Department of Defense
INSTRUCTION

NUMBER 5015.02
February 24, 2015
Incorporating Change 1, August 17, 2017

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:

a. 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").

b. DoD information created, received, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the DoD, in any medium or form, including information managed by DoD or a third party on behalf of DoD.

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), Office of Management and Budget (OMB) M-12-18 (Reference (e)), and OMB Circular A-130 (Reference (f)).

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. Essential records (formerly vital records) will be identified, protected, and managed to ensure availability after an event that disrupts normal operations to support continuity of operations and to protect rights and interests in accordance with Reference (c).

e. All DoD records will be covered by a records schedule. Approval of the schedules must be obtained from NARA in accordance with Reference (c).

f. All permanent electronic records will be managed electronically for eventual transfer and accessioning to NARA in an electronic format.

g. 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 (g)), the NARA Federal Enterprise Architecture Records Management Profile (Reference (h)), and statutory requirements.

(1) Records management requirements (as described in DoD 5015.02-STD (Reference (i))), 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, risk management, capital planning, enterprise architecture, business process design, and system development.

h. The acquisition, development, and enhancement of electronic information systems (EIS) and IT services must incorporate records management and preservation considerations, and any records contained in the systems or IT services must be managed in accordance with NARA-approved records disposition schedules.

(1) For new EIS and IT services, records will be managed electronically by recordkeeping functionality provided by the EIS or IT service, or by transferring records to an electronic recordkeeping repository, such as a records management solution that is compliant with Reference (i).

(2) For existing EIS and IT services, records will be managed electronically, manually, or a combination of both. To manage records electronically, recordkeeping functionality will be

provided by the EIS or IT service, or records will be transferred to an electronic recordkeeping repository, such as a records management solution that is compliant with Reference (i).

i. Records created, sent, or received using electronic messaging accounts must be managed electronically, including the capability to identify, retrieve, and retain records for as long as they are needed, in accordance with part 1236.22 of Reference (c) and in accordance with Reference (i), NARA Bulletin 2012-02 (Reference (j)), or NARA Bulletin 2013-02 (Reference (k)), as applicable.

j. Unstructured electronic records, other than electronic messages, must be managed in a records management solution that is compliant with Reference (i) or Reference (j), as applicable. This includes records created using any electronic applications.

k. Electronic records, EIS, and IT services 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 (Reference (l)).

l. Records and non-record materials are government-owned and cannot be copied or removed from government custody or destroyed, except as authorized in accordance with References (c) and (d) and DoD Component guidance. This applies to electronic messages used to conduct DoD business because electronic messages include record and/or non-record material and cannot be copied, transferred, or removed as personal files. Non-record materials will be destroyed when no longer needed for business, at the discretion of the DoD Component.

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

n. Non-official electronic messaging accounts, with very few exceptions, must not be used to conduct official DoD communications in accordance with DoDI 8550.01 (Reference (m)). If a DoD employee uses a non-official electronic messaging account, the employee must copy the message to his or her official electronic messaging account when the record is first transmitted, or must forward a complete copy of the record to their official electronic messaging account within 20 days of the record's original creation or transmission pursuant to Reference (d).

4. RESPONSIBILITIES. See Enclosure 2.

5. RELEASABILITY. **Cleared for public release**. This instruction is available on the Directive Division Website at http://www.esd.whs.mil/DD/.

6. SUMMARY OF CHANGE 1. The changes to this issuance account for changes in statute and evolving technology. They also update references and acronyms.

7. 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)," November 21, 2014, as amended
(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) Office of Management and Budget Circular A-130, "Managing Information as a Strategic Resource," July 28, 2016
(g) Department of Defense Chief Information Officer Memorandum, "Defense Information Enterprise Architecture, Version 2.0," August 10, 2012
(h) National Archives and Records Administration, "Federal Enterprise Architecture Records Management Profile, Version 1.0," December 15, 2005
(i) DoD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard," April 25, 2007
(j) National Archives and Records Administration Bulletin 2012-02, "Guidance on Managing Content on Shared Drives," December 6, 2011
(k) National Archives and Records Administration Bulletin 2013-02, "Guidance on a New Approach to Managing Email Records," August 31, 2013
(l) DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013
(m) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
(n) National Archives and Records Administration Bulletin 2017-01, "Agency Records Management Training Requirements," November 29, 2016
(o) DoD Directive 5100.03, "Support of the Headquarters of Combatant and Subordinate Unified Commands," February 9, 2011, as amended
(p) DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013
(q) DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002, as amended
(r) DoD Instruction 3020.42, "Defense Continuity Plan Development," April 27, 2011
(s) Federal Continuity Directive 1, "Federal Executive Branch National Continuity Program and Requirements," October 2012
(t) DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006
(u) Title 41, Code of Federal Regulations
(v) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
(w) DoD Instruction 6025.18, "Privacy of Individually Identifiable Health Information in DoD Health Care Programs," December 2, 2009
(x) 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 for Records Management (SAORM) pursuant to Reference (e), ensuring compliance with References (c) and (d). Determines which DoD Components are required to designate Component SAORMs. Collaborates with the Component SAORMs 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. Provides records management training, as required, to educate DoD personnel of their records management responsibilities, in accordance with NARA Bulletin 2017-01 (Reference (n)) and pursuant to Reference (e). Maintains this DoD-wide training to ensure its relevancy and timeliness, and provides the training to DoD Components for execution.

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 (i).

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

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 (i). Ready access to this register must be provided to all DoD records management personnel and be available at http://jitc.fhu.disa.mil/projects/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 SAORM. As directed by the DoD CIO, ensure the designated records officer holds the NARA Certificate of Federal Records Management Training within 1 year of designation pursuant to Reference (e).

b. Appoint a Component SAORM, as directed by the DoD CIO. Component SAORM will collaborate with the DoD SAORM to fulfill the SAORM responsibilities pursuant to Reference (e).

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), (d), and (f), and DoDD 5100.03 (Reference (o)).

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 (p)).

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 (q)), 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 an essential records program to identify and preserve essential records (formerly vital records). The essential records program will ensure essential records are maintained, revised and, where appropriate, available after an event that disrupts normal in accordance with Reference (c) and DoDI 3020.42 (Reference (r)) and consistent with Federal Continuity Directive 1 (Reference (s)).

h. For any EIS or IT service developed, acquired, or provided by the Component, require that records contained in the EIS or IT service are managed and scheduled in accordance with Reference (c). Register the EIS or IT service in the DoD IT Portfolio Repository (DITPR) in accordance with DoDI 8115.02 (Reference (t)). For those EISs and IT services that contain records, populate and maintain the associated DIPTR records management data elements.

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

j. Ensure all personnel complete annual records training. This includes incorporating necessary requirements into contracts to ensure records training is accomplished for contractors who create, receive, use, or maintain records. The training will educate DoD personnel and contractors on their records management responsibilities as appropriate.

k. Provide records management training for the staff responsible for the Component's records management program and operations.

l. 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.

m. Direct 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 (u)).

n. Oversee prompt retirement or disposal of temporary records and the timely transfer of permanent records to NARA for preservation under NARA-approved record schedules. Transfer permanent records to NARA in digital or electronic form to the greatest extent possible.

o. Notify the Archivist of the United States of any actual, impending, or threatened unlawful removal, defacing, alteration, corruption, deletion, erasure, or other destruction of records in the custody of the Component pursuant to Reference (d). With the assistance of the Archivist, initiate action through the United States Attorney General for the recovery of records. Inform the DoD SAORM when the notification concerns permanent or long-term records, impacts more than one Component, or attracts interest or scrutiny from other agencies, Congress, or the public.

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

q. Advise the DoD SAORM 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.

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

s. Safeguard all personal data within records, in accordance with DoDD 5400.11 (Reference (v)). Protect all personal data within health-related records in accordance with DoDI 6025.18 (Reference (w)).

t. 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 e-mail, are not automatically publicly releasable and must be reviewed for release to departing officials or employees.

u. 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	DoD directive
DoDI	DoD instruction
EIS	electronic information system
IT	information technology
OCJCS	Office of the Chairman of the Joint Chiefs of Staff
OMB	Office of Management and Budget
NARA	National Archives and Records Administration
SAORM	Senior Agency Official for Records Management
USG	U.S. Government

PART II. DEFINITIONS

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

administrative records. Those records created by all DoD 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 (x)).

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 electronic federal records, electronic messages, and other information.

electronic messages. E-mail and other types of electronic messages that people use to communicate. This includes, but is not limited to, messages created by chat, text, and e-mail systems.

electronic messaging account. Any account that sends or receives electronic messages.

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.

essential records (formerly vital records). Records an agency needs to meet operational responsibilities during national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the USG and those affected by USG activities.

essential records program. The policies, plans, and procedures the agency develops and implements – and the resources needed – to identify, use, and protect essential records. This is a program element of an agency's emergency management function.

IT service. Engagement of the time and effort of a service provider, through the use of IT, whose primary purpose is to perform an identifiable task, or tasks, rather than provide an end item of supply.

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 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 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.

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

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 e-mail and other messaging applications, word processing, or presentation software.