



# Department of Defense **INSTRUCTION**

**NUMBER 5015.02**

February 24, 2015

---

---

DoD CIO

**SUBJECT:** DoD Records Management Program

**References:** See Enclosure 1

1. **PURPOSE.** This instruction reissues DoD Directive (DoDD) 5015.2 (Reference (a)) as a DoD instruction (DoDI) in accordance with the authority in DoDD 5144.02 (Reference (b)) to establish policy and assign responsibilities for the management of DoD records in all media, including electronic, in accordance with subchapter B, chapter XII, of Title 36, Code of Federal Regulations (CFR) and chapters 29, 31, 33, and 35 of Title 44, United States Code (References (c) and (d)).

2. **APPLICABILITY.** This instruction applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff (OCJCS) and the Joint Staff, the Combatant Commands (CCMDs), the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this instruction as the “DoD Components”).

3. **POLICY.** It is DoD policy that:

a. The information and intellectual capital contained in DoD records will be managed as national assets. Effective and efficient management of records provides the information foundation for decision making at all levels, mission planning and operations, personnel and veteran services, legal inquiries, business continuity, and preservation of U.S. history.

b. Records, regardless of media or security classification, will be created, maintained and used, disposed, and preserved to document the transaction of business and mission in wartime and peacetime. Records are evidence of DoD Component organization, functions, policies, procedures, decisions, and activities pursuant to References (c) and (d), and will be maintained in accordance with guidance issued by National Archives and Records Administration (NARA) and Office of Management and Budget M-12-18 (Reference (e)).

c. DoD records must be managed in compliance with this instruction and References (c) and (d) while protecting the legal and financial rights and interests of the Federal Government and of persons affected by U.S. Government (USG) activities.

d. Record schedules will be developed for all DoD records. Approval of the schedules must be obtained from NARA in accordance with Reference (c).

e. Sound records management principles must be incorporated into DoD business processes in accordance with the Department of Defense Chief Information Officer (DoD CIO) Memorandum (Reference (f)), the NARA Federal Enterprise Architecture Records Management Profile (Reference (g)), and statutory requirements..

(1) Records management requirements (as described in DoD 5015.02-STD (Reference (h))), issues, and solutions must be identified and linked to their implementing technologies and business processes.

(2) Records management requirements will be integrated into DoD Component information technology (IT) governance processes for portfolio management, capital planning, enterprise architecture, business process design, and system development.

f. The design, development, enhancement, and implementation of electronic information systems (EIS) must incorporate records management and preservation considerations, and must be managed in accordance with NARA-approved records disposition schedules.

(1) For new systems, records will be managed electronically by building recordkeeping functionality into the EIS or by transferring records to an electronic recordkeeping repository, such as a records management solution that is compliant with Reference (h).

(2) For existing systems, records will be managed electronically, manually, or a combination of both. To manage records electronically, recordkeeping functionality will be built into the EIS or records will be transferred to an electronic recordkeeping repository, such as a records management solution that is compliant with Reference (h).

g. Unstructured electronic records must be managed in a records management solution that is compliant with Reference (h), NARA Bulletin 2012-02 (Reference (i)), or NARA Bulletin 2013-02 (Reference (j)), as applicable. This includes records created using applications, electronic mail, and other messaging applications, word processing, or presentation software.

h. Electronic records and EIS must be interoperable at the DoD Component and interagency levels where data is shared or transferred to another federal agency, such as the Department of Veterans Affairs or NARA. Metadata, standards, and/or mediation will be used in accordance with DoDI 8320.02 and DoD CIO Memorandum (References (k) and (l)).

i. Vital records will be identified, protected, and managed to ensure they are available in the event of a catastrophic event to support continuity of operations in accordance with Reference (c).

j. DoD's ability to control the disclosure of official information (including assertion of privileges against disclosure) must not be impaired through unauthorized removal of non-record information. This applies to all non-record information, including those claimed as personal files. Non-record materials will be destroyed when no longer needed for business, at the discretion of the DoD Component.

k. DoD personnel will receive overview records management training annually in order to understand their responsibilities in managing DoD information as records and how to carry out these responsibilities.

4. RESPONSIBILITIES. See Enclosure 2.

5. RELEASABILITY. **Cleared for public release**. This instruction is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.

6. EFFECTIVE DATE. This instruction is effective February 24, 2015.



Terry A. Halvorsen  
Acting DoD Chief Information Officer

Enclosures

1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

- (a) DoD Directive 5015.2, "DoD Records Management Program," March 6, 2000 (hereby cancelled)
- (b) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," April 22, 2013
- (c) Subchapter B, chapter XII of Title 36, Code of Federal Regulations
- (d) Title 44, United States Code
- (e) Office of Management and Budget and National Archives and Records Administration M-12-18, "Managing Government Records Directive," August 24, 2012
- (f) Department of Defense Chief Information Officer Memorandum, "Defense Information Enterprise Architecture, Version 2.0," August 10, 2012
- (g) National Archives and Records Administration, "Federal Enterprise Architecture Records Management Profile, Version 1.0," December 15, 2005
- (h) DoD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard," April 25, 2007
- (i) National Archives and Records Administration Bulletin 2012-02, "Guidance on Managing Content on Shared Drives," December 6, 2011
- (j) National Archives and Records Administration Bulletin 2013-02, "Guidance on Managing a New Approach to Managing Email Records," August 31, 2013
- (k) DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013
- (l) Department of Defense Chief Information Officer Memorandum, "DoD Net-Centric Data Strategy," May 9, 2003
- (m) Office of Management and Budget Circular A-130, "Management of Federal Information Resources," November 28, 2000, as amended
- (n) DoD Directive 5100.03, "Support of the Headquarters of Combatant and Subordinate Unified Commands," February 9, 2011
- (o) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013
- (p) DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002, as amended
- (q) Federal Continuity Directive 1, "Federal Executive Branch National Continuity Program and Requirements," October 2012
- (r) DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006
- (s) Title 41, Code of Federal Regulations
- (t) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (u) DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 24, 2003
- (v) Title 10, United States Code

ENCLOSURE 2  
RESPONSIBILITIES

1. DoD CIO. The DoD CIO:

a. Develops and establishes DoD policy and standards to implement a DoD Records Management Program, including the life-cycle management of records in all media in accordance with References (b), (c), and (d).

b. Oversees DoD records management.

c. Serves as the DoD Senior Agency Official (SAO) for Records Management pursuant to Reference (e), ensuring compliance with References (c) and (d). Determines which DoD Components are required to designate Component SAOs for records management. Collaborates with the Component SAOs to fulfill the duties pursuant to Reference (e).

d. Appoints the DoD Records Officer to guide and coordinate the DoD Records Management Program. The DoD Records Officer collaborates with DoD Components and NARA to execute the DoD Records Management Program in accordance with this instruction and the responsibilities contained in section 1220.34 of Reference (c) and References (b) and (d).

e. Develops records management overview training to educate DoD personnel of their records management responsibilities pursuant to Reference (e). Maintains this DoD-wide training to ensure its relevancy and timeliness, and provides the training to Components for execution. The training will address:

(1) The responsibilities of DoD personnel related to the life-cycle management of records.

(2) The identification of records and how to distinguish them from non-records.

(3) The identification of personal papers and the need to maintain them separately from organizational records in compliance with Reference (c).

(4) The identification of electronic records and the need to manage them throughout their life cycle.

(5) The preservation of electronic mail records with attachments and metadata in accordance with Reference (c).

(6) The policies and procedures associated with copying and removal and destruction of government records and non-records. Records and non-record materials cannot be copied or removed from government custody or destroyed, except as authorized in accordance with References (c) and (d) and DoD policy.

(7) The designation and handling of personal files. An employee may remove only personal files. Email messages that include record or non-record material cannot be copied or removed as personal files because these messages were used to conduct DoD business. Non-record materials (paper or electronic) are government-owned and must be protected from unlawful removal or disclosure.

(8) The rules for removing and donating official records. Official records cannot be copied, including electronic mail records, solely for the purpose of removal or donation.

(9) The procedures to inform appropriate officials of any current, impending, or threatened unlawful removal, alteration, or destruction of records.

f. Identifies DoD Components that are required to have their designated records officer hold the NARA certificate of Federal Records Management training pursuant to Reference (e).

g. Cultivates a DoD records management community of interest by encouraging use of collaborative tools and technologies to distribute and evaluate the best practices and lessons learned in records and information management.

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in section 3 of this enclosure, the Director, DISA:

a. Establishes and maintains a test and evaluation program for certifying automated records management solutions that meet the standard functional and automated system requirements for records management in accordance with Reference (h).

b. Recommends to the DoD CIO any revisions to records management functional baseline requirements to be incorporated into Reference (h).

c. Establishes and maintains a register of automated records management solutions and active DoD recordkeeping systems that meet the standard functional and automated system requirements in Reference (h). Ready access to this register must be provided to all DoD records management personnel and be available at <http://jrtc.fhu.disa.mil/cgi/rma/reg.aspx>.

d. Develops and provides records management subject matter expertise for planning and executing the implementation and integration of electronic records management.

3. DoD COMPONENT HEADS. The DoD Component heads:

a. Establish, sufficiently resource, and maintain a DoD Component records management program at an organizational level of sufficient authority to ensure this instruction and References (c) and (d) are efficiently and effectively implemented. Designate a records officer

to administer the Component program and provide written notification of designation to the DoD SAO.

b. Appoint a Component SAO, as directed by the DoD CIO.

c. Use the most economical, efficient, and reliable means to create, maintain and use, dispose, and preserve Component records in any media in accordance with References (c) and (d), Office of Management and Budget Circular A-130 (Reference (m)), and DoDD 5100.03 (Reference (n)).

d. Implement records management controls and accountability standards necessary to capture, manage, and preserve Component records, including electronic records and electronic messages and their attachments, using internal controls in accordance with DoDI 5010.40 (Reference (o)).

e. For operational records, support the Combatant Commanders' (CCDRs) operational plans for managing records throughout their life cycle. Records generated as a result of campaigns and contingency operations in the CCMD area(s) of operation (AO) are operational records and must be managed pursuant to this instruction. Administrative records are the responsibility of the DoD Component head.

f. For any DoD Executive Agent designations in accordance with DoDD 5101.1 (Reference (p)), require any records that document the transaction of business and mission of the DoD Executive Agent are managed according to current records management policy. Assign records management responsibilities to Components consistent with the DoD Executive Agent designation and determine the processes that will be used.

g. Establish a vital records program to identify and preserve vital records. The vital records program will ensure vital records are maintained, revised and, where appropriate, available in the occurrence of a catastrophic event for continuity of operations in accordance with Reference (c) and consistent with Federal Continuity Directive 1 (Reference (q)).

h. Require that records contained in Component EISs are managed and scheduled in accordance with Reference (c). For Component EISs, register the EIS in the DoD IT Portfolio Repository (DITPR) in accordance with DoDI 8115.02 (Reference (r)). For those Component EISs that contain records, populate and maintain the associated DITPR records management data elements.

i. Deploy and use a records management solution that is compliant with References (h), (i), and/or (j) to manage unstructured electronic records pursuant to this instruction and Reference (e) no later than 5 years after the effective date of this publication.

j. Ensure all personnel complete annual overview training. This includes incorporating necessary requirements into contracts to ensure overview training is accomplished for defense contractors who create or receive records. The training will educate both DoD personnel and defense contractors on their records management responsibilities using the DoD records

management overview training developed by the DoD CIO. Augment the overview training with Component-specific information to address:

(1) Maintenance of personal papers separately from organizational records in compliance with Reference (c).

(2) Management of electronic records throughout their life cycle, including instructions for disposition and assigning metadata if managed within a DoD-approved recordkeeping system.

(3) Preservation of electronic mail records with attachments and metadata in accordance with Reference (c).

k. Advise senior leaders of their record management responsibilities within the first 30 days of assumption of duties. Provide out-briefings to senior leaders to ensure capture of the records generated during their tenure.

l. Direct defense contractors performing DoD program functions to create and maintain records to document these functions. Contracts must specify the delivery to the USG of all the data required for adequate documentation of the contractor-operated program in accordance with parts 102 through 193 of Title 41, CFR (Reference (s)).

m. Oversee prompt retirement or disposal of temporary records and the timely transfer of permanent records to NARA for preservation under NARA-approved record schedules.

n. Monitor Component compliance with the DoD Records Management Program and Reference (c), and implement corrective actions as deemed necessary.

o. Advise the DoD CIO of records management issues that could have broad implications across DoD or between DoD and other government agencies, and fully cooperate with the DoD CIO in resolving these issues.

p. Work with the DoD CIO to coordinate responses to existing, new, or changing records management requirements in accordance with Reference (e).

q. Safeguard all personal data within records, in accordance with DoD 5400.11-R (Reference (t)). Protect all personal data within health-related records in accordance with DoD 6025.18-R (Reference (u)).

r. Require requests for removal of non-record materials outside of DoD be reviewed by proper DoD authority, as designated by the DoD Component head. Unclassified documents, including electronic mail, are not automatically publicly releasable and must be reviewed for release to departing officials or employees.

s. Maintain accountability of records when they are loaned and transferred to other DoD Components or federal agencies, and accept possession and management responsibility when the



loaned records are returned to the Component. Continue life-cycle management of the records in accordance with NARA-approved records disposition schedules.

4. CHAIRMAN OF THE JOINT CHIEFS OF STAFF (CJCS). In addition to the responsibilities in section 3 of this enclosure, the CJCS:

a. Develops, implements, evaluates, and refines records management policies and procedures for programs and organizations for which the OCJCS has oversight, including joint operation planning.

b. Requires each CCDR to develop and implement plans and procedures so that all information and records created or received by the CCMD are identified, safeguarded, and properly managed.

c. Oversees and assesses records management programs for which the OCJCS has oversight by reviewing the efficient life-cycle management of records and the scheduling of records in accordance with References (c) and (d). Monitors the compliance of the CCDR and other supervised activities with this instruction, directs corrective action be implemented as necessary, and notifies the DoD CIO of any issues and recommended resolutions.

5. CCDRs. In addition to the responsibilities in section 3 of this enclosure, the CCDRs:

a. Are responsible for operational records to ensure proper management of these records throughout their life cycle. CCDRs may task any subordinate unit or command, including Service component commands and theater special operations commands, to fulfill this responsibility in accordance with the CCMD established priorities, operational guidance, and CCDR intent.

b. Assign and document accountability for the management and ownership of operational records during deliberate and crisis action planning and throughout the operation.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AO	area of operation
CCDR	Combatant Commander
CCMD	Combatant Command
CFR	Code of Federal Regulations
CJCS	Chairman of the Joint Chiefs of Staff
DISA	Defense Information Systems Agency
DITPR	DoD Information Technology Portfolio Repository
DoD CIO	DoD Chief Information Officer
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
EIS	electronic information system
IT	information technology
OCJCS	Office of the Chairman of the Joint Chiefs of Staff
NARA	National Archives and Records Administration
SAO	Senior Agency Official
USG	United States Government

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this instruction.

administrative records. Those records created by all Joint or Single Service Military organizations, regardless of organizational level, in performing common functions that support the organization's mission activities, but do not directly document the performance of mission functions. Administrative records relate to activities such as budget and finance, human resources, medical, equipment and supplies, facilities, public and congressional relations, contracting, and similar administrative housekeeping or facilitative functions common to most agencies.

campaign. A series of related major operations aimed at achieving strategic and operational objectives within a given time and space.

contingency operation. A military operation that is either designated by the Secretary of Defense as a contingency operation or becomes a contingency operation as a matter of law pursuant to chapter 1 of Title 10, United States Code (Reference (v)).

defense contractor. Any person who enters into a contract with the USG for the production of material or for the performance of services for national defense.

DoD personnel. Military and civilian employees of the DoD.

EIS. An information system that contains and provides access to computerized federal records and other information.

electronic records. Any information that is recorded in a form that only a computer can process and that satisfies the definition of a federal record pursuant to chapter 31 of Reference (d), also known as the “Federal Records Act.” The term includes both record content and associated metadata that the agency determines is required to meet agency business needs.

intellectual capital. Intellectual capital is the value associated with the knowledge, applied experience, organizational technology, synergistic interface (corporate-private-public collaboration), and professional skills that provide an organization with relevance within the DoD.

interoperable. The condition achieved among communications-electronics systems or items of communications-electronics equipment when information or services can be exchanged directly and satisfactorily between them and their users.

metadata. Information describing the characteristics of data; data or information about data; or descriptive information about an entity’s data, data activities, systems, and holdings. For example, discovery metadata is a type of metadata that allows data assets to be found using enterprise search capabilities.

non-record materials. Federally owned informational materials that do not meet the statutory definition of records in accordance with section 3301 of Reference (d), or that have been excluded from coverage by the definition. Excluded materials are extra copies of documents kept only for reference, stocks of publications and processed documents, and library or museum materials intended solely for reference or exhibit.

operation. A military action or the carrying out of a strategic, operational, tactical, service, training, or administrative military mission.

operational records. Records and information in any medium (paper or electronic) created or received during the planning or execution of campaigns and contingency operations within a CCMD’s AO. Records generated as result of operational level actions such as fragmentary orders, situation reports, military intelligence summaries, etc., are considered operational records. Information dealing with internal administrative matters or any other record whose

creation is solely required through a Service regulation is not considered operational records for this purpose. See administrative records.

personal files (also called personal papers). Documentary materials belonging to an individual that are not used to conduct agency business. Personal files are excluded from the definition of federal records and are not owned by the USG.

record. All books, papers, maps, photographs, machine-readable materials, and other documentary materials, regardless of physical form or characteristics, made or received by an USG agency under federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that federal agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the USG or because of the informational value of the data in them (in accordance with section 3301 of Reference (c)). A DoD record also includes operational logistics, analysis, support, and other materials created or received by the DoD Components in training, contingency, and wartime operations as well as in all routine and peacetime business.

recordkeeping system. Manual or electronic system that captures, organizes, and categorizes records to facilitate their preservation, retrieval, use, and disposition.

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

unstructured electronic records. Records created using office automation applications, such as electronic mail and other messaging applications, word processing, or presentation software.

vital records. Essential federal agency records that are needed to meet operational responsibilities under national security emergencies or other emergency conditions or to protect the legal and financial rights of the USG and those affected by USG activities.