation holds or moratoriums on destruction for certain records believed to be potentially responsive or helpful in ongoing or pending litigation.

Office

Any place where record information is created, maintained, or used.

Office records list

A list of the specific RRS—A record titles and numbers describing record information accumulated or generated in an office. The list includes the ACRS, System of Records Notice, disposition code, and prescribing directive information for each record title and record number entry. It is prepared within each element where records are accumulated or generated by using the ARIMS office records lists and folders module (tab). Office records lists are coordinated with the organization or installation RMO.

Permanent records

The designation applied to records worthy of permanent retention by the United States and accessioned into NARA.

Record copy (official)

That copy of a record kept by the agency, office, or element directly responsible for the function to which the record relates. It does not include reading file copies or copies held for convenience or reference.

Record freeze

Records whose scheduled disposition has been temporarily suspended because of special circumstances that alter the administrative, legal, or fiscal value of the records.

Record number

The number assigned to an RRS—A record title describing a unique category of record information.

Record series

A group of records that are generally used and filed as a unit because they relate to a particular subject or function, result from the same activity, document a specific type of transaction, or relate in some other fashion.

Recorded information

Includes all traditional forms of records, regardless of physical form or characteristics, including information created, manipulated, communicated, or stored in digital or electronic form.

Records

As defined in the Federal Records Act of 1950, as amended, the term, "records" includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the U.S. Government or because of the informational value of data in them.

Records center

A secure facility that is designed and constructed for low-cost and efficient storage of records, and for reference service on semi-current records, pending their ultimate disposition.

Records holding area

A secure facility established to collect and maintain cutoff records until they are either eligible for destruction or retirement to an FRC or other records depository. When located outside continental United States, these facilities are referred to as overseas command RHA.

Records management

The planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to record information creation, maintenance (use, storage, retrieval), and disposition in order to achieve adequate and proper documentation of Federal policies and transactions and effective and economical management of DA operations.

Records Retention System—Army

The system governing the identification, retention, and disposition of recurring series or types of Army record information. An Army Directive, usually an AR prescribes policy on the creation, maintenance, and use of the record information. The DA Pam provides procedures on how to implement the policy established in the AR. The purpose of the RRS–A is to provide continuing authority to dispose of, transfer, or archive record information.

Retention period

The length of time a record must be kept (either in the office, system, or in off-site storage) before it is destroyed. Records not authorized for destruction have a retention period of permanent.

Retire

The movement of records from an office, unit, or RHA into an FRC.

Shared drive

Shared drives, also known as network drives, are typically used to store and share content. Agencies have also used shared drives to group and store content by function, project, committee, or other logical category. The use of shared drives poses recordkeeping challenges because agencies may store content that includes Federal records and non-record materials.

Social media

As defined by NARA, social media tools use internet and web-based technologies to integrate technology, social interaction, and content creation. Social media use the “wisdom of crowds” to connect information in a collaborative manner online. Through social media, individuals or collaborations of individuals create web content, organize content, edit, or comment on content, combine content, and share content.

Staff journal

Chronological record of events pertaining to a unit or a staff section during a given period. A journal file is one that contains material necessary to support entries in the journal.

Transfer

The movement of records from an office or unit into an RHA or the AEA.

Unscheduled records

Records that have not been approved by NARA for disposition. They may not be destroyed or deleted.

Vital or essential records

The vital or essential records needed to meet operational responsibilities under national security emergencies, or other emergency or disaster conditions (emergency operating records), or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records).

SUMMARY of CHANGE

AR 25–400–2
Army Records Management Program

This administrative revision, dated 15 June 2023—

- Changes proponentcy from the Administrative Assistant to the Secretary of the Army to the Chief Information Officer (title page).

This major revision, dated 18 October 2022—

- Changes the title of the regulation from “The Army Records Information Management System (ARIMS)” to “Army Records Management Program” (cover).
- Updates responsibilities (chap 1, sec II).
- Adds the definition of a “record” according to the Federal Records Act of 1950 as amended by the Presidential and Federal Records Act Amendments of 2014 (para 2–2b).
- Updates recordkeeping information as it pertains to various types of media and social media (para 2–9).
- Moves procedures on directions for handling the loss or destruction of records by fire, flood, or other cause to DA Pam 25–403 (formerly para 2–11).
- Adds guidance for maintaining classified electronic records (para 4–3).
- Moves procedures on records freezes, including electronic discovery actions, preservation orders, and litigation holds to DA Pam 25–403 (formerly para 5–3).
- Provides a new approach for managing wartime and contingency operations records (chap 6).
- Expands the policy and guidance for permanent electronic record information (para 6–1).
- Supersedes DA Memorandum 25–51, dated 29 March 2017.
- Transfers DA Form 534, DA Form 7796, OF 23, OF 24, and SF 115 to DA Pam 25–403.

UNCLASSIFIED

PIN 060671-000