Headquarters
Department of the Army
Washington, DC
10 November 2022

***Department of the Army Pamphlet 25–403**

Information Management

Army Guide to Recordkeeping

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 revision are listed in the summary of change.

Applicability. This pamphlet applies to the Regular Army, the Army National Guard/Army National Guard of the United States, the U.S. Army Reserve, unless otherwise stated. It also applies to and Department of the Army Civilians who perform recordkeeping duties. This pamphlet applies during partial and full mobilization.

Proponent and exception authority. The proponent for this pamphlet is the Chief Information Officer. 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 requirements.

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 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, the U.S. Army Reserve, and Department of the Army Civilians.

*This pamphlet supersedes DA Pam 25–403, dated 11 August 2008.

Contents (Listed by chapter and page number)

Contents—Continued

Figure List

Glossary of Terms

Summary of Change

Chapter 1
Introduction

Section I

General

1–1. Purpose
This pamphlet provides procedures for implementing policies established in AR 25–400–2. It contains operational procedures for the creation and/or receipt, maintenance and use, and disposition of Army records. Procedures include identifying records, managing the various types of records media, applying Retention Schedules and performing unit evaluations. This pamphlet illustrates the management of electronic records, the records scheduling process, records transferring, certifying information systems or electronic collections and proper handling of wartime and contingency operations (CONOPS) records. Specifically, this pamphlet addresses duties performed by records management officials (RMOs) and staff in carrying out the recordkeeping subprogram of the Army Records Management Program.

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
Policy associated with this pamphlet is found in AR 25–400–2.

1–4. Records management (recordkeeping) requirements
The records management requirement for all record numbers, associated forms, and reports required by this publication are addressed in the Records Retention Schedule–Army (RRS–A). 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, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance. To provide explanation of terms used in statutes and Army regulations and by providing guidance on the application of these terms to the documentary materials that the Army accumulate in their daily operations.

Section II

Appointment of Roles

1–5. Designated records management roles
Everyone is responsible for managing records. Designated personnel will be assigned roles to oversee various aspects of the Army Records Management Program at different levels.

a. In accordance with AR 25–400–2, Headquarters, Department of the Army (HQDA) principal officials, Army commands (ACOMs), Army service component commands (ASCCs), and direct reporting units (DRUs) will appoint at each level of command, in writing, the following RMOs.

(1) Records administrator (RA).
(2) Records manager (RM).
(3) Records Holding Area Manager (RHAM).
(4) Records coordinator (RC).

b. Contractors will only be assigned records management responsibilities within the scope of their duties as assigned through their contract's provisions, obligations, and/or requirements who perform records duties on behalf of the Army.

c. See appendix D for sample appointment memorandum.

1–6. Records management official duties and functions
a. RAs will—

(1) Complete within 90 days of being appointed Records Management Training and RMO Training via Army Learning Management System (ALMS) and Army Records Information Management System (ARIMS) training from the Army Records Management Directorate (ARMD), Records Management Division (RMD).

(2) Serve as the command subject matter expert (SME) for records management by providing policy interpretation and procedural guidance ensuring compliance with applicable regulations and laws.

(3) Provide command-wide oversight ensuring the creation and preservation of official mission records throughout subordinate units and activities.

(4) Ensure senior officials receive orientation training (when taking new positions) and exit briefings before departing the position on the appropriate disposition of the records, including email, under their immediate control (see 36 CFR 1222.24(a)(6) and 36 CFR 1230.10(a & b)). Orientation training will include an overview of the Army Records Management Program and the senior official's responsibilities pertaining to the program. The training may be given in any forum conducive to the senior official's schedule or included in their training from either the War College or Civilian Senior Leader Management Office (CSLMO) in coordination with RMD.

(5) Survey and evaluate the Army Records Management Program at least every 2 years. Upon completion, provide findings, recommendations, and corrective actions in the evaluation report to RMD (see para 12–3 for procedures).

(6) Ensure all records management officials within the organization receive records management and RMO training annually via the ALMS website (available at https://www.lms.army.mil/) and ARIMS training via RMD.

(7) Ensure all personnel within the organization receive Annual Records Management Training via the ALMS website available at https://www.lms.army.mil/.

(8) Ensure record information is identified, maintained, and the RRS–A disposition applied, with temporary records destroyed on schedule and permanent records ultimately accessioned to National Archives and Records Administration (NARA). Ensure all unscheduled records are scheduled regardless of location (see para 2–4 for procedures).

(9) Approve ARIMS office records lists (ORLs) for sub-units and supported organizations (see ARIMS User Guide for procedures).

(10) Instruct personnel on their legal responsibility to report any actual or potential unlawful removal, change, or destruction of records and inform personnel to attempt to recover or reconstruct the records (see para 7–12 for procedures).

(11) Notify the organization of the legal requirement to suspend routine destruction practices during a record freeze to ensure the preservation and retention of electronic and hardcopy records (see para 10–4 for procedures).

(12) Validate the establishment of an Essential Records Program formerly known as vital records (see chap 11 for procedures).

(13) To the fullest extent possible, promote a paper-free business environment using technology.

(14) Annually identify records eligible for destruction in accordance with the NARA approved records disposition (see chap 7 for procedures).

(15) Maintain a working relationship with the local Army Staff Judge Advocate (SJA) or legal advisor, security manager(s), and information system or electronic collection owners.

(16) Participate in the planning, development, and use of cloud computing solutions (see para 4–13 for procedures).

(17) Ensure information system or electronic collection owners, program or project managers implement records management requirements in systems throughout their life cycle and complete the Department of Army (DA) Form 7796 (Automated Information System (AIS) Questionnaire) (see para 6–3 for procedures).

(18) Ensure the Department of Defense (DD) Form 2930 (Privacy Impact Assessment (PIA)) Section 1, Question l, "What is the NARA approved, pending, or general record schedule (GRS) disposition authority for the system or for the records maintained in the system?" is filled out correctly for all systems listed in the Army Portfolio Management Solution (APMS).

(19) Support legal advisors, particularly regarding discovery actions, records freezes, and other legal issues regarding records management.

(20) Engage with social media content managers to ensure record information and social media sites/platforms are identified and appropriately preserved.

(21) Provide advice and assistance to security managers in the identification, creation, sharing, marking, safeguarding, storage, dissemination, disposition, destruction, and records management of controlled unclassified information (CUI) documents and materials.

(22) Engage in the planning and use of collaborative spaces where teams share, store, search, and access files.

(23) Review and recommend approval of new user requests for access to the Archives and Records Centers Information System (ARCIS) (see para 9–2 for procedures).

(24) Ensure the DD Form 67 (Form Processing Action Request) is properly staffed with the appropriate record disposition for new or modified DD and DA Forms.

(25) Ensure the appropriate record disposition schedule has been identified for a system of record notice (SORN).

(26) Collaborate with local information technology (IT) staff on records management requirements for any government furnished equipment such as mobile phones (text messages).

b. RMs will—

(1) Complete within 90 days of being appointed Records Management Training and RMO Training via ALMS and ARIMS training via RMD.

(2) Serve as the command or local SME for records management by providing policy interpretation and procedural guidance ensuring compliance with applicable regulations and laws.

(3) Provide command-wide oversight ensuring the creation and preservation of official mission records throughout subordinate units and activities.

(4) Ensure senior officials receive orientation training (when taking new positions) and exit briefings before departing the position on the appropriate disposition of the records, including email, under their immediate control (see 36 CFR 1222.24(a)(6) and 36 CFR 1230.10(a & b). Orientation training will include an overview of the Army Records Management Program and the senior official's responsibilities pertaining to the program. The training may be given in any forum conducive to the senior official’s schedule and in most cases will be included in their training from either the War College or Civilian Senior Leader Management Office (CSLMO) in coordination with RMD.

(5) Survey and evaluate the Army Records Management Program at least every 2 years. Upon completion, provide findings, recommendations, and corrective action in the evaluation report to the servicing RA (see para 12–3 for procedures).

(6) Ensure all records management officials within the organization receive records management and RMO training annually via ALMS website available at https://www.lms.army.mil/ and ARIMS training via RMD.

(7) Ensure all personnel within the organization receive records management training annually via the ALMS website available at https://www.lms.army.mil/.

(8) Ensure record information is identified, maintained, and the RRS–A disposition applied, with temporary records destroyed on schedule and permanent records ultimately accessioned to NARA. Ensure all unscheduled records are scheduled regardless of location (see para 2–4 for procedures).

(9) Approve ARIMS ORLs for sub-units and supported organizations (see ARIMS User Guide for procedures).

(10) Instruct personnel on their legal responsibility to report any actual or potential unlawful removal, change, or destruction of records and inform personnel to attempt to recover or reconstruct the records (see para 7–12 for procedures).

(11) Notify the organization of the legal requirement to suspend routine deletion practices during a record freeze to ensure the preservation and retention of electronic and hardcopy records (see para 10–4 for procedures).

(12) Validate the establishment of an Essential Records Program formerly known as vital records (see Chapter 11 for procedures).

(13) To the fullest extent possible, promote a paper-free business environment using technology.

(14) Annually identify records eligible for destruction in accordance with the NARA approved records disposition (see chap 7 for procedures).

(15) Maintain a working relationship with the local Army SJA or legal advisor, security manager(s), and information system or electronic collection owners.

(16) Participate in the planning, development, and use of cloud computing solutions (see para 4–13 for procedures).

(17) Ensure information system or electronic collection owners, program or project managers implement records management requirements in systems throughout their life cycle and complete the DA Form 7796, AIS Questionnaire (see para 6–3 for procedures).

(18) Ensure the DD Form 2930 PIA Section 1, Question l, "What is the NARA approved, pending, or GRS disposition authority for the system or for the records maintained in the system?" is filled out correctly for all systems listed in APMS.

(19) Support legal advisors, particularly regarding discovery actions, records freezes, and other legal issues regarding records management.

(20) Engage with social media content managers to ensure record information and social media sites and/or platforms are identified and appropriately preserved.

(21) Provide advice and assistance to security managers in the identification, creation, sharing, marking, safeguarding, storage, dissemination, decontrol, disposition, destruction, and records management of CUI documents and materials.

(22) Engage in the planning and use of collaborative spaces where teams share, store, search, and access files.

(23) Review and recommend approval of new user requests for access to ARCIS (see para 9–2 for procedures).

(24) Ensure the DD Form 67 (Form Processing Action Requests) is properly staffed with the appropriate record disposition for new or modified DD and DA forms.

(25) Ensure the appropriate record disposition schedule has been identified for a SORN.

(26) Collaborate with local IT staff on records management requirements for any government furnished equipment such as mobile phones (text messages).

c. In addition to the responsibilities listed above RMs that oversee a Records Holding Area (RHA) will—

(1) Ensure RHAMs are appointed, in writing, for all established and approved RHAs (until permanently closed) and are registered as an RHAM in ARIMS.

(2) Ensure records are properly arranged and packed before movement from the RHA to an authorized records center.

(3) Maintain liaison with and coordinate the transfer, retirement, and retrieval of records with the Federal Records Centers (FRCs).

(4) Index records submitted by installation offices and tenant offices into ARIMS.

d. RHAMs will—

(1) Complete within 90 days of being appointed Records Management Training and RMO Training via ALMS and ARIMS training via RMD.

(2) Ensure records are maintained in a facility constructed with non-combustible materials including walls, columns and floors in accordance with CFR 36 Chapter 12, Subpart B 1234.10.

(3) Ensure all records are indexed in the ARIMS master index down to the folder level.

(4) Ensure records removed from the RHA for reference or other actions are returned in a reasonable time frame.

(5) Establish a locator and disposition file.

(6) Ensure that eligible records are retired or destroyed at the appropriate time in accordance with the RRS–A.

(7) Notify organizations of impending records destruction dates for their records stored in the RHA and obtain their written approval prior to destruction of the records.

(8) Inventory the holdings of the RHA annually (until permanently closed).

e. RCs will—

(1) Complete within 90 days of being appointed Records Management Training and RMO Training via ALMS and ARIMS training via RMD

(2) Ensure recordkeeping procedures are implemented and documented throughout their office of responsibility.

(3) Develop and review ORLs for their unit; ensure ORLs being submitted are pertinent to the unit's mission (see ARIMS User Guide for procedures).

(4) Ensure electronic records are transferred to the Army Electronic Archives (AEAs) via the ARIMS Bulk Archive Tool (BAT) (see BAT User Guide for procedures).

(5) Coordinate the transfer and retirement of long-term permanent records.

(6) Resolve indexing problems with the RHA (until permanently closed).

(7) Maintain a working relationship with the local SJA or legal advisor, security manager(s), and information system or electronic collection owners.

(8) Ensure information system or electronic collection owners, program or project managers implement records management requirements in systems throughout their life cycle and complete the DA Form 7796 (see para 6–3 for procedures).

(9) Ensure the DD Form 2930 PIA Section 1, Question l, "What is the NARA approved, pending, or GRS disposition authority for the system or for the records maintained in the system?" is filled out correctly for APMS.

Chapter 2
Identifying Records

2–1. Records

a. Records document the Army's business and can be found in all media formats such as paper, email, instant messaging, chat and text messages, telephone messages, voicemail messages, presentations, websites, social media, audio or video recordings, word processing documents, spreadsheets, and information systems or electronic collections. If the information is not a record, then such information would be categorized as either a non-record or personal paper.

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.

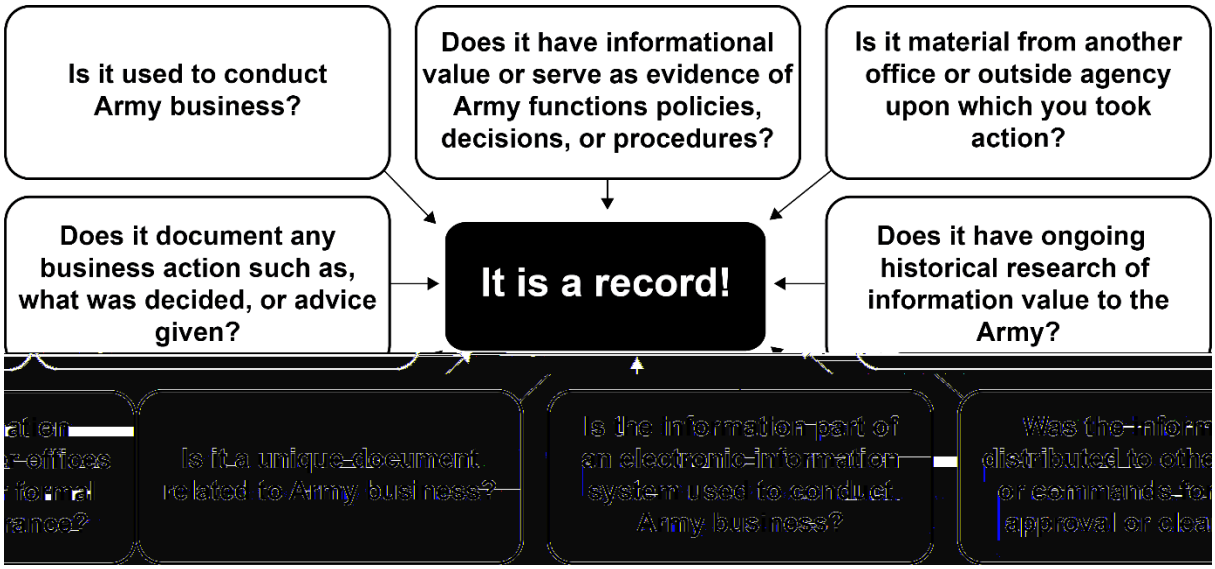


Figure 2–1. Identifying records

2–2. Non-records

Not all information created or received by the organization constitutes a record. Non-records are those federally owned informational materials excluded from the legal definition of records because they either do not meet the general conditions of records status, or fall into one of the following specific categories:

a. Extra copies of documents such as those used for reference purposes.

b. Stocks of publications and blank forms.

c. Library and museum materials made or acquired and preserved solely for reference or exhibition purposes.

d. Non-record materials also include the following:

(1) Information copies of correspondence, directives, forms, and other documents on which no administrative action is recorded or taken.

(2) Routing slips and transmittal sheets adding no information to that contained in the transmitted material.

(3) Tickler, follow-up, or suspense copies of correspondence, provided they are extra copies of the originals.

(4) Duplicate copies of documents maintained in the same file.

(5) Extra copies of printed materials for which complete record sets exist, such as current and superseded manuals maintained outside the office responsible for maintaining the record set.

(6) Catalogs, trade journals, and other publications received from other Government agencies, commercial firms, or private institutions and require no action are not part of a case on which action is taken.

(7) Physical exhibits, artifacts, and other material objects lacking evidential value.

2–3. Personal papers

a. Personal papers are documentary materials belonging to an individual not used to conduct agency business. They relate solely to an individual's personal and private affairs or are used exclusively for that individual's convenience. Personal papers may contain references to or comments on agency business but are considered personal if they are not used in the conduct of business. All personal papers must be filed separately from records and non-records. Personal papers are not owned by the government. Categories of personal papers includes the following:

(1) Business or professional records created before entering Government service. For example, records created during or relating to previously held positions, political materials, and reference material.

(2) Private documents brought into, created, or received in the office, such as—

(a) Family and personal correspondence.

(b) Materials documenting professional activities and outside business or political pursuits.

(c) Manuscripts and drafts for articles and books.

(d) Volunteer and community service records that do not relate to Army business are considered personal, even if created or received while in office.

b. If information about private matters and official business appears in the same document, the document should be copied at the time of receipt (with the personal information deleted) and treated as a record.

c. When departing, personal papers may be removed without Army or NARA approval.

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

2–4. Unscheduled records

Unscheduled records are Federal records whose final disposition has not been approved by NARA on a Standard Form (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 (RN). See chapter 6 for the scheduling process.

2–5. Contractor records

All data created for Army use and delivered to the Army are Federal records and therefore Government property. Such data is subject to the provisions of Title 44, United States Code, Chapters 33 (see 44 USC Chapters 21, 29, 31, and 33) as amended, the Freedom of Information Act (FOIA) (see 5 USC 552), as amended, and the Privacy Act of 1974 (see 5 USC 552a), as amended.

a. All Army contractors and subcontractors, including those performing congressionally mandated program functions must create and maintain records to document these programs.

b. The contract between the Army and the contractor must include requirements for the delivery of all pertinent documentation of contractor program execution to the Army.

(1) Contracts must specify Army ownership and delivery to the Army of all record information created or received by the contractor in fulfilling the contract requirements.

(2) Contracts should require that sufficient technical documentation and background information must accompany any deliverables in electronic formats to permit use of that information by the Army.

(3) Deferred ordering and delivery information clause should also be included in the contract to permit acquisition of any data/records information that may have value to the Army but were not identified in advance.

(4) Contractors must comply with the terms of the contract concerning the Government's rights in deliverables. If the contract is ambiguous or silent on the matter, contractors should treat all deliverables under the contract as the property of the U.S. Government for which the Army will have unlimited rights to use, dispose of, or disclose such data contained therein if determined to be in the public interest.

c. Contractors will comply with Army Records Management policies, including policies associated with safeguarding records covered by the Privacy Act of 1974, as amended.

(1) These policies include the preservation of all records created or received regardless of format or mode of transmission (hand deliver, email, and fax) or state of completion (draft and final).

(2) Contractors will assign the appropriate RN and disposition instructions to all records delivered to the Army.

(3) The Army record is the official record; copies retained by the contractor must be authorized by the Army and then destroyed in accordance with RRS–A record instructions.

(4) The contractor will delete and/or destroy non-delivered information.

d. Army oversight of records created by contractors is necessary to ensure that all Army recordkeeping requirements are met.

(1) Army-owned records are subject to inspection by the servicing RMO.

(2) Many contracts involve the creation of additional background information that may also have value to the Army. Whenever appropriate, RMOs should require the delivery of such background information in addition to the final product deliverables. For example—

(a) Contracts to produce statistical analyses will specify the delivery of background formulation information that may have value to the Army.

(b) Contracts to produce reports that represent Army policy will specify the delivery of background information needed to verify assertions or justify conclusions.

(c) Research contracts will specify the delivery of background information that has value to the Army.

2–6. Special records collections

Special records collections are a group of records that may or may not fall under the same series but are considered a collection based on common characteristics. Examples include the Gulf War Collection, Hurricane Andrew Relief Effort, and the Contingency Operations Collection (Operation Just Cause).

2–7. Federal Advisory Committees records

Federal Advisory Committee Act (FACA) records that are created by Army FACAs will be managed in accordance with the Office of the Secretary of Defense (OSD) Records and Information Management (RIM) Program policies and procedures. Specific responsibilities and requirements for the DoD Federal Advisory Committee Management Program are listed in DoDI 5105.04. Please include RMD in all communications with OSD.

2–8. Records of Joint staff and combatant commands

Records created in support of the Joint staff and combatant commands are managed in accordance with the Chairman of the Joint Chiefs of Staff (CJCSM) 5760.01A, Volume 1 and CJCSM 5760.01A Volume, 2.

2–9. Records life cycle

The records life cycle consists of three phases that a record goes through during its life span. The phases are create and/or receive, maintenance and/or use and disposition:

a. Create and/or receive. The Army either create or receive records as it conducts its business and records can exist in many formats on various media.

(1) When records are created, records must be identified as the official record copy that will be maintained to support the organization's business needs.

(2) When records are received, the original is usually classified as the record copy. Once the record copy is identified, it should be managed along with other office records. For both temporary and permanent electronic records, the official copy is to be moved to the official records filing area.

b. Maintenance and use. Records are kept for documenting an action taken, support a decision or legal requirement, respond to inquiries, and for reference purposes. In the maintenance and use phase, records are assigned a RN, which is used to file and retrieve the records. During this phase, records are referred to as active or inactive, depending on how often the record is accessed.

(1) *Active records.* Records are considered active if they are used frequently. Active records are maintained in the current file area (CFA) where they are available for easy retrieval.

(2) *Inactive records.* Records that must be retained but not routinely referred to on a regular basis. Records become inactive when the need or value for current business activity has ended.

c. Disposition. During the final phase of the record's life, it will either be destroyed if it is a temporary record or accessioned to NARA if it is permanent. A record is disposed of according to its approved disposition instructions.

(1) *Temporary records.* Temporary records are destroyed after a fixed period, or a specified event has occurred. The time may range from 90 days to several years. Over 90 percent of Army records are categorized as temporary.

(2) *Permanent records.* Records considered sufficiently valuable as to warrant ongoing preservation by the Federal Government, are categorized as permanent. Less than 10 percent of Army records are categorized as permanent.

Note. In accordance with AR 25–400–2, before disposal, it is required to conduct an inventory of all records to ensure proper disposition.

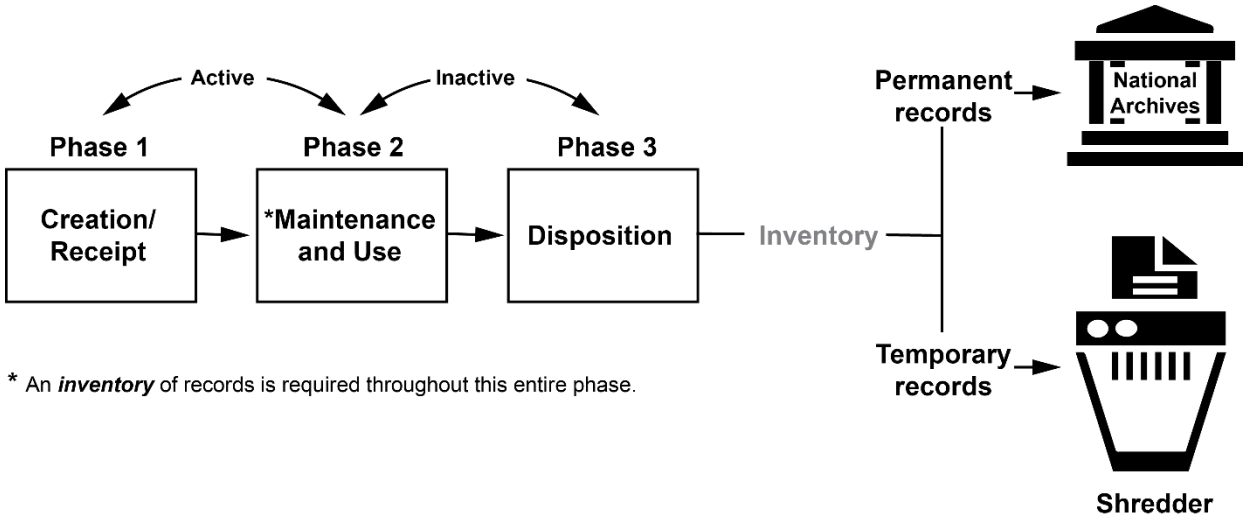


Figure 2–2. Records life cycle

2–10. Recordkeeping requirements

Recordkeeping requirements are statements in laws, regulations, or organization directives providing general and specific guidance for records to be created and maintained by an organization.

a. The Army is legally obligated to create and maintain adequate and proper documentation of its organization, functions, and activities and must issue recordkeeping requirements for—

(1) Activities at all levels.

(2) Records in all file formats and media.

(3) Distinguish non-record materials and personal papers.

b. According to AR 25–400–2, proponents of prescribing directives will ensure DA Administrative publications identify records required to support their business processes as required by AR 25–30 and DA Pam 25–40. These records are created or received when carrying out the missions or functions of the programs prescribed therein. If the publication has a records management requirement state "Records management requirements for all RNs, associated forms and reports required by (proponent's publication) are included in the Army's RRS–A. Detailed information for all RNs, forms and reports associated with (proponent's publication) are located in the RRS–A at https://www.arims.army.mil."

c. If a DA Administrative publication does not have a records management requirement, state in the publication, "This publication has no recordkeeping requirements."

d. Proponents will coordinate any new, revised, or rescinded recordkeeping requirements (including recommended retention periods for the new or revised requirements) in Army directives with their RMOs.

(1) In accordance with AR 25–400–2, RMOs will use the RRS–A to identify the RN under which the records will be kept and send requests for new, revised, or rescinded numbers to RMD along with proposed disposition instructions as needed.

(2) Temporary RNs, titles, and disposition instructions for new RNs will be established by RMOs in coordination with RMD. The requirements will be submitted in the same format as shown for RNs in the RRS–A and will include a complete description of the records to be created, identifying any specific forms or documents that are to be used and information systems or electronic collections that are used to produce or store the records.

e. Proponents will review the recordkeeping requirements whenever making changes to the prescribing directive, to include rescinding the directive, and inform RMD of the changes.

2–11. Maintaining information as records

Effective records maintenance and reference procedures are essential to document the Army's official business. Records should be fully maintained electronically possible. All media and systems selected to store and manage electronic records throughout their life cycle must meet the requirements of DoD 5015.02–STD.

2–12. Arranging records
Unless specified by the prescribing directive, records can be filed either chronologically or alphabetically as suits the business practices of the individual office and the types of records that the office maintains.

2–13. Maintaining records for multiple organizations
The organization hosting the records will coordinate the maintenance of the records being saved in its environment. Officials performing duties will develop procedures for the records created in each capacity.

2–14. Maintaining records in libraries
Record copies of publications and other permanent documents as described in the RRS–A will not be maintained as a part of library collections or manuscript collections in libraries or museums. When extra copies are maintained in these collections, they should be distinctly marked "library copy" or "museum copy."

2–15. Records inventory
An inventory is a detailed listing that includes the record types, locations, dates, volumes environments, classification, and usage data of an organization's records.

a. General. An inventory comprises of four actions—

(1) Physically inspect all files in the unit and/or office.

(2) Record the essential information about the files.

(3) Identify duplicate, fragmented, and related records.

(4) Match the records to the appropriate RN and/or records disposition schedule.

b. Records Inventory Process. All Army elements will provide accountability status of all textual records (such as paper, maps, and photos) and analog records (such as audio, video, and motion picture files).

c. The inventory process should include all records and exclude non-records.

(1) A record is created when an office either generates or receives information that gives evidence of its activities, such as completed forms, reports, correspondence, maps, drawings, and photographs. The recording media may be paper, microform, optical disk, magnetic tapes, network drives, and file servers.

(2) Non-records include reference materials, blank forms, and personal papers:

(a) Reference materials. These are the convenience copies made of records created or received, and publications that are not evidence of governmental activities (such as magazines, catalogues, trade journals, and Federal and State policies) or regulations, books, and pamphlets. These are not records and are not, therefore, candidates for a records retention schedule.

(b) Blank forms. Until they are filled, blank forms are supplies, not records.

(c) Personal papers. Personal papers are documentary materials belonging to an individual that are not used to conduct agency business. Personal papers are excluded from the definition of Federal records and are not owned by the Federal Government.

d. Who conducts the inventory ? Individuals experienced with the records, filing systems, and operations of the division, office, or program area.

e. Planning the inventory. Survey all office and storage areas before launching the inventory to determine the locations of records and their estimated total volume, and to flag any hazards or problems with space and storage. The success of an inventory project depends on the cooperation of the people involved with the records. Communicate with the office staff to let them know the inventory is meant to identify records and not to criticize their methods. Ensure that inventory personnel have access to:

(1) All unrestricted records and the information needed for restricted records.

(2) Office staff, to obtain information about how the records are organized and used (including organizational charts and other information that describes the main functions of each office).

f. Conducting the inventory. The inventory process should begin with all the information in office spaces, with a concentrated effort on mission and/or program records, as well as administrative and housekeeping records held in many or all offices that are already described and scheduled in the RRS–A (www.arims.army.mil). When accessing program records, pay special attention to those records designated for permanent retention.

g. Inventory quality control. The RM will assess the quality of the records inventory results. The results should be spot-checked for obvious errors. Those errors could include failing to indicate the location of

the records inventoried, exaggerating their volume, and intermixing two or more potentially permanent series or two or more temporary series having potentially varying retention periods.

h. Inventory preparation. If someone else has prepared the inventory, the RM will physically examine some of the records inventoried to confirm the accuracy of the information recorded on the inventory form. The RM will verify more thoroughly and re-inventory the records when spot checks reveal serious and frequent problems with the comprehensiveness and accuracy of the original inventory.

Chapter 3
Records Management

3–1. The Army Records Information Management System

a. Army Records Information Management System is a web-based IT system used for identifying, arranging, managing, storing, retrieving, and applying dispositions to Army record material. ARIMS is accessed via the Army website at https://www.arims.army.mil. ARIMS provides a suite of software tools for managing both electronic and hardcopy Army records and information that includes, the RRS–A, the Army Consolidated Records Schedule (ACRS), and the AEA. Access to the system and its tools is based on the role of the user. ARIMS technology supports Army recordkeeping methodology for effective records management. ARIMS provides a suite of web-based tools and applications to facilitate and improve the management of Army records. Some of these tools assist in identifying which mission related records should be maintained, how long the records should be kept, appropriate disposition instructions for each record, and the ability to produce on-demand printing of folder labels.

b. ARIMS also enables the transmission of electronic records to the AEA from within typical office automation applications such as Microsoft office (MS) products, spreadsheets, and so forth. Records sent to the AEA are stored in read-only mode and can be accessed from the ARIMS master index. The master index also contains information on hardcopy records physically stored in an RHA. RHAMs are provided the necessary tools to index hardcopy records and manage their physical location within the RHA.

c. ARIMS is managed and operated by the Information Technology Management office and RMD and is available for use to all registered users. To use most of the records management features of ARIMS, a user must be registered in ARIMS. Registered users log into ARIMS with their valid common access card. Non-registered users can access some ARIMS features, such as the RRS–A and several links located on the ARIMS homepage (see ARIMS and the ARIMS User Guide for more detailed information).

3–2. The Records Retention Schedule-Army

a. Record information will be identified in ARIMS according to the RRS–A. The RRS–A is the records retention schedule approved by NARA and the only legal authority for destroying non-permanent Army information. For a comprehensive listing of NARA approved record disposition schedules, see https://www.archives.gov/records-mgmt/rcs/schedules/list-all-record-groups. The RRS–A provides life cycle management instructions for the systematic identification, maintenance, storage, access, retrieval, retirement, and destruction or permanent preservation of Army information recorded on any medium (such as electronic, paper, and microforms).

b. The RRS–A focuses on management of temporary and permanent records. It addresses only the record copy of information; all other copies of the same information may be destroyed when no longer needed for business, not to exceed the time the record copy is kept.

c. Records are identified according to the primary directive that prescribes the records be created, maintained, and used. The RRS–A record titles are determined by the proponents of the prescribing directives and provide an overall identification of the categories and types of records needed to support the business processes of those functional areas.

d. An RN associated with each record title serves as an additional identifier for records personnel and RHA staff use in performing records management functions. RNs correspond to the number of the directive prescribing the creation and maintenance of that particular record.

(1) In the absence of an AR, the RN may be based on a DA pamphlet, engineering regulation, or some other directive.

(2) If no directive can be pinpointed, the RN is based on the functional category number under which the program falls (for example, 25 for information management and 40 for medical).

(3) When a prescribing directive is rescinded, the associated RNs are coded “Rescinded.” Existing records continue to be maintained and disposed of as originally scheduled; however, new records may not be maintained under a rescinded disposition.

(4) If a prescribing directive is superseded by another directive—

(a) All associated RNs that remain valid are changed to reflect the new prescribing directive. The superseded RNs are coded “Superseded” in ARIMS and a pointer is added to each original RN. For example, RN 37–49b (Allocations) was superseded, so a pointer in ARIMS states “Superseded, use RN 37–1a.” All labels will be updated to reflect the new RN and disposition.

(b) All associated RNs that are not included in the new prescribing directive will be rescinded. Existing records continue to be maintained and disposed of as originally scheduled. New records may not be maintained under a rescinded disposition. See figure 3–1 for an example of a rescinded label.

(c) An alpha or alphanumeric suffix is added to the RN to distinguish several records prescribed by a single directive and separate between differing agency and or office responsibility levels when more than one disposition instruction is needed. For example, records prescribed by AR 600–20 are identified by RNs 600–20a1, 600–20a2, and 600–20b (see table 3–1).

(d) The RNs for office administrative housekeeping files are combined under the administrative category and numbered 1a through 1oo. Housekeeping files are the records created because an office exists and not why an office exists; they do not relate to the functions or mission of an office.

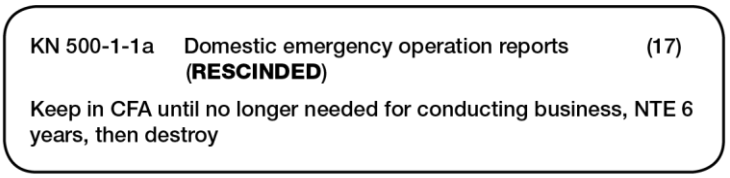


Figure 3–1. Label for a rescinded record number

Table 3–1
Relationship Between Prescribing Directives and Record Numbers—Example

Record number	Record titles
600–20a1	EO reports–Office with Armywide responsibility
600-20a2	EO reports–Table of organization and equipment units and other offices
600-20b	EO surveys
600-20e	Pregnancy and Family care
60-20f	Accommodation of religious practices

(e) All records are categorized as either—

1. *Short-term.* The records have no value beyond the business process.

2. *Long-term.* The records have value beyond the business process, such as for historical value, lessons learned, research purposes, or rights and interests of the Federal Government or of persons affected by U.S. Government activities and including those records having permanent retention.

(f) Disposition instructions are coded and have an initial letter “K” for keep or “T” for transfer, followed by an “E” for event when applicable. The last part of the code is a number representing the retention period or the letter “P” for permanent retention. See table 3–2 for examples of disposition codes and their meanings.

Table 3–2
Examples of Disposition Codes and Their Meanings—Continued

Code	Meaning
K	Along with a retention period means, the record must be kept for the time period specified before it can be destroyed (example: K3).
KE	Along with a retention period means the disposition is event driven and the record must be kept until the event occurs plus the specified time after the event before it can be destroyed (example: KE3).
KN	Used when a specific time period is not known. Records are kept until no longer needed for conducting business, but no longer than 6 years.
KEN	Used when a specific time period is not known and the disposition is event driven. Records are kept until the event occurs and then until no longer needed for conducting business, but not longer than 6 years after the event.
T	Used for retention periods longer than 7 years. Records are retired to the RHA, AEA, or other location as specified in the disposition instruction, when no longer needed for conducting business (for example, T15).
TE	Used with retention periods longer than 7 years and which have dispositions that are event driven. Records must be kept until an event occurs and until no longer needed for conducting business before they are retired to the RHA, AEA, and/or other location as specified in the disposition instruction (for example, TE30).
TP and TEP	Records with permanent retention periods. Records are retired to the RHA or AEA when no longer needed for conducting business or after an event occurs.
U	Records that have not been formally appraised by NARA are “unscheduled” records and are coded with a “U.” They will be retained in the CFA as permanent records until disposition instructions are published and the approved disposition instructions applied.

(g) All “K” codes apply to short-term records kept according to the business process until no longer needed (or until no longer needed for business after an event occurs) not to exceed the authorized disposition; “T” codes apply to long-term (retentions over 6 years) and permanent records.

(h) The retention and disposition of “K” records are based on the period of time the creating office needs to keep such records to meet business needs. Once that period of time is met, the records should be destroyed. These records should not be kept longer than their authorized disposition or the authorized length of time after an event occurs.

(i) The retention and disposition of “T” records are applied by the servicing RHA, AEA, or, in the case of organizations such as HQDA staff elements and any organization not residing on an installation, by the organization's RMO. Once the disposition for “T” records is established, the precise holding period for those records is calculated and applied to the records according to the instructions in the RRS–A.

(j) Records that have not been formally appraised by NARA are “unscheduled” records and are coded with a “U.” They will be retained in the CFA as permanent records until disposition instructions are published and the approved disposition instructions applied.

(k) There is a “general correspondence” RN within each record series. General correspondence RNs do not contain alpha suffixes but are further divided between “ACTION” and “NONACTION” correspondence.

3–3. The Army Consolidated Records Schedule

The Army Consolidated Records Schedule (ACRS) is a large aggregation schedule crosswalk in ARIMS. RNs will be categorized and arranged according to the ACRS. All records document specific actions taken in support of a primary function. Every office creates and maintains record information in the process of performing administrative and mission functions.

a. Within each subseries the RNs are grouped into three retention periods:

(1) *0–6 years.* Short-term records that have minimal value beyond the business process.

(2) *6+ years.* Long-term records that have value beyond the business process.

(3) *Permanent.* Permanent records will ultimately be transferred to NARA.

b. ACRS is based on 11 functional series plus one special use series (CONOPS) which correspond to the Army’s primary lines of business. Each series contain several functionally related subseries

containing unique RNs. The entire inventory of RNs is identified within the ACRS crosswalk (see ARIMS for the Record Series Crosswalk).

c. See chapter 13 for additional information on CONOPS record series.

Chapter 4
Managing Electronic Records

4–1. Electronic records

Office of Management and Budget (OMB)/NARA Memorandum M–19–21 requires that Federal agencies must manage all records in an electronic format to the fullest extent possible and must close agency operated records storage facilities. To comply with OMB and NARA requirements, all Army activities must transition to electronic records.

a. The criteria for identifying official records apply to the records information regardless of media. Electronically recorded information created or received by an organization or in connection with the transaction of business and serve as evidence of organization activities because of the value of the information they contain are Federal records.

(1) Recorded information within the Army may be created, manipulated, communicated, or stored in digital or electronic format. NARA approved disposition instructions apply to all Army records, regardless of the medium upon which it is recorded. To protect the rights and interests of the Army and its members, keep costs to a minimum, and serve the study of history, storage media for long-term records must be selected to best serve the operational needs of the Army and meet statutory scheduling and NARA storage requirements (see 36 CFR).

(2) Electronic records require the same levels of protection as any other media. Proper management provides for economic, efficient, and reliable maintenance, retrieval, preservation, storage, and applied disposition of the information. All personnel must comply with the NARA approved records schedules when disposing of or purging media that stores the only copy or the official copy of the record.

b. Electronic recordkeeping involves the use of IT to create, store, retrieve, use, and retire or dispose of digitally recorded information. All electronic information generated by or contained in an information system or other IT source, created or received during the conduct of business/electronic commerce, must be preserved according to a records retention schedule. This includes record information contained in information systems, command or installation unique systems, email systems, systems maintained in the office environment, web files, collaborative sites, instant messaging, text messaging, social media sites, and through the use of cloud-based services or storage solutions. The procedures for identifying and managing electronic records should be determined as early as possible in the life cycle of a system or initiative.

c. Official channels of communication.

(1) Official email, text messages, and similar Army-approved means of communication are official records when they are created or received in the transaction of business or mission and retained as evidence of official policies, actions, decisions, or transactions. Official messaging accounts will be used to conduct official Army communication.

(2) In the absence of official communication channels or when other appropriate circumstances exist, use of non-official electronic messaging accounts may be warranted.

(3) In accordance with DoDI 5015.02 and 44 USC 2911, record information sent and/or received using an unofficial electronic messaging account will be copy furnished to the official electronic messaging account no later than 20 days after the original creation/transmission of the record information. Adverse actions in the case of intentional violations can be found in 44 USC 2911.

4–2. Electronic messages

a. Electronic messages should accurately reflect the purpose of intended communications, decisions, and completion of actions. In accordance with AR 25–400–2, electronic messages will be retained as records, which are evidence of an organization’s or an individual’s activities and business transactions; they should support the needs of the organization to which they relate and be accessible for accountability purposes. Preserved electronic message records should contain or be persistently lined to the content and the metadata necessary to document a transaction such that:

(1) The metadata, structured information that describes, explains, locates, or otherwise makes it easier to retrieve, use or manage information recourses necessary, to reduce (present) and make

understandable the content, context, uses, and structure of the message are maintained for as long as that message is retained.

(2) The logical and physical structure remains intact including the format and the relationships among the elements comprising the electronic message.

(3) The business context in which the message was created, received, and used is apparent within the record.

(4) Combining links and/or attached documents to form a compound electronic message.

(5) The hyperlinks remain intact and permit access to link the source to the designated content, document, object, or web pages.

(6) The integrity of a complex electronic message with multiple threads, embedded files, or digital objects is maintained to permit comparable presentation upon retrieval.

b. Components of electronic messages include—

(1) Address.

(2) Account.

(3) Subject.

(4) Conversational threads.

c. See table 4–1 for types of electronic messages.

Table 4–1
Types of electronic messages Continued

Electronic mail (email)	Allows the exchange of discrete electronic messages between user accounts. See paragraph 4–3 for additional information.
Forums and/or list servers or bulletin boards	Allows the posting of messages to a shared system, either through email or direct entry via the system's user interface. Messages are usually organized in a structured manner (for example, by topic or subject area).
Instant message (IM)	Multiple message streams run simultaneously. Filter(s) select messages for viewing, culling them by subscription, a mutual agreement of parties, or message content.
Short message services and/or texting	Short phrases, sentences, and/or paragraphs are exchanged by users in real-time mode. Like email, these messages differ in that they are associated with communications services routed via mobile phone networks.

4–3. Electronic mail

Email is the electronic transfer of information typically in the form of electronic messages, memoranda, and attachments from one party to another through a telecommunications system.

a. Email messages are official records when they are created or received in the transaction of business and retained as evidence of official policies, actions, decisions, or transactions.

(1) Examples of messages sent by email that typically are records, includes the following:

(a) Policies and directives.

(b) Correspondence or memorandum related to official business.

(c) Work schedules and assignments.

(d) Agendas and minutes of meeting

(e) Drafts of documents that are circulated for comment or approval.

(f) Any document that initiates, authorizes, or completes a business transaction.

(g) Final reports or recommendations.

(h) Information supporting or affecting decisions made in conduct of Government business.

(2) Some examples of messages that typically do not constitute records includes the following:

(a) Personal messages and announcements not related to official business.

(b) Announcements of social events, such as holiday celebrations

b. Official records communicated through email systems must be identified, managed, protected, and retained if needed for ongoing operations, audits, legal proceedings, research, or any other known purpose in accordance with AR 25–400–2, this pamphlet, and the RRS–A. Users should—

(1) Protect email messages, files, and records from unauthorized release to third parties in accordance with AR 25–400–2, AR 25–55, and AR 25–22.

(2) Remove personal messages from personal inboxes on a regular basis.

(3) Protect email messages from inadvertent loss or destruction by complying with backup requirements and record-keeping requirements of AR 25–400–2.

(4) Coordinate disposition of records with the organizations' RMO to ensure that retention requirements are met.

c. Any copies of records maintained on users' systems for reference purposes after transfer of the official copy may not be kept longer than the retention period approved for the record copy.

d. An email server is not a record repository and will not be used as such. In accordance with AR 25–400–2, ARIMS is the official repository for all electronic records, including emails, and will be uploaded through the BAT.

(1) Users can upload emails through the BAT by either directly saving the message as an .msg file or converting the email to a pdf. Saving or printing the email as a pdf is the preferred format.

(2) The BAT may be executed directly from ARIMS to set up electronic folders on a file system such as an individual drive, a shared drive, or a shared drive site. The BAT feature is the preferred means for retiring long-term temporary records into the AEA.

4–4. Imaged and/or digitized records

Imaging is the process of using a scanner to digitize and convert hardcopy documents to electronic bitmapped images. Imaging also refers to creating a duplicate of a hardcopy or computerized document onto a micrographic media, such as film or fiche. See paragraph 5–9 for more detailed information.

a. Digital imaging. Use indexing to enhance retrieval time and facilitate access to records for users searching from various perspectives (mission, research, and litigation). Construct the indexing scheme using organization defined metadata fields (such as project names or numbers, subject(s), originating office symbol, RNs) in addition to the mandatory record metadata components discussed in DoD 5015.02–STD. Establish quality control (QC) processes into the entire life cycle of the system, from document preparation (prior to digitization) through disposition. Most importantly, the functional proponent of the imaging system is responsible for the maintenance, recovery, quality, utility, and accessibility of the record information. See also 36 CFR 1236.

b. Microform media. Record copy microforms have been used for archival purposes and still reside within the Army's records holdings. Detailed instructions and requirements for the management, standards, storage, use, and disposition of microforms are available in 36 CFR 1238.

4–5. Journaling

Emails are captured utilizing a process known as journaling. Journaling automatically captures all email communications (both sent and received, to include attachments from ".mil" email addresses). These emails are managed and stored by the Defense Information Systems Agency (DISA) and U.S. Army Network Enterprise Technology Command (NETCOM).

4–6. Capstone journaling

The "Capstone" approach is used to preserve senior officials' emails. Senior Leader emails are automatically captured, managed, and preserved as permanent record information to support the Army's routine receipt of FOIA requests, congressional inquiries, and statutory compliance investigations.

a. Under the Capstone approach, the Army has identified top-level senior Army officials who, by virtue of their work, office, or position, are likely to create or receive permanently valuable Federal records. The identified senior officials are—

(1) All general officers (including Reserve Component general officers who are in permanent Title 10 billets).

(2) Career Senior Executive Service and/or Defense Intelligence Senior Executive Service.

(3) Non-Career Senior Executive Service and/or Defense Intelligence Senior Executive Service.

(4) The Sergeant Major of the Army.

(5) President appointed and/or Senate confirmed officials.

(6) Appointed Schedule C officials. These are non-competitive general schedule positions; the officials report directly to a political appointee.

b. Capstone emails of the identified senior officials will be maintained for a minimum of 15 years, at which time the records are eligible for transfer to NARA for permanent retention and historical preservation.

c. All emails will be managed by individual senders and recipients. Record emails must be captured, moved into an electronic recordkeeping system such as ARIMS AEA, and saved in files based on the organization's ORL. Ensure that email satisfies the legal definition of a record and is not deleted prior to the authorized destruction date.

4–7. Information systems or electronic collection

Information systems or electronic collections must also be managed and fall under the same recordkeeping requirements as other electronic records. An information system or electronic collection is defined as a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, transmission, display, disposition and dissemination of information in accordance with defined procedures, whether automated or manual.

4–8. Information system or electronic collection documentation

Documentation on information systems or electronic collections that produce, use, or store electronic records will be retained according to applicable technical bulletins and standards.

a. Program managers and information managers of information systems or electronic collections must ensure—

(1) Electronic records are accompanied by sufficient documentation guaranteeing the information is accessible and usable. Minimum documentation consists of identifying the software programs and operating systems used to create the documents. Program and system documentation must be maintained for as long as the records generated are kept.

(2) Documentation, to include a copy of the software code, for information systems or electronic collections containing or generating long-term records are transferred along with the related electronic records sent to the AEA, unless a prior transfer of the same information occurred, and no changes were made. However, a statement to that effect will be included with the subsequent transfers to ensure that the information may be accessed and used.

b. Documentation must—

(1) Adequately specify all technical characteristics necessary to read or process the records.

(2) Identify all inputs and outputs of the system.

(3) Provide an audit trail of changed or deleted information and the correct disposition of the information content and use.

(4) Define the contents of the files and records.

(5) Clearly state the purpose and functions of the system.

(6) Determine restrictions on system access and use.

4–9. Record information on shared drives

Shared drives are used to store and share content such as word processing documents, presentations, spreadsheets, scanned and photographic images and databases. They are not recordkeeping systems; however, through a combination of policies and procedures they can be made to meet the requirements in Part 1236, Title 36, Code of Federal Regulations (see 36 CFR 1236). In accordance with AR 25–400–2, RMOs must be involved with the planning for the drive and audit its use. A designated point of contact for the drive (such as the records coordinator) will be responsible for management of the content residing on the drive. Alternates may be needed to assist the primary point of contact.

a. Content on shared drives may include record and non-record items. Record material must be separate from non-record material and procedures should be established for the deletion of all non-record material.

b. Identification of the record copy, mandatory use of standardized easy-to-use naming conventions, and establishment of version control are critical requirements. Official records must be maintained in an organized fashion that facilitates search, retrieval, and the application of appropriate disposition instructions. For example, a file plan with levels of folders, sub-folders, and files should be developed.

c. Additional considerations focus on access to and the sensitivity of the content. RMOs in coordination with information officers and/or IT specialists should ensure the sensitivity of the content is addressed through prevention of unauthorized access. Additionally, RMOs should—

(1) Implement controls to ensure trustworthiness of the records and their metadata. Organize records and related dispositions when organizations change, merge, or cease to exist.

(2) Develop a migration plan to ensure long-term temporary and permanent records with their metadata remain technologically accessible throughout their life cycle.

d. Manage record information on shared or network drives which consists of declaring, capturing, organizing and preserving official records plus maintaining security, managing access and applying the authorized disposition.

4–10. Hardcopy records converted to an electronic format

Record Digitization (commonly referred to as scanning or imaging) uses technology to convert paper documents to electronic format. Record digitizing provides many benefits, such as reductions in physical storage space, productivity increases, and better customer service. 36 CFR 1225.24 allows agencies to apply previously approved disposition authorities for permanent hardcopy records to electronic versions of the records, with notification to NARA, instead of requiring that the records be rescheduled. Important imaging standards (that NARA accepts as archival formats) must be scanned at 300 dots per inch to allow optical character recognition conversion to text search. Use color scanning only when it has significant value of the document (for example, maps and color coding). The imaging process includes:

a. Preparation. Document preparation is the process of ensuring that documents are in the proper condition to move through the scanning process. Prepping includes separating documents from any folders and binders, removing staples and clips, and ensuring corners are smooth and unfolded prior to scanning. A separator sheet is often inserted between documents to allow the scanning software and users to indicate where one document ends, and another begins. Most scanning software also uses bar codes printed on these separator sheet to automate document indexing.

b. Indexing. Documents must be manually indexed when automated index point recognition is not available. Indexing involves data entry by a scan operator to distinguish one document from another. The desired data fields to be captured must be determined before indexing (that is, employee name field). Indexing is essential for data retrieval and file naming conventions.

c. Scanning. Scanning documents can be a simple process or involve multiple steps, depending on the size and complexity of an imaging operation.

(1) A desktop scanner can be used for small amounts of document imaging. This may only require placing a document in a feeder tray and clicking a desktop icon.

(2) The process for large departmental production scanning operations is more complex requiring high speed scanners coupled with document capture software. Capture software is used to profile the different document types. Document profiling occurs by creating a batch class in the software. The batch class indicates the type of document, whether all documents are single page or multipage, and the different software processing queues the documents will pass through.

d. Quality control. The last major step in the scanning process is QC. QC involves examining document images upon completion of the scanning and indexing process to ensure the image document is a true and accurate replication of the original paper document, and that all appropriate index data was assigned to the image.

e. Disposal. After imaging and QC is completed, original hardcopy documents may be destroyed.

(1) *Temporary records.* In accordance with 36 CFR Part 1236, agencies may destroy the paper records after verification of successful conversion.

(2) *Permanent records.* No approved digitalization standards as the date of publication has been approved by NARA.

4–11. Web pages

Web pages vary in content and sources. If the information contained and/or displayed on a web page qualifies as record material, then the owner or managing organization of that web page is responsible for ensuring the record information has a record copy identified and preserved according to the retention requirements in the Army records schedules.

a. Documentary materials. Documentary materials that commands accumulate in connection with the transaction of official business are Federal records. Since Army websites are used to carry out mission business, the related records meet this definition and like all other records must be managed and disposed of in accordance with Army disposition schedules. The schedule should cover web content records that document the information on the site itself, as well as website management and operations records, which provide the site's context and structure.

(1) Web content records include—

(a) Content pages that comprise the site, including the hypertext markup language.

(b) Records that specify a commands web policies and procedures by addressing such matters as how records are selected for the site and when and how they may be removed.

(c) Records documenting the use of copyrighted material on a site.

(d) Records relating to the software applications used to operate the site.

(2) Web management and operations records that provide context to the site includes the following:

(a) Website design records.

(b) Records that specify a commands web policies and procedures by addressing such matters as how records are selected for the site and when and how they may be removed.

(c) Records documenting the use of copyrighted material on a site.

(d) Records relating to the software applications used to operate the site.

(e) Records that document user access and when pages are placed on the site, updated, and/or removed.

(3) Web management records that provide structure related to the site includes:

(a) Site maps that show the directory structure into which content pages are organized.

(b) Commercial off-the-shelf software configuration files used to operate the site and establish its look and feel, including server environment configuration specifications.

b. Records management risks associated with a website. There are two basic records management risks associated with a website. If these risks are not mitigated, the Army may be unable to document and/or validate transactions that occurred via a web front end interface, or it may not be able to show what was on a site at a given point in time, who put materials onto the site and when they were modified or removed. As a result, program operations could be impaired, citizens' rights compromised, negative publicity might be generated among Army stakeholders, the media, and/or the public at large, and in some instances, the Army could be exposed to costly litigation. The two risks are:

(1) Failure to create records that are needed to ensure the site is trustworthy.

(2) Failure to maintain records for an adequate period of time.

c. Web snapshots. Business needs and the need to lessen risk determine whether or not such snapshots are warranted and their frequency. In determining whether or not snapshots should be taken, the command should also consider the frequency with which the information on a site changes. Other things being equal, the more frequent the site undergoes change, the more frequently snapshots should be taken.

d. Retention periods for web records. When determining retention periods, the command needs to assess how long the information is needed to satisfy business needs and mitigate risk, considering Government accountability and the protection of legal rights. In the case of web content that is available in other places in addition to the web, records would take on the same retention period and use the already in place schedule as the records disposition authority. In the case of information unique to the website, the web version would be the only recordkeeping copy and would require scheduling.

(1) In many cases, particularly where the risk is low, the web content and related site management and operation records should be assigned a retention period that allows disposal as soon as records are no longer needed to conduct agency business.

(2) In instances where risk levels are higher, web content and related web management and operations records would warrant retention for a period of time that exceeds the time needed to satisfy all business requirements in order to mitigate risk. The additional time needed should normally be no more than 3 to 5 years beyond the retention period mandated by business needs alone. The mitigation of risk may require an even longer retention period in select instances. See chapter 6 for additional information on scheduling web records.

4–12. Social media

a. Social media, when used in the conduct of Army business, may result in the creation of official record information and needs to be managed in compliance with records management laws, regulations, and policies. The Office of the Chief of Public Affairs posts a listing of authorized social media at https://www.army.mil/media/socialmedia/.

b. Commands, units, and other organizations will ensure records management guidance is included in social media policies and procedures. RAs and/or RMs should consult with functional proponents, web management staff, privacy staff, information security staff and IT staff on appropriate records management for each social media activity, platform, or system.

c. When social media content is determined to be official record material, disposition instructions must be applied in the

d. RRS–A and the records must be managed throughout their life cycle. If an appropriate retention does not exist, the records must be scheduled.

e. Comments or other postings that are inconsistent with an organization's policies may require removal from the platform. Retain removed content in accordance with NARA approved schedules.

f. Organizations need to understand their responsibilities and obligations when dealing with social media providers and third parties.

(1) Each organization is responsible for managing its records, whether they reside on a third-party social media platform or are housed within the organization. Even if a service provider stops providing their service or deletes information from an organization's account, or if the organization stops using a social media platform, the organization must fulfill its records management obligations.

(2) Organizations should include a records management clause when negotiating a Terms of Service Agreement or other contract vehicle with a service provider for social media services. NARA Bulletin 2014–02 (see https://www.archives.gov/records-mgmt/bulletins) provides a general clause that can be modified to fit the social media platform and specific organization records management needs when using a service provider.

(3) See DoDI 5400.17 and AR 360–1 for more information.

4–13. Cloud computing

a. Cloud computing is a technology that allows users to access and use shared data and computing services via the internet or a virtual private network. Users have access to resources without having to build infrastructure to support these resources within their own environments or networks. The cloud is also used extensively in social media applications, cloud-based email, and other web applications. There are three ways the Army can use cloud computing; these options are known as cloud computing service models.

(1) *Software as a service.* The Army uses applications running on a provider's cloud infrastructure via a web browser. For example, web-based email.

(2) *Platform as a service.* The Army deploys its applications onto the provider's cloud infrastructure. These applications are created using programming languages and tools supported by the provider. The Army retains control over the applications, while the provider manages and controls the cloud infrastructure including network servers, operating systems, and storage.

(3) *Infrastructure as a service.* Hardware infrastructure located in the cloud is used by the Army to deploy and run its software operating systems and applications. The hardware infrastructure can include storage, servers, and networks.

b. There are four ways cloud computing services are typically deployed, they are:

(1) *Private clouds.* Operated solely for one organization.

(2) *Community clouds.* Shared by several organizations with shared concerns.

(3) *Public clouds.* Owned by organizations selling cloud services that are made available to the general public or large industry groups.

(4) *Hybrid clouds.* Composed of two or more cloud services (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that allow for data and application portability. For example, system load-balancing between clouds for performance optimization known as cloud bursting.

c. There are records management challenges associated with cloud computing centers related to implementing and executing records disposition schedules. Specific issues include—

(1) Maintaining records in a manner that preserves their functionality and integrity throughout the record life cycle.

(2) Maintaining links between the records and their metadata.

(3) Preserving long-term records and pre-accessioning permanent records to NARA.

(4) Ensuring cloud service providers comply with records retention requirements such as the accessibility of records for litigation discovery and FOIA and/or Privacy Act (PA) or similar requests.

(5) Ensuring Army control of any deletion of records located in the provider's cloud.

(6) Planning for how continued record information preservation and access issues will be resolved in the event cloud service provider's business operations materially change or cease altogether.

d. In accordance with AR 25–400–2, RMOs must participate in the planning, development, deployment, and use of cloud computing solutions. Guidelines for creating standards and policies are available in NARA guidance. An agency has the responsibility for managing its records whether the records reside in a contracted environment or under agency physical custody.

e. Cloud services. Organizations that maintain official record information in cloud environments must ensure records are identified and the disposition applied under the RRS–A. In particular, long-term temporary and permanent records must retain their functionality and integrity throughout their life cycle. A general records management clause, which should be included in any contract, or similar agreement for cloud services is available in NARA Bulletin 2010–05 (see https://www.archives.gov/records-mgmt/bulletins). It can be modified to fit an organization's specific requirements.

4–14. Electronic discovery

a. Electronic discovery (e-discovery) is the litigation process of identifying and collecting electronically stored information that may potentially be significant and relevant to a particular civil lawsuit. Any information on government equipment or under government control, or for which the government has responsibility, including official record information and personal information, can be subject to litigation e-discovery actions.

b. E-discovery actions often involve searches over a variety of sources (for instance, hard drive, compact disk (CD), shared drive, and cloud storage). This may require extensive staff time, particularly if the material is maintained in a disorganized fashion, with few established constraints for capturing, identifying, maintaining, and disposing of the information. Without proper records management, the Government is at risk for incurring high costs, additional lawsuits, and adverse public perceptions.

c. Implementing best records management practices is a critical component in efficient and economical e-discovery.

(1) Clear disposition instructions must be issued and applied uniformly and consistently to Army record information.

(2) Standard records management practices such as maintaining record information along with its related metadata, cutting off active records regularly at the appropriate time and retiring records on schedule, purging duplicate copies and other non-record items, ensuring access limitations are enforced, plus the many other procedures discussed throughout this publication facilitate efficient, adequate e-discovery.

(3) Non-record information should be identified and maintained as transitory or "keep until no longer needed but not to exceed" a set time limit to establish the basis for its destruction.

d. After learning of a lawsuit or an event which is likely to trigger a lawsuit, in accordance with AR 25–400–2, RMOs must consult with their command legal advisors to develop plans for e-discovery and immediate suspension of all destruction actions of relevant information (record and non-record).

(1) An e-discovery search will be initiated by a request from legal staff for an e-discovery action which includes search procedure instructions containing key words and other search aids.

(2) RMOs (working with IT staff) will identify information responsive to the search request and list it on a manifest with a point of contact/file type/location/date. The information will be copied and provided to the initiating legal staff along with the manifest. The original responsive information remains with the office of record.

(3) Resumption of the suspended destruction actions will occur only with the concurrence of the command legal advisor.

e. RMOs, IT staff, and legal office should work together to develop control mechanisms over electronic holdings in order to respond to e-discovery actions in an efficient, comprehensive manner. To enhance the legal admissibility of electronic records, implement procedures that—

(1) Document that similar kinds of records generated and stored electronically are created by the same processes each time and have a standardized retrieval approach.

(2) Substantiate that security procedures prevent unauthorized addition, modification, or deletion of a record and ensure system protection against such problems as power interruptions.

(3) Identify the electronic media on which records are stored throughout their life cycles, the maximum time span that records remain on each storage medium and the NARA approved disposition of all records according to AR 25–400–2.

4–15. Labeling

Records will be identified clearly by electronic labeling, marking, designation, or other means of identification. RMOs and SharePoint POCs will make the necessary fields within SharePoint available to users to mark and manage records within each site.

a. Labeling electronic records. Labeling electronic records. Organizations will develop file naming conventions that are descriptive, consistent, and meaningful. File names will not contain any spaces and will contribute to a file path that contains no more than 255 characters in total length. The data elements will include:

(1) Access (Unclassified, CUI).
(2) Organization (office symbol).
(3) Content (Name of the document).
(4) Date (current date by day, month and year).
(5) Versions (version V1, V2, V3, or F for final document).
(6) File Extensions (such as .docx, .pdf, .xlsx).

b. External labels.

(1) Labels used on disks (for example, compact disc read-only memory (CD–ROM) and digital video disk (DVD)) should include the disposition code, RN(s)/titles, start and end dates, whether a PA SORN is applicable, software used to create the records and classification if classified.

(2) Labels on magnetic tape containers should include the volume/serial number, name of the program office sponsoring the data, and data set names. RNs/titles, start and end dates, whether a PA number is applicable, software used to create the records and classification if classified.

(3) Access restrictions should be included on any external label if applicable.

c. Internal labels.

(1) Internal labeling, document, file, and directory naming conventions should be easily understandable and standardized so authors and their colleagues or successors can find stored information and maintain and dispose of records in accordance with NARA approved schedules.

(2) Labeling, naming, and filing conventions should be simple. One method is to file like documents in the same directory.

(3) Indexing is another way to find electronic documents. When used, the system should require the document creator to indicate the name of the document, the addressee, the date, and the identifier of the location (disk, server, or other) on which it is stored.

(4) Any access restrictions should be controlled by the software application.

4–16. Use of optical media for preservation of permanent records

a. CD–ROM and DVD may be used to temporarily store permanent records that include fielded data files or text files for eventual preservation by NARA. Such records can be transferred to NARA as soon as they become inactive or whenever the organization cannot provide proper care and handling of the records. The organization's RMO must coordinate transfer actions of permanent records through RMD, who will further coordinate with NARA. The record information and media must comply with the technical and documentation requirements specified in 36 CFR 1235. For example, they must—

(1) Conform to the American National Standards Institute/National Information Standards Organization/International Standards Organization (ANSI/NISO/ISO) 9660 standard.

(2) Comply with the American Standard Code for Information Interchange (ASCII) standard.

(3) Comply with the ASCII character set and not be dependent on control characters or codes not defined in the ASCII character set.

(4) Not be compressed unless the software to decompress files is provided.

(5) Not be individually addressable.

b. When retiring permanent electronic records stored on CD–ROM, DVD, magnetic tape or other electronic storage media, the organization will coordinate with the RMD to determine which medium is appropriate for transfer of the records to NARA.

c. NARA will accept audio CDs and analog videodisks that typically contain photographs, provided they do not require interactive software or nonstandard equipment for viewing. Original photographs appraised as permanent and copied onto videodisks will be scheduled for transfer to NARA along with a copy of the videodisk.

d. Records stored on CD–ROM or DVD for transfer will be labeled and documented.

e. Organizations may use optical disk systems for storing and retrieving permanent and unscheduled records while the records remain in their legal custody. Approval to destroy the hardcopy source documents must be obtained from NARA. RMD will do the necessary coordination with NARA.

f. Permanent records on optical media other than on CD–ROM and DVD are not accepted by NARA. At the time of scheduled transfer, information must be copied to a medium currently acceptable by NARA.

g. To be accepted by NARA, files on CD–ROM and DVD must comply with the format and documentation requirements specified by the following:

(1) *Formats.* The organization must transfer to NARA electronic records in a format that is independent of specific hardware and/or software. The records must be written in ASCII or Extended Binary Coded Decimal Interchange with all control characters and other non-data characters removed. The records must not be compressed unless NARA has approved the transfer in the compressed form in advance. In such cases, NARA may require the organization to provide the software to decompress the records.

(a) Data files and databases. Data files and databases must be transferred to the National Archives as flat files or as rectangular tables (for example, as two-dimensional arrays, lists, or tables). All records within a file or table should have the same logical format. Each data element within a record should contain only one data value. A record should not contain nested repeating groups of data items. The file should not contain extraneous control characters, except record length indicators for variable length records, or marks delimiting a data element, field, record, or file. If records or data elements in different files need to be linked or combined, then each record must contain one or more data elements that constitute primary and/or foreign keys enabling valid linkages between the related records in separate files.

(b) Textual documents. Electronic textual documents must be transferred as plain ASCII files; however, such files may contain Standard Generalized Markup Language (SGML) tags or Extensible Markup Language tags.

(c) Digital geospatial data files. Digital spatial data files must be transferred to NARA in a format that complies with a non-proprietary published open standard maintained by or for a Federal, national, or international standards organization. Acceptable transfer formats include the Geography Markup Language (GML) as defined by the Open Geographic Information System Consortium.

(d) Other formats (portable document format, electronic mail, and scanned images). For the latest guidance on the current acceptable formats, go to https://www.archives.gov/records-mgmt/policy/transfer-guidance-tables.html.

(2) *Documentation.* Documentation adequate to identify, service, and interpret electronic records that have been designated for preservation by NARA must be transferred with the records. This documentation must include completed NA Form 14028 (Information System Description Form) or their equivalents. Organizations should submit required documentation in an electronic form that conforms to the provisions of this section.

(a) Data files. Documentation for data files and databases must include record layouts, data element definitions, and code translation tables (codebooks) for coded data. Data element definitions, codes used to represent data values and interpretations of these codes must match the actual format and codes as transferred.

(b) Digital geospatial data files. Documentation for digital geospatial data files may include metadata that conforms to the Federal Geographic Data Committee's Content Standards for Digital Geospatial Metadata, as specified in Executive Order 12906 of April 11, 1994 (3 CFR, 1995 Comp., p. 882).

(c) Documents containing Standard Generalized Markup Language tags. Documentation for electronic files containing textual documents with SGML tags must include a table for interpreting the SGML tags, when appropriate.

Chapter 5
Managing Records (Media Neutral)

5–1. Hardcopy records

Hardcopy records (legacy records created prior to 30 November 2020) are defined as any original document, paper copy, computer printout, or other media that exists as a physical object which is human readable without the use of a mechanical device. The term hardcopy itself infers that the object is touchable, viewable, and tangible. Its main purpose is to provide a record of data or information in a physical form that can be stored for safe keeping.

5–2. Records preparation before filing

a. Before filing a record, examine it to ensure all actions are complete and essential information is attached. If essential information is missing and cannot be located, annotate the record indicating what measures are being taken to obtain the information.

b. Remove envelopes, routing slips that bear no essential information, extra copies, and cover sheets, unless records are in suspense files or when placed in record containers pending completion of an action.

c. Assemble related documents with the most recent action on top. Staple hardcopy documents together when possible. Prong fasteners and binders may be used when there are too many papers for stapling or physical characteristics of the documents prohibit stapling.

5–3. Cross references

A records cross reference is filed under one RN to show the location of material filed elsewhere. Prepare a DA Form 1613 (Records Cross Reference) only when essential to retrieving information. They may be used when—

a. A document is related to more than one action.

b. A classified document has a direct relationship to unclassified material. Do not place classified information on cross reference forms filed in unclassified files.

c. A document with various dates relates functions to other sub-functions or actions.

d. A document has been changed from one RN to another RN.

5–4. Classified records

Classified electronic records higher than SECRET will be maintained per authorized disposition requirements and AR 380–5.

a. Classified electronic records (through SECRET) will be maintained in ARIMS–C.

b. Classified and unclassified records will be filed in separate containers, except when—

(1) The reference needs require both classified and unclassified documents be filed together.

(a) Files, folders, and similar groups of documents containing classified and/or sensitive information will be clearly marked as to the highest classification and/or sensitivity of information contained therein.

(b) The classification and/or sensitivity marking will be on the outside, front, back, top, and bottom of the file or folder. Attaching a document cover sheet to the outside of the file or folder is acceptable in satisfying this requirement. When cover sheets are used, they will not be attached when the files are in a secure storage container. When cover sheets are removed and the items are in secure storage, the files or folders must be marked to indicate the highest level of classified and/or sensitive information contained therein.

(c) The records or containers will be secured. Access to the area or containers should be monitored as if all contents are classified to preclude the inadvertent disclosure of the classified materials.

(2) Classified documents, both originally and derivatively (except those containing restricted data or formerly restricted data), will be marked on the face of the document with a “declassify on-line,” with instructions for the declassification of the information. Specific instructions for completing the “declassify on-line” are outlined in AR 380–5.

(3) The volume of classified material is small, and it is more advantageous to use empty space for unclassified material. Classified material must be separated from unclassified material with guide cards or by placement in separate drawers.

5–5. Suspense files

Suspense files are used as reminders that an action is required by a given date. The following are some examples of suspense files:

a. A note kept by an action officer to submit a report or to take some other action. The note would be destroyed after the report is submitted or the action is taken.

b. An outgoing communication filed by the date on which a reply is expected.

(1) When the reply is received, the communication is withdrawn, and the record copy is filed.

(2) Destroyed if it is an extra copy.

5–6. Labeling legacy records created prior to 30 November 2020

File labels for hardcopy records will be generated in ARIMS by using the "ORLs and Folders" tab in ARIMS. Labels may be altered by the preparer in any manner that best suits the business needs of an office.

a. All hardcopy labels will include:

(1) The disposition codes. (Note. ARIMS does not print the disposition codes by default; they will need to be added manually)

(2) ACRS record subseries number.

(3) RN and title and current year.

(4) Disposition instructions.

(5) PA: "Yes" or "NA" (as applicable). If "Yes," insert the PA SORN located under the RRS–A details index.

(6) Bar code (long-term and permanent records only).

(7) The location for those records not stored in the labeled folder or container. This includes, but not limited to, information stored in a system and not printed for record and hardcopy records stored in other physical locations for mission purposes.

b. When there are several folders, drawers, or other containers with records under the same category, only the first folder, drawer, or container will show all of the required label information; the remaining folders, drawers, or containers need only be identified by the RRS–A number and year of accumulation (where appropriate) plus name, number, or other feature identifying the contents. Labels may be placed anywhere on folders, disks, tapes, drawers, containers, and so forth, that is suitable and visible for easy identification and retrieval of records.

c. When written exceptions to disposition instructions are granted, include a reference to the document authorizing the exception on the label below the title line or following the disposition instruction. Exceptions to disposition instructions may be retained under "Records disposition standard exceptions," RN 25–400–2d, or filed directly with the records.

5–7. Micrographic records

Micrographic technology involves recording information on a microform by reducing and recording images photographically or by recording directly onto film using computer output microform (COM). The indexed images are located and retrieved via mechanical and/or computer means and viewed using a microfilm viewer which magnifies them on a display screen or prints them out on paper. Micrographic systems should be designed so the microform serves as the record copy, except when it is not practical or cost-effective.

5–8. X-ray film records

Most x-rays today are made and stored as digital files or digitized by scanning from film originals, however, legacy x-ray records from previous years may still be on file for reference in RHAs and/or FRCs.

a. Storing microforms and x-ray films. Storage conditions significantly influence rates of deterioration, proper climate control, and may extend the film's useful life. The black and white silver halide image created on film is vulnerable to the excessive heat, moisture, and harmful gases, such as sulfur dioxide and nitrogen oxides, often found in urban and suburban environments. The organic compounds of the photographic emulsion also become susceptible to fungal growth in storage areas where the relative humidity (RH) exceeds 60 percent.

(1) Nitrate-based film, manufactured from the 1910s to 1930s is highly flammable and akin to gun cotton. Nitrate film deteriorates as it ages, emitting an obnoxious odor, discolors to amber, and becomes sticky and brittle. The word nitrate is imprinted on the film. Nitrate film is combustible under extreme storage conditions, especially where temperatures exceed 100 degrees Fahrenheit, and the humidity is in the upper ranges. Safety concerns are paramount. Contact RMD for handling and specific disposition instructions if you locate and identify any legacy nitrate films.

(a) For short-term storage, remove from records storage areas and place in conditions that do not exceed 70 degrees Fahrenheit and 50 percent RH. Storage in a freezer or cold storage is highly recommended.

(b) Copy to polyester film and, after verification of the copy, destroy in accordance with applicable regulations governing the disposal of hazardous waste (see Environmental Protection Agency Hazardous Waste Code, D001, D003, and D0011).

(c) For long-term storage, store the film at 35 degrees Fahrenheit and 20 to 30 percent RH in accordance with requirements of the National Fire Protection Association 40, which describes building and fire safety specifications for the storage of nitrate film. Ventilation may be needed depending upon the quantity of stored film. Store separately from other types of photographic records as off-gassing can accelerate deterioration of nearby film in good condition.

(d) The packing and shipping of nitrate film are governed by Department of Transportation regulations 49 CFR 172.101, 172.504, 173.24, and 173.177.

(2) Acetate-based film, manufactured from the 1920s to mid-1960s. Manufactured as a safety film (the words are imprinted on the film's edge), acetate film is flame resistant. However, it deteriorates as it ages, emitting a vinegary odor derived from vapors of acetic acid; a phenomenon preservationists call the vinegar syndrome. Once deterioration begins, the chemical process becomes autocatalytic, perpetuating at a faster and faster rate. As the base shrinks, the emulsion starts to separate from the base in the form of cracks and channels and the film becomes brittle and eventually shrivels or buckles beyond use.

(a) Place in cool and dry storage conditions to slow down deterioration. Research shows that storage temperatures from 35 to 55 degrees Fahrenheit at 50 percent RH can extend degraded film's life from 15 to 75 years longer, depending on the state of deterioration of the film.

(b) Only American National Standards Institute (ANSI) cold storage recommendations for acetate film will ensure preservation for 100 years or more (ANSI/PIMA IT9.11).

(3) Polyester-based, mid-1950s to the present. The most stable base, polyester film tends to resist chemical and physical changes as it ages under varied storage conditions. The word safety is imprinted on the film's edge.

(a) Virtually all microforms and x-ray film in use today are polyester-based.

(b) Polyester film has excellent long-term storage characteristics that normally extend its longevity beyond records retention requirements.

(4) Other formats. Other film formats which include micrographic images like microfilm and aperture cards must also be stored under conditions that will ensure availability for their full retention period.

b. Disposition. See chapter 7 for disposition instructions.

c. Enclosures for x-ray films. See NARA website Title 36, Chapter XII, Subchapter B for additional requirements.

5–9. Visual information

Visual information products are managed under the provisions of AR 25–1 and DA Pam 25–91.

5–10. Cartographic and architectural records

a. Cartographic records are graphic representations drawn to scale of selected cultural and physical features of the surface of the earth and other planetary bodies. They include maps, charts, photomaps, orthophoto maps, atlases, cartograms, globes, and relief models. Related records are those that are integral to the map making process, such as field survey notes, geodetic controls, map history case files, source materials, indexes, and finding aids.

b. Architectural and engineering drawings, also known as design and construction drawings, are graphic records which depict the proposed and the actual construction of stationary structures, such as buildings, bridges, and canals, as well as movable objects, such as ships, aircraft, vehicles, weapons, machinery, and equipment. Closely related records, like indexes and written specifications, frequently accompany these drawings.

c. Cartographic and architectural records exist in various media formats and should be managed in accordance with the guidelines specified for that media type in this pamphlet. They should be disposed of in accordance with the applicable RRS–A retention schedules and disposition instructions.

d. Cartographic and architectural records require special storage and handling because of their diverse physical attributes.

(1) Avoid storing maps and drawings rolled or folded. NARA recommends placing maps and architectural drawings inside acid-free folders for added protection and storing them flat in shallow drawer or ‘flat-file’ cases. The FRCs are generally not equipped to handle flat storage of large format documents; therefore, maps and drawings must be rolled, never folded, for storage. For this reason, when feasible, transfer permanent cartographic and architectural records directly to NARA rather than to intermediate storage in an RHA or FRC.

(2) Do not laminate oversized records. Encapsulate old or fragile maps in clear, stable, archival quality acetate sleeves.

(3) Store large, heavy atlases and other bound volumes of maps or drawings flat. Storing the volumes upright strains their bindings. If a spine is weak or damaged, the binding can be removed, the pages deacidified and encapsulated, and the volume reassembled in post binders. Further information on preservation problems is available from NARA.

(4) Store aerial negative film rolls in inert plastic containers in an upright position on shelves with identification codes assigned to each roll of film affixed to the outside of the container.

(5) Always wear white cotton gloves when handling film to prevent skin oils from damaging the surface emulsion.

(6) Store film in a climate-controlled environment at constant temperature and humidity that meets NARA guidelines found in 36 CFR 1237.

Chapter 6
Scheduling Records

6–1. Records retention schedules

a. A records retention schedule provides mandatory instructions for what to do with records when they are no longer needed for current Government business. The instructions specify when—

(1) Records should be cut off and when eligible records are to be moved to an approved on or off-site storage area.

(2) Eligible temporary records must be destroyed or deleted.

(3) Permanent records are to be accessioned to NARA.

b. All organizations must schedule their records within 2 years of establishment and schedule the records of a new program within 1 year of its implementation (see 36 CFR 1225.22).

c. According to Section 3303, Title 44 United States Code (44 USC 3303), agencies are required to develop records schedules which covers all their records that are not covered by the GRS. The GRS is a records retention schedule issued by the Archivist of the United States that provides disposition instructions for records that are 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 records related to military pay and military personnel.

(3) Only applies to records.

d. If the proponent wants to apply a different retention period for any series of records included in the GRS, RMD (on behalf of the proponent) must submit a records schedule modification in Electronic Records Archives (ERA) to NARA providing justification for the requested deviation.

e. According to 44 USC 3309, some schedules (especially those containing records relating to financial management, claims, and other related matters), must also be approved by the General Accounting Office (GAO) before NARA will approve them.

6–2. Scheduling process

a. If Army personnel identify unscheduled records (records that cannot be filed under one of the existing RNs) they will request assistance through their servicing RMO who will work in coordination with RMD in establishing a new RN.

b. The RMD (working with the owner of the records and the proponent of the prescribing directive that caused these records to be created) initiates action to get the records scheduled. This involves reviewing the business process, determining how the records are used; the records location; legal, financial, and other rights involved; volumes; how long the records must be kept to meet business needs, statutory or regulatory needs; proposed description and disposition.

c. After all issues have been resolved between RMD, the owner of the records, the proponent of the prescribing directive and the proposed description and disposition have been developed, the draft schedule is staffed with the proponent who in turn staffs it internally with their servicing legal office to ensure the proposed retention period meets all legal requirements.

d. When all coordination has been finalized, the draft schedule is forwarded to the RMD approving official who submits it electronically to NARA in the ERA.

e. NARA's appraisal process requires an understanding of the agency's functions, business process, documentation practices, and record and information policies, procedures, and systems. NARA may need

to consult with organization officials and either see samples of the records or examine them at the agency or an FRC. The appraisal archivist prepares a draft appraisal report upon completion of the appraisal, and reviews and concurrences are obtained from internal stakeholders at NARA.

f. NARA is required by law to publish notice in the Federal Register of schedules proposing the disposal of unscheduled records or a reduction in the retention period of records already approved for disposal. These notices provide the public with the opportunity to request copies of pending schedules from NARA and provide comments. Notices of pending schedules are published at least monthly. Members of the public have 45 days from the date of publication to submit comments. The Federal Register stage is generally the lengthiest portion of the schedule review process.

g. After NARA and the agency resolve any issues arising from NARA review and Federal Register publication, the schedule is finalized, and a dossier is created. The dossier is reviewed by several managers in NARA's Office of the Chief Records Officer for the U.S. Government before being sent to the Archivist of the United States for approval. After the schedule is approved, NARA maintains the original (a permanent record) and posts a copy to the web. RMD is be notified by email and can obtain the approved or withdrawn information from the ERA system.

h. The complete scheduling process from receipt to final approval generally takes NARA approximately six months or less to process simple schedules that pertain to records that are clearly temporary and do not have legal rights implications. These timelines are subject to change based on the complexity of the schedule.

i. RMD updates ACRS and the RRS–A to reflect the approved retention periods and coordinates with the proponent for any withdrawn schedules.

6–3. Scheduling records in an automated information system or electronic collection

a. In accordance with 44 USC Chapters 21, 44 USC Chapter 29, 44 USC Chapter 31, and 33 and 36 CFR 1220.34(g), each Automated Information System (AIS) or electronic collection that creates or contains record information must be scheduled. RMD identifies electronic systems in the Army Portfolio Management System (APMS) which may contain records and requests that the proponent complete the DA Form 7796 (Automated Information System Questionnaire) to determine if an approved disposition authority is required.

b. APMS tracks IT investments and is used for Federal compliance reporting including records management functionality. A system is certified as being compliant with records scheduling requirements when RMD has determined the system—

(1) Does not contain records.

(2) Is covered under an existing approved schedule (General Records Schedule (GRS) or Agency Records Control Schedule (RCS) in the RRS–A).

(3) Contains records and a draft disposition schedule for the system has been submitted to NARA for approval.

c. Once RMD certifies the system in APMS, the status will change to green for compliance reporting purposes.

d. Status of non-compliant systems will remain red in APMS.

e. Establishing recordkeeping requirements for an information system or electronic collection requires (at a minimum):

(1) Full and accurate documentation of the system or collection.

(2) Functions supported by the system or collection.

(3) The operation, legal, audit, oversight, or historical requirements for the information.

(4) How the information will be used, accessed, and maintained on each medium to meet these differing requirements.

(5) The procedural controls employed to preserve the integrity of the data in the system.

(6) All components of an information system of records, such as input, output, master file (digital data stored in a variety of ways), and the related documentation.

f. Any information generated by or contained in an information system or electronic collection must be preserved according to the disposition instructions contained in the RRS–A. This includes information contained in Standard Army Management Information Systems (registered in APMS), command or installation unique systems, standalone systems maintained in the office environment (not registered in APMS), cloud-based systems, web-based systems (such as milSuite, MAX Survey, and SharePoint),

network drives and commercial applications (such as Microsoft Teams). (Note: Information in a commercial application must be moved to an Army owned environment when the project is complete.)

g. Information owned by agencies outside of the Army maintained in Army systems, must be managed in accordance with that agency's NARA approved disposition authority and a signed memorandum of agreement (MOA) provided by the outside agency. The MOA is required and authorizes the Army to manage non-Army information within the system or electronic collection in accordance with the approved authority.

h. In accordance with AR 25–400–2, functional proponents and information system or electronic collection owners must—

(1) Define electronic record information disposition instructions during each milestone in the life cycle management of the system in accordance with AR 25–1.

(2) Evaluate information systems or electronic collection to determine the record information needed for business purposes and validate the retention periods of that information according to the disposition instructions identified in the RRS–A. Any new, revised, or rescinded requirements will be coordinated with the RMO, who will notify RMD. The information needed to establish recordkeeping requirements and retention periods for records can also serve as a catalyst for answering many management questions that should be addressed when designing or updating an information system or electronic collection.

(a) What is the system's purpose? Does it serve different purposes for different users? Do the different purposes reflect different needs for retaining data?

(b) What inputs are needed and how long should they be retained? Are they needed for legal or audit purposes?

(c) How long does information need to be kept online? Are online retention requirements directly mapped onto unit records or data sets?

(d) If the organization no longer needs data online, does it need to be retained offline? For how long?

(e) What metadata will be captured to aid search, retrieval, identification, and life cycle maintenance of the record information?

(f) How will requirements for retention and disposition of data be integrated with system design and operations, for example, with update procedures, regular backup operations, transfer to AEA, and create history files, subset files, and public use data sets?

(g) How will output products such as reports be handled? Will they be maintained on the system or another location? For how long?

(h) Are multiple copies of the data needed? If so, in what media? In what locations? Do all media need to be maintained for the same length of time? What will happen to the different media, and when? How will the integrity and authority of the data be ensured?

(i) Is the information subject to the provisions of the PA? Does the information include personally identifiable information (PII)? How do PA and/or PII requirements for maintenance of timely, complete, relevant, and accurate information and limitation access affect the agency's estimate of how long data should be kept?

(j) Is the information in the system or electronic collection part of the agency's essential records program? If so, what provisions must be made to ensure availability of the information in emergency situations?

(k) Who is responsible for maintaining up-to-date, authoritative documentation of the system and the data it contains? Where will the documentation be maintained?

(l) Is there a comprehensive and clearly written migration plan in place to ensure periodic and timely migration of both the hardware/software and the record information? Does the migration plan ensure continued preservation of protection of and access to the record information in accordance with specific disposition instructions?

(m) Is the system in compliance with DoD 5015.02–STD?

(n) Determining the record information of an information system or electronic collection may be accomplished by reviewing the mission and functions statement of the office or offices supported by the system and evaluating its administrative, legal, or fiscal value.

(o) Documentation on all information systems or electronic collection that produce, use, or store electronic records will be kept current according to applicable technical bulletins and standards. This means, in accordance with AR 25–400–2, program managers and information managers must ensure—

1. All electronic records are accompanied by documentation sufficient to ensure that the information is accessible and usable. Minimum documentation consists of identifying the software programs and

operating systems used to create the documents to the extent that technical specification, file arrangement, contents, coding, and disposition requirements of the files can be determined. Program and system documentation must be maintained for as long as the related information is kept ensuring accessibility.

2. That documentation—

(a) To include a copy of the software program, for information systems or electronic collections containing or generating temporary records is retired along with the related electronic records sent to the AEA, unless a prior retirement of the same information occurred, and no changes were made. However, a statement to that effect will be included with the subsequent retirements to ensure that the information may be accessed and used.

(b) Specifies all technical characteristics necessary to read or process the records adequately.

(c) Identifies all inputs and outputs of the system.

(d) Provides an audit trail of changed or deleted information and the correct disposition of the information content and use.

(e) Defines the contents of the files and records.

(f) Clearly states the purpose(s) and function(s) of the system or electronic collection.

6–4. Scheduling web records

There are two options available for scheduling web records.

a. Option 1 single item schedule. This option would be to schedule web content records along with related records that pertain to site management and operations. This option would be appropriate if all the records related to the site warrant the same retention period to meet business needs and mitigate risks.

b. Option 2 multiple item schedule. Under this option, web content records and website management and operations records would be scheduled separately. This option would be appropriate if business needs and the mitigation of risk mandate different retention periods for the site content records and the management and operations records.

Chapter 7
Record Dispositions

7–1. Disposition

The final phase of the records life cycle is disposition. Records disposition includes transfer to the AEA and RHAs, retirement to FRCs, transfer from one agency to another, SAORM approved donations, accession of permanent records to NARA, and disposal of temporary records. 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.

7–2. Records disposal

The most important factor in disposing of record information is to match the technique to the media and the degree of protection required by the record information. Always coordinate with the organization's RA/RM, information assurance (IA) personnel and security manager for current requirements and to determine the most efficient and effective means of disposing or sanitizing temporary record information and/or the media upon which it is stored.

a. Classified records will be destroyed in accordance with AR 380–5.

b. Unclassified records will be destroyed in accordance with Title 36 Chapter XII, Subchapter B, Part 1226, Code of Federal Regulations, DoD Precious Metals Recovery Program, and DA Pam 25–2–8.

c. Records may be donated to an eligible person, organization, institution, corporation, or government if the donation is approved by the SAORM or the delegated authority. Process requests through local records management channels to RMD. Specify the name, email, and address of the records custodian, the name and address of the proposed recipient, and a complete description of the records retention schedule, associated record number, title and inclusive dates of the records.

d. For early disposal of records that are a threat to human life, health, or property—

(1) Contact local fire officials if they have nitrocellulose base film that emits a noxious odor, contains gas bubbles, or has retrograded into an acid powder and then notify RMD.

(2) Notify RMD to obtain authority for disposing records of other threat. Provide the RRS–A RN and title, description of records, volume, location, and nature of the menace. RMD will notify/obtain authority for disposal from NARA.

(3) Decisions on whether to dispose of or destroy records cannot be made by contractor personnel.

7–3. Applying disposition Instructions

Disposition is a comprehensive term that includes retention actions, such as the transfer of permanent records to NARA as well as destruction other Army records need to be distinguished from non-record materials and personal papers for disposition purposes. Non-record information requires only Army approval for disposition, and the individual owner determines the disposition of their personal files. Disposal of Federal records is only authorized when an agency has received an approved Disposition Authority signed by NARA. Retention periods and disposition instructions for RNs listed in the RRS–A have received NARA's approval, except for those marked as “Unscheduled” (Retain until disposition instructions are published). All unscheduled RNs listed in the RRS–A should have a working request for Records Disposition Authority under review at NARA. Submission of a request for Records Disposition Authority to NARA is restricted to the RMD.

7–4. Records value

All records have value to the organization creating or receiving them or for oversight by other agencies. Some records also have permanent value and warrant preservation by the National Archives after the organization no longer needs them to conduct regular current business.

a. Administrative value. All records that are necessary to conduct the organization's current business have administrative value. This value can be short-term or long-term depending on what the records document.

b. Fiscal value. Financial records (such as budget records, accounting records) have fiscal value. The retention of these records is usually based on a statutory requirement.

c. Legal valu e. Some records also have legal value. Examples of records with legal value include formal decisions and legal opinions; documents containing evidence of actions in particular cases, such as claims papers and legal dockets; and documents involving legal agreements, such as leases, titles, and contracts. The retention period for such records is usually based on regulations or statutes of limitation. Special concern for legal value applies only to temporary records, if permanent, they will always be available to protect legal rights.

d. Historical value. Long-term and permanent records serve to document the history of the organization, including policies, decisions, events, and actions which provide context to the significance of the organization and the American experience.

7–5. Retention periods

Army organizations may recommend retention periods; however only NARA can determine and approve final disposition. NARA works with the Army to ensure that retention periods for temporary records are adequate, but not excessive, for Army needs. NARA also ensures that disposition instructions meet the requirements of other agencies having an interest in certain categories of Army records. For example, the Office of Personnel Management (OPM) in Civilian personnel records, and the GAO in program and financial records.

a. Permanent records. NARA designates records as permanent if they have sufficient historical or other value to warrant their continued preservation by the Government.

(1) All records that NARA designates as permanent must be transferred in accordance with approved schedules.

(2) Records may be held for a specific time in the AEA, an RHA and/or FRC pending retirement to NARA.

(3) When records are retired, the agency also transfers legal custody of the records. NARA takes conservation measures needed to preserve the records and also provides reference service, including service to the creating organization provided at no charge.

(4) Types of records normally appraised by NARA for permanent, or archival, retention are listed at https://www.archives.gov/records-mgmt/initiatives/appraisal.html.

b. Temporary records. All records not designated permanent are considered temporary, meaning at some fixed period of time they can be disposed of when that time is met. The period of time may range from several months to many years. Most Federal records are temporary.

7–6. Record cutoffs

Record cutoffs are needed before disposition instructions can be applied because retention periods usually begin with the cutoff. Cutoffs usually happen at regular intervals to permit disposal or transfer of records in complete blocks if they will be transferred outside the CFA. Normally, correspondence type records are cutoff at the end of the year (fiscal or calendar). Once a record has been cutoff, documents are no longer added to that period or year, and new folders are set up for the new sequence of documents. Case files are normally cutoff at the end of the year (fiscal or calendar) in which final action is taken.

7–7. Disposition instructions

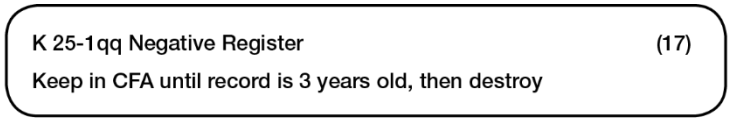
a. Disposition instructions for all Army record titles/RNs that have been approved by NARA are contained in the RRS–A. All Army records are managed and disposed of in accordance with the disposition instructions listed for each RN.

b. There are three types of disposition instructions in ARIMS based on time, event, and time plus event.

(1) Time disposition cuts a record off at the end of the month for a 30-day disposition, at the end of the quarter for a 3-month disposition, semiannually for a 6-month disposition, or at the end of the year for a 1-year or more disposition. Then the retention time period starts. Records are held for the specified period, and then destroyed (see fig 7–1).

(2) Event disposition records are destroyed upon or immediately after a specified event occurs. There is no waiting period, as with time disposition. For example, consider the disposition instruction, “Event is after all corrections have been made and processed. Keep in the CFA until event occurs, then destroy.” When all corrections have been made and processed, the record can be deleted or destroyed (see fig 7–2).

(3) Combination time + event disposition records are disposed of a certain period of time after an event takes place. For example, destroy 3 years after case is closed. This disposition requires management of the record in its active state (prior to the event occurring) and the inactive state (after the event occurs). This requires the creation of two folder labels; one for active which would be created upon creation/receipt of the record, with the second label created upon occurrence of the event. The active folder label does not show a year because the retention period does not begin until the event occurs and there would be no purpose for it. The inactive folder label would show a year because the information is now in the time phase. The occurrence of the event starts the time phase and triggers the inactive state (see fig 7–3).



Time Disposition

Figure 7–1. Time disposition

KEN 25-30zz Office copier files (17)

Keep until NLN after disposal of equipment, NTE 6 years, then destroy.

Event Disposition

Figure 7–2. Event disposition

TP 34-1d1 International military standardization agreements – Office of Army proponent or custodian of the agreement (**ACTIVE**) (17)

PIF on supersession, cancellation, or termination of the agreement

TP 34-1d1 International military standardization agreements – Office of Army proponent or custodian of the agreement (**INACTIVE**) (17)

Keep in CFA until no longer needed for conducting business, NTE 3 years, then transfer to RHA/AEA

Time + Event

Figure 7–3. Time + event disposition

c. New disposition instructions for temporary long-term records should propose specific retention periods and should contain the term destroy or delete if referring to electronic media such as magnetic media (hard disk, tapes, or diskette) and optical media (laser disk, optical disk, optical card, tapes, CD, and DVD). Retention periods can be expressed in two ways—

(1) A fixed period after records in the series or system are created (for example, destroy when 10 years old).

(2) A fixed period after an event occurs (for example, destroy 10 years after revision). In some cases, the retention periods may be based on the likelihood that two different future events may affect a series of records. For example, an event may be "when property is sold or vacated, whichever is later" or another might be "when superseded by revised plan or when building is sold, whichever is sooner."

d. Records proposed as permanent need to include the following elements in the instructions; the word permanent, cutoff instructions, instructions for retiring to the AEA, or FRC and instructions for transferring the records to NARA, including both timing and blocking. The timing should be based on the length of time after the cutoff, although it may be expressed either as "transfer xx years after cutoff" or "transfer when xx years old." Blocking means the chronological grouping of records consisting of one or more segments of cutoff records that belong to the same series and are dealt with as a unit for purposes of their efficient transfer (for example, transfer in 5–year blocks).

7–8. Records created during mobilization

A distinction is made between retention periods in peacetime and during mobilization or the conduct of military operations. Many records that may be considered temporary during peacetime, take on a permanent retention when they are created during conflicts or wartime (see chap 13 for additional instructions).

7–9. Changes to record descriptions, record numbers, and disposition instructions

Sometimes retention periods, record descriptions, and RNs for Army records change due to statutory, legal, financial and administrative requirements; program changes; or because prescribing directives are rescinded or superseded.

a. Email recommended changes to record description and disposition instructions to RMD at usarmy.belvoir.hqda-rmda.mbx.rmda-certification@army.mil stating the rationale or justification for the recommended change. The proposed change can be sent on a DA Form 2028 (Recommended Changes to Publications and Blank Forms).

b. When a prescribing directive is rescinded or superseded, the proponent should notify RMD and provide disposition guidance for the RNs required by that directive. Generally, guidance is to rescind the RN if the directive is rescinded or change the numbers to reflect the new prescribing directive if the directive is superseded by another directive. For either option, the proponent's concurrence is required.

c. When a change increases the retention period, the new retention period will be used for all records, both active and inactive under that RN, no matter when the records were created or where they are maintained.

d. When a change decreases the retention period or changes from a permanent to a temporary period (for example, from permanent to 15 years), the new retention period will be used for all current year records except those existing permanent records will remain as permanent. Efficiency and cost effectiveness should be considered when applying a decreased retention period to inactive records (prior years). For example, if the volume of records involved would require a considerable amount of time and effort to sort through and dispose of and storage space is not an issue, the records should be kept for the longer (former) retention period. If space is an issue or record volume is low, inactive records will be disposed of using the shorter (new) retention period.

7–10. Deviations from disposition instructions

The Archivist of the United States must approve deviations from disposition instruction in the RRS–A. Requests for deviations will be sent through RMO channels after evaluation at the HQDA principal official, ACOM, ASCC, or DRU level to determine whether an exception is warranted or if the disposition instructions should be changed. Valid requests will be forwarded through the proponent of the prescribing directive to RMD and will include the following:

a. The record title, RN, and brief description of the records involved.

b. Justification for the deviation, consisting of evidence of specific need for the records and information on their continuing administrative, legal, or fiscal value to the Government.

c. The physical location of the records, including information on whether the records were (or will be) transferred to a FRC or to the AEA.

7–11. Disposition of records on change of status

a. When there is a change of status in a unit or organization, the records disposition of instruction may change as well. The term change of status refers to—

(1) Redesignation or reorganization.
(2) Transfer of functions.
(3) Discontinuance.
(4) Movement.

b. See table 7–1 for the disposition of records rules.

Table 7–1
Disposition of Records on "Change of Status" Continued

Redesignation/ reorganization	Realign the ORL to the organization using the reorganize ORLs feature in ARIMS and continue records retention, cutoff, disposition until business process is reassessed and all record numbers in the ORL are reviewed/updated.	
Transfer of functions	Send current records relating to the transferred functions to the gaining organization. Transfer or retire inactive records to the AEA. A list of the records transferred to the gaining organization and a copy of the Standard Form (SF) 135 (Records Transmittal and Receipt) listing the inactive records transferred or retired, will be given to the RMOs of the gaining organization and the next higher headquarters.	
Discontinuance	Transfer records not eligible for immediate disposal to the AEA. Send a copy of the SF 135 listing the records transferred or retired to the RMO in the next higher headquarters.	
Movement	Continental United States (CONUS) to outside	Immediately prior to overseas movement, destroy records eligible for destruction; prepare records prescribed for retention by the unit for shipment; and transfer other records promptly to the AEA.

Table 7–1
Disposition of Records on "Change of Status"—Continued

	continental United States (OCONUS)	
	OCONUS to CONUS	With personnel and equipment: Records will be transferred to the AEA; records found essential to operation of the unit in CONUS may be requested from the AEA.
	OCONUS to CONUS	With personnel and equipment: Records will go with the unit.
	CONUS to CONUS	Without personnel and equipment: Cut-off records as of the date of the transfer and immediately send to the AEA of the losing installation. Records essential to the operation of the unit, at its new location, may be obtained upon request to the losing installation.
	CONUS to CONUS	With personnel and equipment: Records will go with the unit.
	OCONUS to OCONUS	Current records will go with the unit. Transfer other records not required for future actions to the AEA.

7–12. 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 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.

e. Cases of accidental loss or destruction of records by fire or other cause, the custodian of the records will—

(1) Notify the RA or RM as soon as possible when such a loss occurs. The RA or RM will immediately notify RMD.

(2) Reconstruct as much of the lost or destroyed records as possible. A series can often be reconstructed from other copies of the information maintained in other elements of the Army. Reconstructed records should be documented with cross-referenced material to aid in identifying their original content.

(3) Provide identification of the records that cannot be reconstructed to the RA or RM for recording on Standard Form (SF) 135 (Records Transmittal and Receipt) at the time that records of the same period are transferred to the RHA or AEA. A SF 135 will be forwarded to the FRC through ARCIS by RHA or AEA (RMD) personnel at the time the records would have been retired if they still existed.

f. The maximum penalty for the willful and unlawful destruction, damaging, defacing, or removal of Federal records is a fine, imprisonment, or both (see 18 USC 641 and 18 USC 2071). In accordance with 36 CFR 1230, removal means selling, donating, loaning, transferring, stealing, or otherwise allowing a record to leave the custody of the Army without the permission of the Archivist of the United States (see 18 USC 2071).

7–13. Destruction as result of international armed conflict or threatened war

a. During an international armed conflict between the United States and any other nations or when hostile action by a foreign power appears imminent, records in the custody of the Army outside the territorial limits of the CONUS may be destroyed if it is determined that:

(1) Their retention would be prejudicial to the interest of the United States.

(2) They occupy space urgently needed for military purposes and are without sufficient administrative, legal, research, or other value (see 44 USC 3311).

b. Within 6 months of the destruction, forward the following information through RMO channels to the RMD for notification to NARA: description of the records, when and where the destruction was accomplished, and the method of destruction.

7–14. Notification of pending disposition

RMOs are responsible for notifying organizations when records reach the end of their life cycle and are ready for disposition by AEA, an RHA, or an FRC. The organization will provide signed approval to destroy the identified records prior to their destruction or justification for their non-concurrence to destroy. Specifically, RMOs will use the ARIMS "Disposition Report" function located under the "Reports" tab semi-annually to identify which records in the AEA and RHAs are eligible for destruction at the end of the fiscal year (FY) or calendar year (CY) and initiate the approval process. FRCs notify RMD who forwards the notices of records eligible for destruction to the appropriate Army organization RMO.

a. Records in the AEA and RHAs. RAs, RMs, or RHAMs will—

(1) Identify records eligible for destruction by using the ARIMS "Disposition Report" function and complete an NA Form 13001 (Notice of Eligibility for Disposal). The SF 135 used to transfer the records and the records schedule may be useful in providing a description of the records.

(2) Send the NA Form 13001 and an explanatory memo to the commander, director, or agency head of the organization having custody of the records eligible for destruction.

(3) Ensure a response including the NA Form 13001 signed by the commander, director or agency head or a signed justification for non-concurrence based on audit, legal, or other pertinent issues is obtained within 30 days and retained with program files.

(4) Use the "Request Destruction of Records" function located under the "Manage" tab to—

(a) Approve disposal of the eligible records. The RHAM will ensure the records approved for disposal and stored in the RHA are destroyed.

(b) Request continued retention if a written justification was provided.

(5) If warranted, use the "Request Records" function located under the "Manage" tab to request their return to the originating/gaining organization or its higher proponent organization.

b. Records in FRCs. Organizations are notified of the pending disposition of records with one of three forms—

(1) NA Form 13001 (Notice of Eligibility for Disposal) is sent 90 days before scheduled destruction to RMD who in turn sends it to the HQDA principal officials, ACOMs, ASCCs, or DRUs of the organization having custody of the records. Upon return of the disposal notice and a positive concurrence, or a signed statement that destruction is authorized, the records will be destroyed as scheduled. Since the records center must receive a written, positive concurrence before disposition takes place, a timely review of the disposal notice is required. If the organization does not concur with the disposal, a signed and dated justification for non-concurrence must be returned to RMD.

(2) NA Form 13000 (Agency Review for Contingent Disposal) is sent during October of each year to RMD who in turn forwards it to the appropriate HQDA principal officials, ACOMs, ASCCs, or DRUs. The organization must sign and return the form, indicating approval of the disposal before the records can be destroyed. If the records cannot be destroyed, the form will be signed, dated, and returned, indicating a new review date. Please reply promptly; if a response is not received within 90 days, the records center will be instructed to return the records to owner (see 36 CFR 1228.164(b)). RAs, RMs, RCs, and/or RHAMs should complete the DA Form 7914 (Destruction Certificate) certifying that the records listed on the certificate have been retained in accordance with the assigned ARIMS RRS–A schedule, required audits have been completed and there are no known ongoing litigation holds and/or freezes or investigations involved with these records.

(3) A partially completed Agreement to Transfer Records to NARA of the United States, SF 258 (Agreement to Transfer Records to the National Archives of the United States), is forwarded to RMD when permanent records stored at an FRC are scheduled for transfer into NARA. The SF 258 is used to document the change in legal custody of the records and to state terms of the transfer.

Chapter 8
Records Transfer and Retirement

8–1. General

Short-term records (1+ year) are managed and destroyed within the CFA and/or AEA. Long-term and permanent records are retired to a Federal Records Center (FRC) and/or the AEA, when they are no longer needed for day-to-day operations within the office.

8–2. When to retire

a. Records should be retired in accordance with NARA approved schedules.

b. Long-term temporary records should be transferred as soon as all action on them are complete. An action is complete when all issues and/or decisions have been made and no further action is required. A copy may be kept within the CFA for reference purposes; however, the reference copy will be deleted as soon as it is no longer needed for reference and in no case will it be kept longer than the record copy.

c. If the record copy needs to be maintained on site past the time the action has been completed, an email request for exception will be forwarded to the RMD including a point of contact (name, address, email address, and telephone number) for coordinating and completing the information that will be entered to the master index of records in ARIMS.

8–3. Retiring electronic records

a. Electronic long-term records must be managed as described in chapter 4. Paragraph 4–8 provides requirements for information systems or electronic collections, emphasizing the need for authoritative, up-to-date system documentation, compliance with DoD 5015.02–STD to ensure access and retrieve ability of the electronic records throughout their entire life cycle.

b. Whether record information is preserved in online, nearline, offline (Online storage is immediately available for input/output. Nearline storage is not immediately available but can be made online quickly without human intervention. Offline storage is not immediately available and requires some human intervention to become online.) or cloud storage, the functional proponent is responsible for management of its record information and must comply with these requirements.

c. Originating offices or units can transfer long-term electronic records to the AEA as soon as they are complete. This is accomplished using the BAT tool.

8–4. Retiring legacy hardcopy records prior to 31 December 2022

Offices will provide hardcopy long-term records to activity RMOs, upon request. Installation RMOs will periodically visit tenant units and installation staff organizations while in garrison to collect these records; deployed units will transmit these records monthly and at the end of the deployment.

a. Temporary records with retention period beyond 31 December 2022 will be transferred to a FRC.

b. Permanent records with a retention beyond 31 December 2022 will be transferred to a FRC where they will be managed until their custody is transferred to NARA according to the specific time stated in the disposition instructions.

8–5. Preparing hardcopy records for transfer or retirement

a. Organization and installation RMs or designated coordinators will organize, pack, receipt, and send records to the servicing RHA and/or FRC on a periodic basis. When an office has records to retire that are not part of a scheduled pickup, the organization's records official should be notified.

b. If RMs are not available to an organization to pack and transfer the records, the office that created the records is responsible for doing so.

c. Records will be retired to a FRC using the electronic SF 135 (Records Transmittal and Receipt) through Archives and Records Centers Information System (ARCIS). The SF 135—

(1) Is the transmittal and tracking document for records sent out of the office files area.

(2) Accompanies the records until they are destroyed or accessioned into NARA.

(3) May be used to transfer records to a RHA that will be destroyed soon or retired to an FRC as soon as possible.

(4) Serves as a receiving document, receipt for the creating office, an inventory tool showing where the records are located in the RHA (if an automated tool is not used), an input source for the master index, and to retire the records to an FRC.

(5) Copies will be retained by all offices concerned during the life cycle of the pertinent records.

d. Prior to packing the records, the files should be reviewed and purged of unnecessary documents such as duplicates and non-records.

e. Do not transfer or retire records that are subject to the PA unless they are covered by a SORN listed on the Defense Privacy and Civil Liberties Office website. Cite the SORN number on the SF 135. If the SORN associated with an RN is incorrect, or newly created recordkeeping requirements lack PA protection, promptly notify your organization’s privacy official or the ARMD’s Privacy Office.

f. The originating office or unit remains the legal custodian of the records even when they are retired to an FRC and will provide input or review of the SF 135s when requested to enable retrieval of these records if needed at a future date. For example, if the originating office receives a FOIA request for records that were transferred to an RHA or retired to an FRC, that office is responsible for locating the records and retrieving them for review.

g. RMs or designated coordinators will consolidate records transfers and retirements from the different offices within their organizations. Installation RMs will consolidate records transfers and retirements from units and installation staff organizations while in garrison. Records retirements from deployed units will be handled as expeditiously as possible (see chap 13).

h. When submitting a Transfer request through ARCIS, ensure records under a litigation hold or freeze are properly identified with wording such as “Freeze Code XXX” in the “comments” field. Add these words only to boxes that contain frozen records. Records identified under a freeze will remain at the FRC until the freeze is lifted.

i. Returned and/or rejected transfer requests from NARA.

(1) When a transfer request is returned/rejected by NARA through ARCIS using the electronic version SF 135 (Records Transmittal and Receipt), the originating agency or command must correct the discrepancies. NARA will notify the approving official (normally the RA) of the agency and/or command with an explanation of errors found on the transfer request. The request may come through ARCIS and/or by email. Submitters must check ARCIS frequently for the status of the transfer request until it has been approved by NARA. Records officials (RA/RM) must work together to ensure all discrepancies are corrected and the transfer request is resubmitted to NARA through ARCIS.

(2) When transfer requests using the electronic version SF 258 (Agreement to Transfer Records to the National Archives) are returned and/or rejected through the ERA, NARA will change the transfer request status from proposed to draft status, indicating there is an issue with the request. NARA will provide the reason for the change in status. RMD will coordinate with the originating agency to correct the transfer request and resubmit to NARA through the ERA for approval.

j. All permanent records will be transferred to NARA per an approved NARA disposition instruction. This conforms with EO 13526 which requires that classified permanent records be reviewed for declassification at 25 years.

k. Permanent records are offered to NARA according to the time period specified in the disposition instructions for the specific records. Permanent records may only be offered to the National Archives by RMD, as the designated agency for the Office of the Administrative Assistant to the Secretary of the Army. Permanent records are transferred to NARA using the SF 258 (Agreement to Transfer Records to the National Archives of the United States). The SF 258 is prepared by the FRC, RHAM or RMO holding the records and is then sent to RMD for signature and forwarding to NARA.

l. Do not retire records for which the disposition is dependent on some future event occurring unless you have the date upon which the event is to occur. Otherwise, the records holding facility would have no way of knowing when to dispose of these records.

m. Do not mix temporary and permanent records on the SF 135. Do not include more than one permanent records series on the SF 135. Each series should be transferred as a separate accession.

8–6. Classified records

a. Agency security managers must be consulted before retiring classified records and initiating actions, as specified in AR 380–5. The RHAs should only accept classified documents that are properly marked. Classified information will not be disclosed on the SF 135, only an unclassified title may be used to identify the records. Agency security managers should be consulted for specific information.

b. Top secret records will not be retired until downgraded to a lower classification, except those in overseas commands and those which are to be deposited with the Defense Investigative Service and in the U.S. Army Intelligence and Security Command (INSCOM) records center. When top secret records must be retired, transmission and accountability will be in accordance with AR 380–5 and other applicable security management instructions.

c. Instructions for listing, receipting, and packing material with secret and confidential classifications are the same as those for unclassified, except those unclassified titles will be used on the SF 135 to list the records. In addition, other receipts may be needed such as DA Form 3964 (Classified Document Accountability Record).

d. Special intelligence documents, including top secret, will be retired only to the INSCOM records center.

e. Regardless of classification, restricted data and formerly restricted data will not be intermingled with other information when being transferred to the AEA or a FRC.

8–7. For controlled unclassified information records

Records with the CUI protective marking will be packed as prescribed in this chapter for unclassified records.

8–8. Transferring records to other organizations

The procedures for packing records and preparing and distributing records transmittal lists when transferring records to organizations other than RHAs or FRCs are the same as those described above.

8–9. Packing the boxes

a. Use the proper box size when packing the records. See table 8–1 for types of boxes to use in shipping records. For legal and letter-size material, use standard-size boxes. Use half-size or other boxes only for microfilm, index cards, or other odd-size material. Contact the records center for assistance in selecting the proper container for odd-size materials. Do not use boxes that are damaged or have information obscuring the accession number blocks or reuse boxes that have stick on labels as they are subject to falling off after several years in storage.

b. Place letter-size records in the box with labels facing the numbered end. The numbered end will be opposite the stapled end. Place legal-size records in the box so that the labels face the left of the box as you face the numbered end. Leave approximately one inch of space in each box for working the files (more if interfiles will be added later). Guides and tabs may be left in the records if they will help the records center personnel service the records.

c. Do not over pack the boxes. Never add additional material on the bottom, side, or top of the records in the box.

Table 8–1
Storage container types and uses Continued

Container	Description and/or use
Standard letter/legal	Universal storage box for legal or letter-size files. Used exclusively for retiring, storing, and shipping paper files to FRCs. Features lapped joints secured by wire stitching. Lock-bottom box includes hand holes.
Half-Size	Half-height box; use for microfilm, index cards, or odd-size material. Two half-size boxes fit on FRC shelving in the same space as one standard box. 14–¾ inches x 9–½ inches x 4–¾ inches; NARA supply number (NSN) 8115–00–117–8338
Microfiche	Use for microfiche, COM and microfilm jackets 14 ¾ inches x 6 ½ inches x 4 ½ inches; NSN 8115–01–025–3254 *Note: Do not store silver halide master film in the same box with diazo duplicate film.*
Microfiche (archival)	Acid free box; use for long-term storage of microfiche, COM and microfilm jackets. 14 ¾ inches x 6 ½ inches x 5 inches; NSN 8115–01–132–1923 *Note: Do not store silver halide master film in the same box with diazo duplicate film.*
X-Ray	Used for storing x-ray film White, 9–¾ inches x 15–¾ inches x 5–¼ inches; NSN 8115–00–290–3386 *Note: Do not mix silver halide master x-ray film with diazo duplicate film.*
Magnetic tape	Used exclusively for retiring, storing, and shipping magnetic tapes to the FRC. Corrugated, fiberboard box features lapped joints secured by wire stitching. Lock-bottom box includes hand holes.

Table 8–1
Storage container types and uses—Continued

	Bursting strength–275 psi. White, 14–¾ inches x 11–¾ inches x 11–¾ inches; NSN 8115–00–117–8347
Hollinger	Acid-free fiberboard boxes; available in various sizes to accommodate different record types. Used for archival preservation of permanent records. https://www.gsaadvantage.gov/ and https://www.hollingermetaledge.com/

Note: Do not over-pack boxes; never add excess material on the bottom, sides, or top of records inside the box. Leave one or two inches of space for accessing files and documents within the box.

8–10. Numbering boxes for shipment

a. Before the boxes are shipped to the records center, write the transfer number and/or accession number and the box number in the designated printed blocks on each box at least 1.5 inches high.

b. For boxes without the printed blocks, write the transfer number in the upper left corner and the Army organization box number in the upper right corner of each box at least 1.5 inches high. Begin with box number 1, and include the total number in the transfer, such as 1/10 (1 of 10), 2/10, 3/10, and so forth. The sides of the boxes may be used to write any information concerning box content.

c. Do not use labels other than the barcode label to supply additional identifying information. No standard method of affixing labels is effective in long-term storage.

d. Do not write on sealing tape. Do not place tape over transfer or box numbers.

8–11. Shipment of boxes

a. Records must be shipped to a FRC within 90 days after receipt of the approved SF 135. If the transfer cannot be made within this period, promptly advise the FRC. Unexplained delays of more than 90 days will result in the FRC canceling the transfer number and returning the SF 135. If this happens, the organization will then be required to resubmit the transfer paperwork, obtain approval for the shipment, and renumber the containers with a new transfer number.

b. Records may be sent by mail, commercial carrier, or common carrier on pallets (portable wooden platforms without wheels). Some records centers will pick up agency records. Check with your local center for scheduling and fees. For shipments of less than 20 boxes, organizations will find it more economical to mail or ship them via commercial carrier. Using a commercial carrier also has the advantage of automatic registration and tracking.

c. For shipments over 20 boxes, make all the necessary arrangements to ensure boxes arrive at the records center in numerical order so that box 1, with a copy of the SF 135 included, is the first box unloaded. If shipments of 20 boxes or more must be mailed, they may be sent in a postal container or by bulk mail.

d. Organizations shipping their boxes on pallets using a commercial carrier should complete a Transportation Services Order. Go to https://www.archives.gov/files/frc/forms/transportation-services-order.pdf for the transportation services order form.

e. For shipments of 100 or more boxes to an FRC, call the records center to schedule a shipping date, and instruct commercial carriers to contact the records center 24 hours before delivery.

f. Shipments arriving at a FRC out of order, in oversize boxes, improperly taped, or improperly marked, may require extensive remedial effort and increased costs. These costs are the responsibility of the shipping organization. See table 8–2 for a general conversion formula.

Table 8–2
General Conversion Formula

Media and/or container type	Size	Volume (estimated)	Cubic feet
Sheets of paper	Letter-size	3,000 pages	1.0
Records storage box	Standard (letter/legal)	10 inches x 12 inches x 15 inches/3,000 pages	1.0
Records storage box	Transfer case (letter-size)	10 inches x 12 inches x 36 inches/6,000 pages	2.5
Records storage box	Transfer case (legal-size)	10 inches x 15 inches x 36 inches/6,000 pages	3.0
Standard file cabinet	Letter–8.5 inches x 11 inches	1 full drawer 6,000 pages	1.5
	Legal–8.5 inches x 14 inches	1 full drawer 6,000 pages	2.0
Lateral file cabinet	Letter–8.5 inches x 11 inches	1 full drawer 9,000 pages	3.2
	Legal–8.5 inches x 14 inches	1 full drawer 9,000 pages	4.0
Shelf files (12 inches x 36 inches)	Letter–8.5 inches x 11inches	1 full shelf 6,000 pages	3.0
Shelf files (15 inches x 36 inches)	Legal–8.5 inches x 14inches	1 full shelf 6,000 pages	3.4
Microfilm	16mm x 100 feet	90 reels	1.0
	35mm x 100 feet	44 reels	1.0
Index cards	3 inches x 5 inches	10.0 linear feet 12,000 cards	1.0
	4 inches x 6 inches	6.0 linear feet 6,000 cards	1.0
	5 inches x 8 inches	3.6 linear feet 4,800 cards	1.0
Computer print-outs	12 inches x 15 inches	10 inch stack	1.0

Chapter 9
Reference Procedures and Services

9–1. Army Records Information Management System master index of retired records

a. The ARIMS master index lists all records maintained in the AEA. All records sent to the AEA are processed through the ARIMS “Upload” tools for electronic records or the ARIMS “Manage Hardcopy” tools by AEA personnel. In the case of Army organizations, such as HQDA staff elements and those not residing on an Army installation, the records will be processed by the organization’s RMO. Additionally, information on electronic temporary records that are maintained in an information system or electronic collection with an approved exception are included in the index.

b. Electronic records stored in the AEA are indexed to the document level and may be searched by keyword, phrase, subject, date, file size, and/or organization. Unless otherwise authorized, no record, record report, or list of records is available to persons or organizations that are not the creator/owner of the record or responsible for its maintenance or disposition. Third party requests for records will be forwarded through the proper channels for action, as needed (for example, FOIA and/or PA or congressional requests).

9–2. Records retrieval

a. Army electronic archives and records holding area. The ARIMS search tool located under the “Search” tab is used to seek, locate, request, and retrieve records stored in the AEA. Electronic records in the AEA are retrieved online from a list of records searched and by completing a short request form that is automatically generated. Requests for electronic temporary records being maintained in an information system or electronic collection should be directed to the individual or organization listed on the index for those records and should include the purpose and scope for requesting the information (for example, the last three annual reports for research, to respond to a Congressional).

b. Federal records centers. Request for records stored at FRCs by using ARCIS. ARCIS is an online portal through which organizations can do business with the FRCs while saving time and reducing paperwork. Users may apply and register for access to ARCIS by submitting a request to RMD. In accordance with AR 25–400–2, all new users must—

(1) Coordinate with their RA or RM prior to requesting ARCIS access for their concurrence.

(2) Have a minimum Secret security clearance.

(3) Complete the ARCIS training at https://www.archives.gov/frc/arcis.

(4) Complete the required documentation and submit to RMD at usarmy.belvoir.hqda-rmda.mbx.rmda-certification@army.mil. The required documentation includes.

(a) NARA FRCs ARCIS New User Application.

(b) Authorization to access agency records in the custody of the FRCs.

(c) Verification of Security Clearance Memorandum signed by the requestor's security office. The memorandum must include the requestor's name, clearance type, date granted, date of expiration, and the security point of contact's information. Do not include additional PII on the memorandum.

9–3. Records holding area records and/or Federal Records Centers reference services

OMB/NARA Memorandum M–19–21 requires that Federal agencies must fully manage all records in an electronic format possible and must close agency-operated records storage facilities. Until then, the following procedures may be implemented to provide rapid and efficient records reference services. These procedures may be adapted to organize records retrieval in any size office or large file room operation. The records requester is responsible for the return to the RHA of the charged-out records material intact and in the same folder order within the box as when borrowed. The records will be used for official purposes only.

a. Requests to charge out records will be documented and tracked by using a check-out/-in database, the forms listed in paragraph 9–3*b*, or equivalent memorandum format. Information generally needed to locate and charge-out record materials (most are listed on the SF 135) includes the following:

(1) The RN, description, and classification.

(2) Office of record origin and date of the document(s) (specific or approximate).

(3) The date of records transfers to the RHA.

(4) Box identification number and/or location within the RHA, if available.

(5) Requester's name, organization, location, telephone number, and email address.

b. A charge–out record may be made and substituted for documents removed from a file for reference purposes. Charge–out forms and their recommended use are as follows:

(1) DA Form 543 (Request for Records) is used for documents charged out when the suspense control is needed. The original should be attached to the record material to serve as a routing form and cover sheet and a copy placed in a follow–up or suspense file. A copy of the completed form may also be attached to an optional form (OF) 23 (Charge out Record) or OF 24 (Shelf File Charge out Record) and placed in the location from which the material is removed. These DA forms are available at https://armypubs.army.mil.

(2) OF 23 or OF 24 may be used for documents charged out when suspense control is not desired.

(3) A charge–out system using DA Form 543 involves a suspense and follow–up procedure to control loaned records. A uniform follow-up time (usually 5 to 10 days) for charged out material should be established. The suspense file should consist of a copy of each of these forms representing charged out documents for use in tracing the records that were charged out from the files area.

9–4. Relocation of records within a federal records center

If it becomes necessary to move records within an FRC, the Army will be notified of the relocation. A NA Form 13016 (Notice of Transfer Location Change) is mailed following the relocation.

Chapter 10
Records Holding Areas and Federal Records Centers

10–1. Closing records holding areas

OMB/NARA Memorandum M–19–21 requires that Federal agencies must fully manage all records in an electronic format possible and must close agency-operated records storage facilities.

10–2. Regional and overseas records holding areas

All commands with RHAs outside the continental United States (OCONUS) will follow the guidance in OMB M–19–21.

10–3. National Archives and Records Administration Federal Records Centers

NARA operates Federal records centers in nine regions throughout the United States which provide secure storage for long-term records. The FRCs were established to receive and maintain records of Federal Government agencies with long-term or permanent value, pending their ultimate destruction or accession into NARA. These centers furnish reference service for the records that they maintain.

a. NARA records centers have been established in CONUS to receive and maintain records with long-term or permanent value, pending their ultimate destruction or accession into NARA.

b. Installations and activities not serviced by an installation RHA (such as HQDA staff elements and Army organizations not residing on an Army installation) may use NARA facilities for storing their long-term or permanent value records. The primary FRC for non-Corps of Engineers Army agencies is the Washington National Records Center.

c. NARA runs its services on a reimbursable basis. RMD centrally funds the basic services (storage fees and referencing costs). Other services must be funded by the organization owning the records and be approved by their HQDA principal officials, ACOMs, ASCCs, or DRUs. See NARA Website for a current listing of all Federal Records Centers and the records they maintain.

10–4. Records freezes or moratoriums

a. Records freezes, e-discovery actions, preservation orders, litigation holds, and moratoriums are exceptions to disposition instructions. Records freezes, preservation orders litigation holds, and moratoriums refer to a court or agency-imposed requirement to keep the record until disputes, litigation and all appeals are resolved. A similar litigation process, e-discovery, involves identifying and collecting electronically stored record and non-record information that may be potentially significant and relevant to a particular lawsuit. Authority to destroy records covered by litigation holds will only resume with the concurrence of the Office of the General Counsel (OGC) and/or Office of the Judge Advocate General and/or U.S. Army Legal Services Agency (OTJAG and/or USALSA) who requested the hold.

b. RMD receives notification of the requirement to suspend disposition from OGC, OTJAG, and/or USALSA.

c. RMD notifies NARA, HQDA principal officials, ACOMs, ASCCs, and DRUs RMOs, to suspend regular disposition of the affected records and when the freeze or moratorium is lifted. Each command will notify its subordinate installations and supported activities to the lowest echelon to impose or remove the records freeze. When notified, RMD will provide the DA Form 7915 (Records Freeze Acknowledgement) for agency/command completion.

d. Records affected by an exception to disposition will not be destroyed on schedule and must be held until the action is lifted before normal disposition can be continued. The RHA and/or FRC and AEA managers are accountable for the records in the physical custody of their respective facilities. Records held in the CFA, an automated information system or electronic collection are also subject to suspension of disposition actions. Commands are equally responsible to ensure these automated information systems or electronic collections have been searched for responsive information.

e. When a suspension of disposition action is lifted, the records disposition is carried out based on the original date of the record and not the end of the freeze.

Chapter 11
Essential Records and Disaster Recovery Operations

11–1. General

The provisions of the Army Essential Records Program are applicable agency wide. The program supports the continuation of communications and information flow, as well as the continuation of essential agency functions. Essential records, also known as a vital records, provide an agency with the information it needs to meet operational responsibilities under other than normal operating conditions, to resume normal business afterwards (emergency operating records), and to carry out the agency's essential legal and financial functions (legal and financial rights), pursuant to 36 CFR 1236.14.

11–2. Categories

Two categories of records are typically identified as Essential records: emergency operating records and rights and interest records.

a. Emergency operating records are essential to the continued functioning and reconstitution of an organization before, during, and after a national security emergency or under emergency or disaster conditions. According to AR 500–3, Headquarters, commands, and certain activities maintain copies of emergency operating records at predesignated relocation and alternate sites. Records under this category include the following:

(1) Emergency plans and directives including information needed to operate the emergency operations center and its equipment and records recovery plans and procedures.

(2) Order of succession.

(3) Delegations of authority.

(4) Emergency staffing assignments, including lists of personnel along with their addresses and telephone numbers that are assigned to the emergency operations center or other emergency duties or authorized access to damaged facilities to assess the extent of damage.

(5) Emergency operations center access credentials and classified or restricted access container documentation as required.

(6) Building plans and building systems operations manuals for all agency facilities.

(7) Equipment inventories for all agency facilities.

(8) The ORLs describing the record series and information systems or electronic collections maintained within the office for all agency facilities.

(9) Essential records inventories.

(10) Copies of agency program records (whatever the media) needed to carry out continuing critical functions.

(11) System documentation for any information system designated as emergency-operating.

b. Rights and interest records are essential to the preservation of the legal rights and interests of both individual citizens and the Army (including Soldiers and their Families, DA Civilians, and contractors). These records require protection, but do not have to be maintained at, or in the vicinity of, an emergency operating site because their need would not be immediate. These records include the following:

(1) Accounts receivable records.

(2) Social security records.

(3) Payroll records.

(4) Retirement records.

(5) Insurance records.

(6) Records relating to contracts, entitlements, leases, or obligations whose loss would pose a significant risk to the legal and financial rights of the Federal Government or persons directly affected by its actions.

(7) System documentation for any information system or record collection which contains records designated as needed to protect rights.

11–3. Concept of operations

Through the Essential records program, several key processes are implemented regularly to properly identify records, determine storage, maintenance, access requirements, and protection of essential records/databases.

11–4. Back-up and protection

Existing Army disaster recovery planning identifies that all contents of Army network drives are mirrored at backup site. See AR 25–1 for additional information.

11–5. Maintenance

a. In accordance with AR 25–400–2, HQDA principal officials, ACOMs, ASCCs, and DRUs must create and maintain a Essential Records Program The program consists of a plan which can be stored in electronic and hardcopy format and should contain the following:

(1) The most current continuity of operations (COOP) Team Roster with key agency contact information.

(2) Inventory of Essential records identified by office components.

(3) Documentation of electronic access requirements.
(4) Location of physical keys and access codes for essential records storage.
(5) Location and directions to each area of responsibility.
(6) A list of equipment and telecommunications required to access specific essential records.
(7) A copy of the proponent's COOP Plan.
b. See appendix E for additional guidance.

11–6. Inventory

RMOs must conduct an inventory of records needed to support emergency operations. In addition, HQDA principal officials, ACOMS, ASCCs and DRUs must ensure all essential records and systems in their charge are routinely backed up and maintained at a secure off-site facility (see table 11–1).

Table 11–1
Essential records inventory sample

Office symbol	Records series/ record number	Essential file record or database	Form of record (for example, hardcopy, electronic)	Storage location	Maintenance frequency
AAHS–LGD	400B/380-19k	COOP Plan	Electronic and/or hardcopy	See AR 25–1	Annually
AHS–OOS	800D/1z	Orders of succession	Electronic and/or hardcopy	Executive admin centralized filing cabinet and ARIMS	As needed in the course of business
AHS–OOT	800D/1z	Delegations of authority	Electronic and/or hardcopy	Executive admin centralized filing cabinet and ARIMS	As needed in the course of business
AHS–OOW	800D/1a	ORLs	Electronic	ARIMS and ARIMS back-up location	As needed in the course of business

11–7. Review and risk assessment

a. Annually, a risk assessment of the essential records is conducted to identify any irreconcilable risks regarding the identification, maintenance, securing, and access to essential records. This risk assessment is scheduled to coincide with COOP related exercises, ensuring that lessons learned specific to essential records from COOP related exercises are directly reflected in the risk assessment.

b. Also, access to essential records is tested semiannually to ensure the program's capability to ensure COOP team members have access to essential records.

c. A periodic review of essential files, records, and databases are completed to coincide with COOP related exercises to identify any emerging issues in the program. The review of the records is conducted to ensure the continued effectiveness of the RMO in facilitating the identification, maintenance, protection, and access to essential records during COOP operations.

11–8. Disaster recovery of records

Army records can be stored in hardcopy format or electronically. For both types of records, recovery procedures are necessary to restore electronic data and to restore physical records that may be damaged by fire, water, or other contaminants. During the operations and reconstitution phases of COOP, the following processes should be followed to recover damaged records:

a. Notify the RMO and other appropriate persons 72 hours after the situation has been assessed to relate details about the nature of the emergency and the level of threat to the records.

b. Assess the damage to records as soon as possible after the emergency and take steps to stabilize the condition of the records so further damage will not occur.

c. Assemble a records recovery team of available staff members to expedite stabilization of the records (generally only for major records disasters).

d. Consult with contractors who provide records disaster recovery services if the damage assessment shows a need for their expertise.

e. Recover the records and the information that they contain or provide replacement of any lost recorded information when recovery is not feasible.

f. Resuming normal business using the recovered records and information.

g. Test the records recovery procedures to ensure the recovery runs smoothly (including drills on using the equipment, supplies, and procedures for essential records recovery).

h. Utilize necessary IT troubleshooting procedures to recover lost electronic data from host site.

i. If troubleshooting lost electronic records fails, retrieve back-up tapes from proponents COOP site.

j. Protection and recovery of mission-critical, non-electronic files are the responsibility of each office, if off-site storage is not practical. Army proponents should keep all operational and historical records in fireproof and waterproof file cabinets. These cabinets provide optimal protection for all types of essential records. If essential records, including electronic media, are damaged by an incident, stabilizing the environment, and removing records will prevent further damage.

11–9. Damaged legacy records

It is important to take care of damaged legacy records within 24–48 hours.

a. When records are water damaged.

(1) Many record materials will respond well to simple air drying if minor physical distortion is acceptable. Small quantities may be spread out on top of clean blotting material (paper toweling, and so forth) in a cool, dry location with plenty of air circulation. As long as materials are not too densely packed and active drying conditions are maintained, mold growth should be mitigated. (See para 11–9*c* for instructions on handling records with mold.) While high heat and harsh sunlight will dry records quickly, they may permanently damage record materials and should be avoided. Quantities too large to handle within the first 48 hours should be frozen either for defrosting and air drying later, or for referral to a commercial drying vendor or preservation professional. For response and recovery guidelines consult the NARA Records Emergency Information, Federal agencieswebsiteathttps://www.archives.gov/preservation/disaster-response/salvage-procedures.html.

(2) Some record materials will dry more satisfactorily than others; and metal, plate glass, some photographs and furniture may be exceptions to freezing. Questions about the treatment of particularly valuable wet records should be referred to a preservation professional immediately.

b. When records have bugs.

(1) There are many types of pests that are attracted to paper. Contact your local agricultural extension service or an entomologist for accurate identification. Chemical treatment (fumigation) may permanently damage record materials and should be avoided. Instead, attempt to address the source of the infestation, seal all possible entry points; promptly remove or seal up pest lures, such as food or trash; keep temperature and RH low; and keep the area clean and dust-free.

(2) If the infestation affects only part of a collection, isolate the materials in a tightly sealed plastic bag and consult a preservation professional. Pests found in records are most commonly the types attracted to damp conditions. If the infestation is widespread, it is likely there is excess moisture present that must be located, and the resulting high RH eliminated. Spread the records out in a cool, dry location with plenty of air circulation. This should drive the pests away. As long as proper conditions are maintained, any eggs left behind will not hatch and offspring will either not survive or move on to a more hospitable environment.

c. When records have mold growing on them.

(1) Mold grows in areas with high temperature, high RH, and low air circulation. Isolate moldy record materials in a cool, dry location, with plenty of air circulation so they will not contaminate nearby items; do not return the records to their original location until the conditions causing the mold growth are addressed. Once record materials are removed to a less hospitable environment, the mold will become loose and powdery as the substrate dries and the mold turns dormant. It may then be gently brushed off the record materials. Because the mold is merely dormant, if it remains on the record materials or is distributed throughout the space and onto other objects, it will grow whenever environmental conditions are favorable again. Mold should, therefore, be removed either outdoors or into a vacuum cleaner equipped with a high efficiency particulate air filter; regular vacuum cleaners will merely exhaust and recirculate mold back into the room.

(2) Ideally, the faster record materials are dried the better. However, some record materials may distort physically if dried too quickly. Contact a preservation professional for advice on how to handle moldy record materials of high value.

(3) Many people are sensitive to mold and some mold species are toxic. Moldy items should, therefore, be handled with extreme care. Do not proceed with any treatment once any negative health effects are observed, no matter how minor they appear.

11–10. Deleted or lost electronic records

a. Loss of power is one source of losing data. This can be eliminated using power protection such as surge suppressors and battery packs.

b. Information can also be lost due to hard disk crashes caused by contaminated systems due to dust, snack food, and so forth. Measures should be taken to ensure a clean environment.

c. Storage media such as CDs, magnetic tape, and disks degenerate over time and in substandard physical conditions. Ensure record information is migrated before problems arise.

d. While it might appear deleted or lost data has disappeared; in many instances the information may be recovered. If the information is important and it cannot be easily duplicated, contact your local IT department and if necessary, there are many companies that specialize in recovering such data. The names and contacts for such companies should be readily on hand should the need arise.

Chapter 12
Records Management Metrics

12–1. Purpose

The metrics provides an overall view of the Army Records Management Program. It is an aid for identifying program areas in need of additional emphasis at every echelon. Requirements for measuring various indicators are included in the Code of Federal regulations and the United States Code (Federal law). Looking at specific aspects of the program such as training, the percentage of organizations with valid ORLs, and summarized findings of evaluative visits/inspections provides an indication of the effectiveness of the overall program.

12–2. Training

One requirement of the Army Records Management Program is to train users on their legal responsibilities for managing record information. All military, civilian, and contractor personnel create, use, and store electronic or hardcopy records as a product of their work or official duties. This chapter provides the minimum requirements for records management training.

a. All Department of the Army Personnel.

(1) In accordance with NARA Bulletin 2017–01, all DA personnel with email accounts or IT network resources access will complete the Records Management training within the first 60 calendar days at their first assignment or date of employment and refresher training annually. Training is available via Army Learning Management System (ALMS) at www.lms.army.mil. Certificates will be maintained by the servicing RMO.

(2) Additionally, this includes all personnel that create, receive, access, or use Army records, regardless of whether those individuals have email accounts or IT network access. This training requirement applies to any person that create, receive, access, or use Army records. The servicing RMO of DA personnel with no email accounts will provide copies of the ALMS training slides within the first 60 calendar days at their first assignment or date of employment and maintain any documentation demonstrating completion of training.

b. Senior officials.

(1) Senior officials will receive orientation training (when taking new positions) and exit briefings before departing the position on the appropriate disposition of the records, including email, under their immediate control (see 36 CFR 1222.24(a)(6) and 36 CFR 1230.10(a & b). Orientation training will include an overview of the Army Records Management Program and the senior official's responsibilities pertaining to the program. The training may be given in any forum conducive to the senior official's schedule and in most cases will be included in their training from either the War College or Civilian Senior Leader Management Office (CSLMO) in coordination with RMD.

(2) In addition, senior officials will be briefed by the ACOM, ASCC, or DRU RA on their specific records management obligations within the first month of designation/appointment to their new position and 2

months prior to leaving the position. A best practice is to coordinate with the local legal and IT staff. Completion of the training will be documented and maintained by the RA.

12–3. Evaluation and/or inspection

To ensure good recordkeeping practices have been implemented within the different Army organizations and that all recordkeeping requirements are being met, evaluations must be performed periodically. In accordance with AR 25–400–2, RAs will evaluate their organizations' records management programs at least once every 2 years; records managers will evaluate their organizations' records management programs at least once every 2 years.

a. Evaluation objectives.

(1) To assess the effectiveness of the recordkeeping program.

(2) To ensure the organization's record information is being captured, identified, scheduled, and appropriately managed.

(3) To provide on-the-spot advice and assistance as may be needed to improve the effectiveness of program operations.

(4) To advise the commander of the organization visited, in writing, of the general and specific findings and to offer recommendations for correction of noted deficiencies.

(5) To determine the level of compliance with Army regulations governing the related program elements, Army guidance and NARA requirements.

b. Scheduling the evaluation. Develop and/or update a 2-year program evaluation cycle of all organizations within the area of responsibility and coordinate with each of the organizations to be evaluated.

c. Notification.

(1) Contact the organization's RM or RC and confirm the dates of the visit, 3 months prior to a visit.

(2) After confirming dates for the visit and 2 months prior to the scheduled evaluation date, send a formal notification addressed to the commander of the organization to be visited. In the notification, include the name, security clearance of the person(s) doing the evaluation, program elements to be evaluated, a proposed itinerary, and a request for information needed both prior to and during the visit. Entrance and exit interviews should also be addressed.

(3) Review information provided by the organization and confirmed the itinerary, 1 month prior to the visit.

d. Entrance briefing. Brief the commander of the organization being evaluated or a designated representative. The form of the briefing is normally set by the organization visited; it may be as formal or informal as they desire. The organization visited may elect to provide an overview of the functions and structure of their organization. Unique situations or specific problem areas may be identified requiring a heavier concentration of effort in these areas and an altering of the proposed itinerary.

e. Evaluation process. A considerable amount of time will inevitably be spent in addressing unforeseen problem areas or issues surfaced during the visit. The effectiveness of the following program operations is essential and must be addressed, at a minimum—

(1) *General.*

(a) Supplementation of DA directives and other published or written guidance affecting program elements.

(b) Training program(s) for HQDA principal officials, ACOMS, ASCCs, and DRUs.

(c) Periodic internal command-wide evaluation of the records management program for the identification of record information, maintenance and use, and records disposition.

(2) *Recordkeeping systems management.*

(a) ARIMS web tools, including registration and approved ORLs.

(b) Identification of record information (all media) under the RRS–A.

(c) Records transfer procedures, especially to the AEA and FRCs.

(d) Managing record information on shared drives and collaborative sites.

(e) Records holding area operations.

(f) AEA.

(3) *Information technology systems and storage media.*

(a) Plans and actions to manage record information via imaging systems, electronic record systems and cloud services.

(b) Procedures for the capture and management of email, text messages, social media and chat postings and similar items that meet the legal definition of record information.

(c) Working relationships with IT, legal, information assurance, information management and security personnel. Inclusion of the RA or RM in the IT planning process from its inception and system requirements.

(4) *Contractor-created records.* Contracts must specify Government ownership and delivery to the Government of all record information created or received by the contractor in fulfilling the contract requirements. Inspection of Government owned contractor records should be by the servicing RMO.

(5) *Correspondence management, Privacy Act, and Freedom of Information Act.* Consult the appropriate directives for a list of survey topics.

f. Exit briefing. Brief the commander or designated representative. Normally, individuals of the organization who are responsible for administering the program areas evaluated also attend the exit briefing. Address general and specific findings that will be included in the written report, there should be no surprises.

g. Written report of findings and recommendations.

(1) Submit a written report to the first level of supervision within 7 working days after traveler returns to duty. The report should include a trip report and memo forwarding a report of findings and recommendations to the organization visited.

(2) Forward a report of findings and recommendations to the organization visited within 12 working days after return to duty.

(3) Address the report to the commander or head of the organization visited.

(4) Forward a copy of corrective action(s) taken by the organization to the survey team leader.

h. Evaluation questions. The sample evaluation questions listed in appendix B may be used in evaluating the different components of the records management program. These evaluation questions have been staffed with all the component programs under the records management program.

i. DA Form 7913 (Records Management Program Assessment Checklist) will be used during agency/command assessments and/or inspections.

Chapter 13
Wartime and Contingency Operations Records

13–1. General

Recordkeeping requirements during wartime and contingency operations are governed by the same laws and regulations as recordkeeping during peacetime or while in garrison, except that wartime and CONOPS records are permanent records. Commanders of deployable units will ensure that procedures and processes for collecting and/or harvesting record information during wartime and CONOPS are established in advance of a deployment and implemented immediately upon deployment. See appendix C for a list of wartime and CONOPS record series.

13–2. Records management plan for deployable units

Army commanders of deployable units will develop, maintain, and update a records management plan in writing. The records management plan is scalable and contains specific procedures for creating, identifying, harvesting, and transferring operational record information. The plan will include the following:

a. RMO appointment orders will appoint, in writing, an RM or RC with a minimum of one alternate (pending the size of the deployed unit). Ensure the appointed RM or RC and alternate receive records management training prior to deploying.

b. An approved ORL which lists all the RNs for information that could be created or maintained by the unit while deployed.

c. Identified software to be used for the record information and the type and location of storage media or whether the records will be hardcopy and their location. Be cautious that email, messaging, and social media are sources of record information which will be identified under the ORL RNs, maintained and transferred with the other electronic records.

d. Identified records transition points/collection points for deployed unit's record information.

e. Identified individuals or types of unit positions that are likely to create or maintain record information.

f. Harvesting instructions. Coordinate with an IT specialist, who will be with the deployed unit, to set up a process for periodically and routinely harvesting the unit's electronic record information (such as daily, weekly, or monthly). The ORL should be used to set up electronic and hardcopy files. See AR 25–400–2

and the ARIMS users guide for help in determining the most effective way to maintain and harvest your unit's electronic records.

g. Plans to transfer records. To the greatest extent possible, electronic files should be transferred periodically into the AEA using the BAT process. The BAT will update existing AEA files established under the ORL with recently filed electronic records. Alternatively, procedures such as transferring electronic records to a storage mechanism such as a removable hard drive to be maintained at a designated records transition point/collection point pending transfer to the unit's home command may be the best solution.

Appendix A

References

Section I

Required Publications

AR 25–1
Army Information Technology (Cited in para 5–9.)

AR 25–22
The Army Privacy and Civil Liberties Program (Cited in para 4–3*b*(1).)

AR 25–400–2
Army Records Information Management Program (Cited in para 1–1.)

AR 380–5
Army Information Security Program (Cited in para 5–4.)

AR 500–3
U.S. Army Continuity of Operations Program (Cited in para 11–2*a*.)

DoD 5015.02–STD
Electronic Records Management Software Applications Design Criteria Standard (Available at https://www.esd.whs.mil.) (Cited in para 2–11.)

EO 13526
Classified National Security Information (Cited in para 8–5*j*.) (Available at https://www.govinfo.gov.)

44 USC Chapter 33
Disposal of Records (Cited in para 2–5.) (Available at https://www.access.gpo.gov/uscode/uscmain.html.)

Section II

Prescribed Forms

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

DA Form 543
Request for Records (Prescribed in para 9–3*b*(1)).

DA Form 1613
Records Cross Reference (Prescribed in para 5–3.)

DA Form 7796
Automated Information System (AIS) Questionnaire (Prescribed in para 1–6*a*(17).)

DA Form 7913
Records Management Program Assessment Checklist (Prescribed in para 12–3*i*.)

DA Form 7914
Destruction Certificate (Prescribed in para 7–14*b*(2).)

DA Form 7915
Records Freeze Acknowledgement (Prescribed in para 10–4*c*.)

OF 23
Charge out Record (Prescribed in para 9–3*b*(1).)

OF 24
Shelf File Charge out Record (Letter size) (Prescribed in para 9–3*b*(1).)

SF 115
Request for Records Disposition Authority (Prescribed in para 2–4.)

Appendix B

Records Management Program Evaluation

B–1. Purpose

AR 25–400–2 requires RAs and RMs to evaluate the records management program.

B–2. Statutes

These Federal statutes are the statutory authority for the Army records management programs being evaluated—

a. Federal Records Act of 1950, as amended.

b. Paperwork Reduction Act of 1980 as amended by Paperwork Reduction Act of 1995.

c. E-Government Act of 2002 (codified in 33 USC Chapter 36).

B–3. Sample program evaluation questions

These questions are intended as a guideline for performing a program evaluation. They are not all inclusive and/or may be expanded on.

a. General.

(1) Is a records management program established in your organization? If so, where in the organization are the records management responsibilities placed?

(2) Is the scope of the records management program defined and do the roles and responsibilities of the records management official provide authority to conduct an effective program?

(3) Is the office responsible for your records management program sufficiently staffed to operate the program effectively? What is the staffing?

(4) Has an organizational RM been appointed, in writing, with the responsibility for records management functions in the organization? Has a copy of the appointment orders been provided to the servicing RA and forwarded to RMD? Are RCs appointed, in writing, at the sub-element level to assist with program execution? Has a copy of the appointment orders been provided to the servicing RM?

(5) Does the RM have additional functions? If so—

(a) What are they?

(b) What percentage of time is spent on records management functions?

(6) Are RMs included in the planning process for new or replacement IT systems?

(7) Do RMs have a working relationship with the legal advisor, IT security officer, and system administrators?

(8) Is training offered to serviced and/or supported activities in records management (record information identification, maintenance, and disposition)?

(a) Do all personnel receive annual training?

(b) Do all new employees receive initial records management training in accordance with AR 25–400–2?

(c) Are Senior officials and program managers briefed on the importance of records management and records handling responsibilities? Is training provided?

(d) Do records coordinators, secretaries, executive assistants, and others with regular records duties receive records management training on records maintenance and filing procedures and records disposition?

(9) Do RAs conduct records management evaluations at least once every 2 years?

(10) Do RMs conduct records management evaluations at least once every 2 years?

(a) How are evaluations conducted?

(b) Are all aspects of records management covered during the evaluations?

(c) Is this list used for the evaluations?

(d) Are previous evaluations available?

(e) Are the evaluations documented with findings, actions to be taken to correct deficiencies, and forwarded to the evaluated organization?

(f) Do evaluation reports identify accomplishments as well as deficiencies?

(g) Are follow-up visits/reports conducted to ensure that recommendations have been implemented?

b. Recordkeeping.

(1) Are all RMOs registered in ARIMS?

(2) Are all RMOs trained within 90 days of appointment?
(3) Is the RRS–A used as the legal authority for identifying, maintaining, and archiving or destroying records?
(4) Is AR 25–400–2 consulted for Army policy on all aspects of managing record information?
(5) Have current files been established and set up in accordance with AR 25–400–2?
(a) Is record information in email, texting and social media material maintained as electronic records?
(b) Are minimum labeling requirements for electronic and hardcopy record information being met?
(6) Are official records kept separate from personal papers in a consistent and readily identified manner?
(7) Are active and inactive files maintained separately?
(8) Does the record management program include all records regardless of media (electronic and electronic emails (e-mails), paper, audiovisual, and cartographic)?
(9) Are ORLs prepared using the "ORLs and Folders" tab in ARIMS and approved by the servicing RMO?
(10) Are information custodianship responsibilities understood and clearly designated?
(11) Do program officials review proposed records schedule relating to their office or function?
(12) Does everyone in the organization know the storage location(s) of its hardcopy and electronic records?
(13) Are records stored in a centralized records area or repository? If so, where is the area or repository located?
(14) Do all units identify their records with RRS–A disposition codes, regardless of the media (for example, network or hard drive, CD–ROM, paper) and year of creation?
(15) Are the following controls in place to safeguard and maintain required system documentation, hardware, and software to allow the management of electronic records throughout their life cycle?
(a) Are precautions being taken to ensure that appropriate software and hardware will be available to read electronic records?
(b) Is periodic maintenance or recopying of long-term electronic records being conducted during their life cycles?
(c) Is a routine being followed to backup record information? Describe routine.
(d) Is the backup routine included in the system documentation?
(16) If a system or equipment is used CUI or PA information, have proper safeguards been established? Do computer printouts have appropriate markings?
(17) Are controls being used to prevent the unauthorized alteration or deletion of electronic records? If so, describe the controls.
(18) Do records created on an electronic system have enough data entered to help identify, protect, retrieve, and dispose/transfer the records?
(19) Are procedures in place to ensure that digitized records are kept only as long as needed? If so, describe the procedures.
(20) Are electronic records, digitized images, or microforms stored under environmentally controlled conditions, periodically inspected to detect deterioration, and recopied when appropriate to meet the minimum scheduled retention?
(21) Are storage media such as disks, file drawers, and folders labeled to facilitate quick identification, access, and disposition of record information?
(22) Are any organizations within your command still microfilming?
(23) Are system managers aware of degree of protection to be afforded records stored and used electronically in accordance with classification, release ability, FOIA, and PA?
(24) Are safeguards in place against the removal or loss of official records in accordance with 44 USC 3105?
(25) Are all command unique filing requirements being met?
(26) Is a pre-file check performed to assure that each item belongs in the files, records are complete, and if required by the command, file authority is present?
(27) Are files arranged in order (for example, date, number, alphabetical, subject, name, organization, and so forth)?
(28) Are files cutoff and new files created for current year for each disposition instructions?
(29) Has a distinction been made between retention periods (for example, peacetime, mobilization, or the conduct of military operations) where they apply?

(30) Are all unidentified files brought to the attention of the RM?
(31) Is the documentation required for unidentified files forwarded through command channels for approval? Is a copy maintained by the RM?
(32) Do organization personnel know the standards for storage of security-classified documents?
(33) Are procedures established for staff to follow when they use records?
(34) Is classified material stored in accordance with security regulations? Are classified and unclassified records handled separately?
(35) Does the organization create records with a permanent or long-term retention period ("T" records)?
(36) Are "T" email records and other electronic records being sent to the AEA via the electronic capture and store or middleware software, as applicable?
(37) Are records destroyed or retired as required?
(38) Are permanent records transferred to the National Archives as provided in the records schedule?
(39) Are "K" records being destroyed in accordance with disposition instructions and not kept past the business need?
(40) Have all eligible records been transferred to the RHA, AEA, or FRC, as applicable?
(41) Are records authorized for destruction processed through property disposal channels for sale or recycling when possible?
(42) Is exposed x-ray film, motion picture film, and certain microforms that contain precious metals disposed of under the DOD Precious Metals Recovery Program?
(43) Does the organization know the location and purpose of the RHA or FRC?
(44) Is the RHA accessible only to authorized personnel?
(45) Does the organization transfer records to the RHA or FRC? Which types of records?
(46) Is the SF 135 or equivalent prepared in an acceptable manner for records to be retired or transferred to the RHA? Or FRC?
(47) Are RMs ensuring that no records subject to the PA are being transferred unless they are covered by systems notice?
(48) Are "T" records eligible for transfer and/or retirement being processed in a timely manner?
(49) Is each box accepted into the RHA or FRC labeled correctly, and the corresponding number annotated on applicable SF 135?
(50) Do all accepted records have an SF 135?
(51) Is SF 135 being completed correctly?
(52) Are copies of the SF 135 on file for stored and transferred records?
(53) Has RN 25–400-2a been established in staff office to maintain the SFs 135?
(54) Have procedures for submission of requests for records, charge out procedures, and suspense controls been established?
(55) Does the organization have a method for tracking documents that are removed from the files?
(56) Does the RHA meet NARA facility standards set forth in 36 CFR, Part 1228, Subpart K, 1228.228 through 1228.232?
(57) Does the organization have an Essential Records Program?
(58) Are the essential records reviewed periodically and updated as necessary during COOP exercises?

Appendix C

Wartime and Contingency Operations Records

C–1. General

Recordkeeping requirements during wartime and CONOPS are governed by the same laws and regulations as recordkeeping during peacetime or while in garrison, except that wartime and CONOPS records are permanent records. Wartime and CONOPS record information include but is not limited to staff journal information, assessments, draft and published orders, plans, contracts, agreements, investigations, reports, briefings, and reports generated to describe and/or document the occurrence of particular situations and events.

C–2. Wartime and contingency operations record series

Record numbers are categorized and arranged according to ACRS. In addition to 11 functional series, ACRS has a CONOPS record series. Table C–1 outlines a comprehensive listing of unit records that are to be preserved as official Army records associated with wartime and CONOPS.

Table C–1
Wartime and contingency operations record series

Record series	Record descriptions	Record numbers
	Battle update briefings	11-30a1; 11-30a2
	Battle update assessments	350-1ff; 525d; 525b
	After-action reviews	350-1jj
	Operational lessons learned	11-33a; 11-33c; 11-33d
	Operations orders (higher and lower headquarters)	500-2b
	Fragmentary orders (higher and lower headquarters)	500-2b
	Targeting lists and other fires related material	381-26a; 381-26b
300B Operations	Operational plans	525n; 525n1; 525n2; 530; 525g;
	Daily, weekly, and/or monthly situation reports	381-10c; 381-3b1; 381-3b2; 381-3b3
	Commanders' concerns	525; 525a1; 525a2
	Memorandums of instruction	1e; 25-1gggg; 25-2i; 25-30q1; 25-30q2
	Daily staff journals	220-15a; 220-15a1; 220-15a2; 220-15a3
	Tactical operation center logs	220-15a; 220-15a1; 220-15a2; 220-15a3
	Detainee operations (medical)	190-8i; 190-8i1; 190-8i2
	Military policy journals (blotters)	190-45b; 190-45b1; 190-45b2; 190-45b3
	Graphic intelligence summaries	381-10a1
	Daily intelligence summaries	381-11c; 381a
	Tactical human intelligence team reports	381-100a
300D Intelligence	Special intelligence assessments	381-20b; 381-3d2; 381-3e; 381-47a
	Terrain analysis	350-1ff; 115-11x; 115-11ee
	Enemy order of battle and personalities reports	360-5e
300D Intelligence	Battle damage assessments	381-20n
	By name unit rosters	600f1; 600f2

Table C–1
Wartime and contingency operations record series—Continued

Record series	Record descriptions	Record numbers
	Individual valor award recommendations (with attached witness statements)	600–8-22i; 600-22m
	Unit award recommendations (complete packet)	600–8-22e1; 600–8-22e2
	Strength reports	600–8-6b1; 600–8-6b2; 600–8-6b3; 600–8-6g; 600–8-104bb; 600h1; 71-32o
600A Personnel	Promotions	140-158b; 600h1; 600–8-19d; 600–8-19g; 600–8-19h; 600–8-104j; 600–8-104n; 600–8-104u; 135-155a; 135-156a
	Assignments	614; 600–8-104d3; 600–8-104j; 600–8-104n
	Awards	600–8-104d3; 385-10gg1; 385-10gg2; 215-3cc; 385-10ff; 600-22m; 672
	Casualty reports	600–8-1a1; 600–8-1a2; 600–8-1c1; 600–8-1c2; 525-13d; 40-400y
	Command and staff listings	600
	Congressional inquiries and visits	1-20d; 1-20e; 1-20f; 1-20c
	Equipment status reports and operational readiness rates	700-138c1; 700-138c2; 700-138e; 700-138h
	Supply expenditures	715eee1; 715eee2; 700-127d; 1o
700A Logistics	Fielding of new equipment	700-142a
	Battle loss or damage of major end items	725-50k1; 725-50k2
	Contracts	715w; 715-9m; 715-13a; 715-23c
	“Personal for” memorandums	1e
800D Command Group	Very important person briefings	1-1m1
	Commander's initiative group actions	690-500f
	Staff meeting notes	25-1nnnn; 215-1f
900A Safety	Accidents and/or incidents	385-10ee1; 385-10ee2; 385-10ee3; 385-10f1; 385-10f2; 385-10f3; 385-10f4; 385-10j; 385-10qq1; 385-10qq2; 385-10w1
	Chemical, nuclear, biological accidents, and/or incidents	50-5a1; 50-5a2; 50-6b1; 50-6b2
1000A Legal	15–6 Investigations	15-6b1; 15-6b2; 15-6c1; 15-6c2; 15-6c3; 15-6c4
	Uniform Code of Military Justice actions	27-10f; 27-10m; 27-10n
	Commander’s Emergency Response Program	500-3d
700A Logistics	Purchase request and commitment	37g
	Audits	600–8-104z; 37–2-10bb
	Financial liability investigation of property loss	735-5r1; 735-5r2; 735-5s

Appendix D

Records Management Official Appointment Orders

D–1. Requirements

In accordance with AR 25–400–2, all RMOs will be appointed in writing. See paragraph D–2 for the minimum required information. A duty appointment memorandum sample is provided in figure D–1.

D–2. Required information for appointment orders

At a minimum, appointment orders should include the name, RMO role, effective date of appointment, organization, and authorities. Additional information may be included.

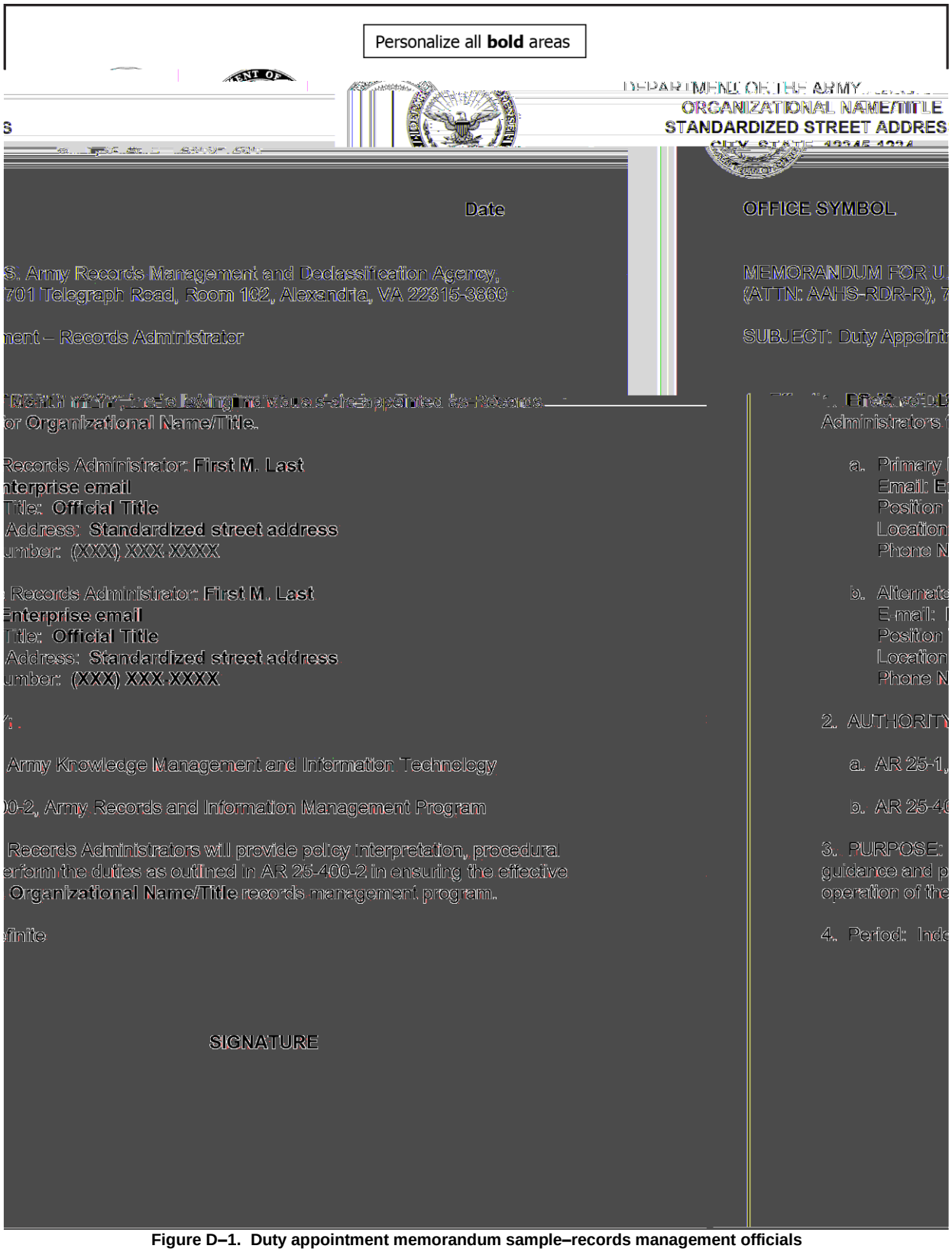


Figure D–1. Duty appointment memorandum sample–records management officials

Appendix E

Essential Records Program

E–1. Step 1-Identify your office's essential records

a. The first thing you need to do is to review the information and records maintained in your office and determine which ones would be needed in an emergency. There are three tiers of essential records protection (see table E–1). There is a link between essential records and the COOP. Therefore, one of the criteria that can be used to determine an office's Tier 3 Essential records is what the office has defined in its COOP as its "essential functions." Any records deemed necessary in supporting the office's essential functions should be a part of the office's set of essential records. There is a link between essential records and the COOP. Therefore, one of the criteria that can be used to determine an office's Tier 3 essential records is what the office has defined in its COOP as its "essential functions." Any records deemed necessary in supporting the office's essential functions should be a part of the office's set of essential records.

b. The acid test for essential records is as follows: for each record thought to be essential, ask:

(1) Can the office agency's critical work continue without record?
(2) Can the record be found elsewhere or reconstructed?
(3) Is it already protected elsewhere?
(4) Is it considered unique and irreplaceable?

Table E–1
Identifying office essential records

Tier	Types of records	Record examples
Tier 1	Records necessary in the first few hours of a crisis	Emergency preparedness plan (such as the Occupant Emergency Plan and the COOP Plan) Emergency telephone tree delegations of authority security clearance roster Office evacuation blueprints and maps (so emergency workers will know where they are going) Policy for talking to the media copy of essential records inventory Note: Generally, a part of the COOP Plan
	Records that may be needed to respond to the crisis	System manuals for critical electronic databases Regulatory information (for example, copies of regulations or data on air quality, so important environmental monitoring work can continue)
Tier 2	Records that may be needed to provide employee benefits	Personnel records for all employees, including medical records and time and attendance records
	Records that may be needed to get back into the office	Combinations and/or keys to get into locked areas Records recovery information (for example, phone numbers of salvage companies)
Tier 3	Any program-specific records on activities that are deemed to be of critical importance, in which case the work cannot be interrupted, even if, as in the worst case, the building has been destroyed and all the agency records are lost. The determination of tier three records must be made by each office. If an office decides that none of their work rises to this level of importance, there will be no tier three records	

E–2. Step 2-Prepare an inventory of essential records

Next you need to prepare a listing, or inventory, of the records identified in Step 1. Decide who needs to have copies and establish a procedure to ensure the inventory is updated and sent to the appropriate people. RMOs will serve as essential records coordinators and implement the essential records program for their offices. Includes preparing the inventory and working with office staff to ensure records are protected. They may also have to compile information, such as a list of lock combinations.

E–3. Step 3-Determine how the records will be protected

Now that you know which records in your office are essential and where they are located, you need to determine how to protect them. There are two basic choices; duplicate them and store them offsite or collect them from other sources and recreate them. If you will be duplicating information, use electronic media whenever possible since the cost to reproduce and store information electronically will be less than duplicating and storing paper. It is also critical to have a backup in case the primary electronic system fails. This can be accomplished by copying onto CD–ROM. The following is a list of questions that will assist you in making your decision.

a. Can these records be found in locations other than this office and geographic location (for example, a regional office, a State, or another Federal Agency)?

b. Is the information contained in these records available in an electronic system or database?

c. What is the most cost-effective manner to recreate these essential records (for example, storage on CDs, photocopying, collecting them from another Agency)?

d. Do these records contain any sensitive information which would require special handling?

e. How often does the information need to be updated and who will be responsible for updating it?

E–4. Step 4-Designate an offsite storage location

Based on the decisions made in Step 3, it is likely you will need to find an offsite location to store duplicates. You may need to consider equipment (for example, computers, microfilm readers) to read the records. Migrate information to new media when software and hardware changes. Records which cannot be read with existing equipment are useless. The records will need to be immediately accessible, therefore, they should be stored as close to the facility for emergency off-site operations as possible.

E–5. Step 5-Protect the records

Decide how the records are to be protected and add the information to your inventory. The inventory should show:

a. The method of protection (for example, photocopies).

b. How often the records are updated (the rotation schedule) and who does it.

c. Contact information if the records are to be collected from other locations. Records should be updated as often as possible. Consider the risk to the recovery effort if the information is out of date. Consider the cost of keeping the information updated. Ensure that any other documents which contain information related to the office's essential records program, such as the office's COOP, reflect the most updated essential records program-related information. Create a resource list of disaster recovery firms for your geographic area and update the information at least annually. Test your plan to be sure the recovery runs smoothly. Include drills on using the equipment, supplies, and procedures for essential records recovery. Evaluate the plan and update it regularly.

Glossary of Terms

Accession
The act and procedures involved in transferring legal title and physical custody of records from Department of the Army to the National Archives.

Action officer
Any individual who creates official records on behalf of the Army.

Administrative records
Records relating to budget, personnel, supply and similar housekeeping, or facilitative, functions common to most agencies, in contrast to program records.

Administrative value
The usefulness of records in conducting an agency's current business; includes fiscal value and legal value.

Alphabetic arrangement
Arranging records in alphabetical order by name or subject.

Alphanumeric arrangement
Arranging records in order by a combination of words and numbers.

Architectural records
Graphic records that depict the proposed and the actual construction of stationary structures, such as building, bridges, and canals, and movable objects, such as ships, aircraft, vehicles, weapons, machinery, and equipment.

Army Electronic Archive
Storage location for records in ARIMS that have been uploaded using the Bulk Archive Tool.

Army Records Information Management System
A web-based IT system used for identifying, arranging, managing, storing, retrieving, and applying dispositions to Army record material.

Bulk Archive Tool
A tool within ARIMS which allows registered users to submit documents as a batch to ARIMS AEA.

Capstone
An approach developed by NARA so that agencies can automatically capture and preserve as permanent the email of senior officials. Capstone supports the Presidential Memorandum on Managing Government Records and aids agencies in complying with NARA Managing Government Records Directive (M–12–18).

Cartographic records
Graphic representations drawn to scale of selected cultural and physical features of the surface of the earth, other planetary bodies and of the atmosphere.

Classified records
Official records or information requiring protection against unauthorized disclosure. The degree of protection is specified by one of the following: top secret, secret, confidential.

Computer Output Microform
Microforms (microfiche, microfilm) containing data produced by a recorder from computer generated signals. A process of converting data from magnetic tape to human readable images on film.

Copy
A reproduction or duplication of an original record. Copies identified by their function include action copy, file or record copy, reading copy, reference copy, and official copy. Copies identified by method of creation include carbon, electrostatic, offset, diazo, and vesicular. In electronic records, the action or result of reading data from a source, leaving the source data unchanged, and writing the same data elsewhere on a medium that may differ from the source.

Crosswalk
The table or chart listing RRS–A record series numbers within the ACRS framework.

Current records
Records necessary for doing the current business or operations of an office or unit. These records should be maintained in the office or unit until such time that they become noncurrent.

Cutoff
Breaking, or ending, files at regular intervals, usually at the close of a FY or CY, to permit their disposal or transfer in complete blocks.

Date arrangement
Arranging records chronologically with the newest record at the front of the file.

Declassification
The determination that security classified information no longer requires, in the interest of national security, protection against unauthorized disclosure. Removal or cancellation of the security information markings is normally involved.

Discontinuance
The placing of an organization in an inactive status or in surplus status when all military functions have ceased. When this term is used, it also includes inactivation, disbandment, and reduction to zero strength.

Disposition
The actions taken with noncurrent records. These include transfer to a RHA, retirement to a NARA records center facility, authorized destruction, and accessioning into the National Archives.

Disposition authority
Legal approval empowering an agency to transfer permanent records to the National Archives or carry out the disposal of temporary records.

Disposition instructions
Precise instructions specifying the time or event for transfer, retirement, or destruction of records.

Disposition Schedule
A document governing, on a continuing basis, the retention and disposition of the recurring record series of an organization or agency.

Documentary material
A collective term used to refer to all media on which information is recorded, regardless of the nature of the medium or the method or circumstances of recording.

Duration period
The period of time a scheduled record must be kept before its disposition. Synonymous with retention period.

Electronic mail
A document created or received on an electronic mail (email) system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message.

Electronic messages
Electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals. This includes, but is not limited to messages created by chat, text, and email systems.

Electronic records
Records stored in a form that only a computer can process.

Emergency operating records
Records that are essential to the continued functioning and reconstitution of an organization before, during, and after a national security emergency, or under emergency or disaster conditions. Emergency operating records are one of two types of essential records: the other type being rights and interest records.

Event
When used as part of the records disposition, the event represents the occurrence that must happen to start the retention period. (Examples, close of case; supersession; and obsolescence.)

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

File number
The number assigned under ARIMS to a specific series of records. The number is based on the prescribing directive specifying they be created. Synonymous with RN.

Fiscal value
The usefulness of records in documenting an agency's financial transactions and obligations.

For official use only
A classification for information not needing the full protection warranted by classified records but which should be protected from unauthorized disclosure based on a privileged or confidential basis because of its content.

Fuzzy search
Fuzzy is another way of saying inexact. One common use of this word is in the term fuzzy search. This is a feature in some software programs that allows you to search for text that is like, but not necessarily exactly the same as what you tell it to look for. For example, you might type in something like phonics, and the fuzzy search might find phonics or telephone or Phoenicia.

Hardcopy records
Records created on paper or some other durable surface, such as microfilm.

Housekeeping files
Records accumulated or generated in an office that document the internal administrative functions of the office as opposed to those that document the primary missions of the office.

Imaged files
Files created by processing hardcopy records through a scanner which digitizes and converts the information to bit-mapped images of the records.

Information System or Electronic Collection
The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. Often used as a synonym for a digitized or electronic records system.

Interface control document
A document describing the interface(s) to a system or subsystem. It may describe the inputs and outputs of a single system or the interface between two systems or subsystems. Its purpose is to communicate all possible inputs to and all potential outputs from a system for some potential or actual user of the system. Interface control documents are a key element of systems engineering as they define and control the interface(s) of a system, and thereby bound its requirements.

Keep event records
Records classified as “KE” records which are usually short-term temporary records that have no value beyond the business process. hey can have retention periods from 1 day up to and including 6 years; however, the retention period does not start until the event occurs. They may be further classified as “KEN” (keep until event occurs and then until no longer needed), “KE1” (keep for 1 year after event occurs), “KE3” (keep for 3 years after event occurs), and so forth.

Keep records
Records classified as “K” records which are usually short-term temporary records that have no value beyond the business process. They can have retention periods from 1 day up to and including 6 years.

Legacy records
Legacy records are records that contain historical value and may be temporary and or permanent. They may be textual, analog and/or electronic. These records may include electronic information held on shared drives, databases, USB peripheral drives, computer hard drives or other media/formats. Often these records may have been inherited from a retired system and/or disestablished department.

Legal value
The usefulness of records in documenting legally enforceable rights or obligations.

Library copy
Reference copy of a record maintained as part of a library collection or manuscript collection, not an official record copy.

Life cycle of records
The management concept that records pass through three states, creation, maintenance and use, and disposition.

Master Index
In ARIMS, the index for all hardcopy records retired to Army record holding facilities and for electronic records that have been transferred to the AEA.

Memorandum of agreement
A formal business document, also known as a memorandum of understanding, used to outline an agreement made between two separate entities, groups or individuals.

Metadata
Elements of information that provide administrative, descriptive, and technical information that describe the structure and content of electronic records.

Microfiche
A 4-inch x 6-inch card-size transparent sheet of microfilm containing up to 240 miniaturized images arranged in a grid pattern.

Micrographic records
Records placed on microfilm by reducing and recording images photographically or by recording directly onto film using a computer.

Migration Plan
A plan of organized tasks for the periodic transfer of digital materials from one hardware/software configuration to another, or from one generation of computer technology to a subsequent generation.

Museum copy
Reference copy of a record maintained as part of a museum collection or manuscript collection, not an official record copy.

Non-current records
Records no longer required for current business or operations, inactive records.

Non–records
Documents excluded from the legal definition of records according to 44 USC 3301.

Numeric arrangement
Arranging records in sequence by number.

Office
Any place where records are created, maintained, or used, excluding RHAs, records centers, and so forth.

Office Record List
List of record titles/RNs used within a specific office annually.

Official record copy
That copy of a record kept by the agency, office, or element directly responsible for the function to which the record relates which has been identified as the copy to be maintained to document the action taken or business transacted. Record copies of incoming or outgoing communications may be in a variety of forms. These include electronic copy, paper copy, handwritten items, specific media, microforms, and so forth. It does not include reading file copies or copies held for convenience or reference. Synonymous with record copy.

Official records
The term, “official records” does not include library and museum material made or acquired and preserved solely for reference or exhibition purposes or duplicate copies of records preserved only for convenience.

Permanent records
The designation applied to records worthy of permanent retention by the U.S. and accessioned into the National Archives.

Personal papers
Documentary materials belonging to an individual that are not used to conduct agency business.

Pre-accessioning
Process by which agencies transfer to NARA a copy of a permanent electronic record while retaining legal custody and control over access.

Preservation
Specific measures, individual and collective, taken for the repair, maintenance, restoration, or protection of information storage media.

Program records
Records documenting the unique, substantive functions for which an agency is responsible, in contrast to administrative records.

Record number
The number assigned under ARIMS to a specific series of records. The number is based on the prescribing directive specifying they be created. Synonymous with file number.

Recordkeeping requirements
Statements in laws, regulations or agency directives providing general and specific guidance on particular records to be created and maintained by an agency.

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 Government or because of the informational value of data in them.

Records administrator
Records official who serves at the headquarters of ACOMs, ASCCs, and DRUs. RAs have command wide responsibilities to ensure the creation and preservation of records throughout their command and serve as the command authority for the records management program, providing program oversight, policy interpretation and procedural guidance.

Records Center
A 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. NARA FRCs serving the Army are operated by GSA.

Records coordinator
Records official who serves below the RM at the unit/office level to ensure records management procedures are implemented.

Records Holding Area
A facility established to collect and maintain cutoff hardcopy records until they are either eligible for destruction or retirement to a NARA FRC or other records depository. When located outside of the CONUS, these facilities are referred to as OCRHAs.

Records inventory
A detailed listing that could include the types, locations, dates, volumes, equipment, classification systems, and usage data of an organization's records.

Records management officials
A collective term used to refer to RAs, RMs, and RCs.

Records manager
Records official who serves below the RA level at HQDA, the major subordinate and installation levels; in separately authorized activities, tenant organizations, and satellite organizations; and on installation garrison staff with command-wide or organizational-wide records management responsibilities. Although a single RM is normally assigned at each organizational element listed above, multiple RMs may be assigned as deemed necessary to meet the command's records management requirements.

Retention period
The length of time that a record must be kept before it is destroyed. Records not authorized for destruction have a retention period of permanent.

Retention Schedule
A document providing mandatory instructions for what to do with records (and non-record materials) no longer needed for current Government business, with provision of authority for the final disposition of recurring or nonrecurring records. Also called records disposition schedule, records retention schedule, records retention and disposition schedule, or schedule. The Army records schedules are contained in the ARIMS RRS–A.

Retire
The movement of records from an office, unit, or RHA into a NARA Records Center Facility.

Rights and interest records
Records essential to the preservation of the legal rights and interests of individual citizens (including service members) and the Army. These records include, accounts receivable records, social security records, payroll records, retirement records, insurance records, contract records, and so forth. Rights and interest records are one of two types of vital or essential records: the other type being emergency operating records.

Roll Microform
Microform consisting of microfilm on reels, cartridges, or cassettes.

Security classified information
Official records or information requiring protection against unauthorized disclosure. The degree of protection is specified by one of the following: TOP SECRET, SECRET, and CONFIDENTIAL.

Source documents
Documents containing images and/or data entered into a microform or electronic records system.

Special records collections
A group of records that may or may not fall under the same series, but which are considered to make up a collection based on common characteristics (for example, John F. Kennedy records collection).

Temporary records
Records approved by NARA for disposal, either immediately or after a specified retention period.

Transfer records
Records classified as "T" records which are long-term records with retention periods over 6 years and up through permanent. "T" records are transferred out of the CFA when no longer needed for business purposes.

Tuples
A data object that holds several objects, such objects are also known as a record.

Unscheduled records
Records that have not been formally appraised by NARA for disposition.

Website
A location on the Internet; specifically, it refers to the point of presence location in which it resides. All websites are referenced using a special addressing scheme called a uniform resource locater. A website can mean a single hypertext markup language (HTML) file or hundreds of files placed on the Internet by an enterprise.

Working papers
Documents such as rough drafts, calculations, or drafts that are assembled or created and used in the preparation or analysis of other documents. These documents are also considered records and are filed under the appropriate ARIMS RN.

SUMMARY of CHANGE

DA PAM 25–403
Army Guide to Recordkeeping

This administrative revision, dated 14 June 2023—

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

This administrative revision, dated 9 February 2023—

- Updates labeling procedures (para 4–15).

This major revision, dated 10 November 2022—

- Changes the title from Guide to Recordkeeping in the Army to Army Guide to Recordkeeping (cover).
- Simplifies and reorganizes information in accordance with DA Pam 25–40 (chap 1).
- Removes detailed responsibilities and adds guidance for appointing records management officials (para 1–5).
- Adds procedures for identifying records (fig 2–1).
- Updates guidance for “contractor records” and strengthens the requirements for record information created by contractors (para 2–5).
- Adds guidance for managing Federal Advisory Committee records (para 2–7).
- Emphasizes the need to inventory records throughout the entire life cycle (fig 2–2).
- Defines an active and inactive record (para 2–9).
- Adds guidance for maintaining information as records (para 2–11).
- Adds guidance for maintaining records for multiple organizations (para 2–13).
- Provides direction for conducting an inventory (para 2–15).
- Changes title from Managing the Various Types of Records Media to Records Management to Records Management (chap 3).
- Defines the Army Records Information Management System as a multi-function website containing the records retention schedule, the Army Electronic Archives and a suite of software tools to manage Army records (para 3–1).
- Revises relationship between record numbers and prescribing directives (table 3–1).
- Removes example DA Form 1613 (Records Cross Reference) (fig 3–1).

- Adds example of a rescinded record number label (fig 3–1).
- Adds examples of disposition codes and their meanings (table 3–2).
- Changes title from Applying Disposition Instructions to Managing Electronic Records to Managing Electronic Records (chap 4).
- Adds guidance on digital imaging (para 4–4).
- Adds types of electronic messages (table 4–1).
- Adds guidance for managing senior official emails under the Capstone approach (para 4–6).
- Adds guidance for maintaining social media content (para 4–12).
- Adds guidance for cloud computing (para 4–13).
- Adds guidance for maintaining electronic discovery content (para 4–15).
- Changes title from Scheduling Records to Managing Records (Media Neutral) to Managing Records (Media Neutral) (chap 5).
- Changes title from The Army Records Information Management System website to Scheduling Records (chap 6).
- Requires a comprehensive and clearly written migration plan be developed for new or enhanced information systems (para 6–3).
- Changes title from Records Transfer and Retirement to Records Dispositions to Records Disposition (chap 7).
- Removes sample Standard Form 135 transferring unscheduled records (fig 7–1).
- Adds the three types of disposition instructions in Army Records Information Management System based on time, event, and time plus event (figs 7–1, 7–2, and 7–3 .
- Adds guidance on disposing of record information with emphasis on electronic records and the media upon which it is stored (para 7–2).
- Changes title from Procedures and Services to Records Transfer and Retirement to Records Transfer and Retirement (chap 8).
- Provides detailed instructions regarding record freeze codes and adds guidance for returned/rejected records transfer requests (para 8–5).
- Changes title from Records Disposition to Reference Procedures and Services to Reference Procedures and Services (chap 9).
- Adds process to request access to the Archives and Records Centers Information System (para 9–2*b*).
- Augments instructions for the activation, change, or discontinuance of a records holding area (para 10–1).

- Changes title from Records Management Program Evaluations to Vital or Essential Records and Disaster Recovery Operations to Essential Records and Disaster Recovery Operations (chap 11).
- Expands on essential records and disaster recovery operations (chap 11).
- Changes title from Contingency Operation Records Collection and Preservation to Records Management Metrics to Record Management Metrics (chap 12).
- Adds guidance for records management metrics (chap 12).
- Provides direction for inspecting records (para 12–3).
- Updates procedures for Wartime and Contingency Operations Records (chap 13).
- Updates questions on the records management program evaluation (app B).
- Changes title from “Quick Reference Guide to Documenting Operations for Deployed Units of the Army” to “Wartime and contingency operations records” (app C).
- Provides a comprehensive listing of wartime and contingency record series (table C–1).
- Adds requirements for records management official appointment orders (app D).
- Adds duty appointment memorandum sample of records management officials (fig D–1).
- Adds outline and example of an Essential Records Program (app E).
- Changes the name from Records Management and Declassification Agency to Army Records Management Directorate (throughout).

- Changes the address of the Army Records Management Directorate (throughout).