ADMINISTRATIVE INSTRUCTION 15

OSD RECORDS AND INFORMATION MANAGEMENT PROGRAM

Originating Component:	Office of the Director of Administration and Management
Effective:	November 27, 2023
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	Administrative Instruction 15, "OSD Records and Information Management Program," May 3, 2013, as amended
Approved by:	Regina M. Meiners, Director, Washington Headquarters Services

Purpose: In accordance with the authority in DoD Directive (DoDD) 5110.04 and DoD Instruction (DoDI) 5025.01, this issuance:

- Implements policy, assigns responsibilities, and provides procedures for the OSD Records and Information Management (RIM) Program in accordance with the policy in DoDI 5015.02; Chapters 29, 31, and 33 of Title 44, United States Code (U.S.C.); and Subchapter B of Chapter XII of Title 36, Code of Federal Regulations (CFR).
- Assigns responsibilities and provides administrative procedures regarding the life-cycle management of records and information program within the OSD Components, OSD RIM Program-serviced Defense Agencies and DoD Field Activities (DAFAs) and DoD Advisory Committees, referred to collectively in this issuance as the "Washington Headquarters Services (WHS)-serviced Components."

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to:

a. OSD and the OSD RIM Program-serviced DAFAs.

b. All advisory committees established and utilized by the DoD, including those advisory committees exempted from Chapter 10 of Title 5, U.S. C. (also known and referred to in this issuance as the "Federal Advisory Committee Act").

c. OSD records and information created, received, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the OSD or OSD RIM Program-serviced DAFAs, in any medium regardless of form, format, function, classification, or location. This includes information systems managed by OSD employees, Service members, contractors, and third parties on behalf of an OSD Component or OSD RIM Program-serviced DAFA.

1.2. POLICY.

In accordance with DoDI 5015.02:

a. And in compliance with Chapter 29 of Title 44, U.S.C., the WHS-serviced Components will limit the creation of records to those essential for the efficient conduct of official business and to preserve those of continuing value. All other records will be systematically eliminated.

b. Records will be managed in compliance with Chapters 21, 25, 29, 31, and 33 of Title 44, U.S.C.; Part 102-193 of Title 41, CFR; and Subchapter B of Chapter XII of Title 36, CFR.

c. The information and intellectual capital contained in DoD records are managed as national assets. Effective and efficient management of records provides the information foundation for:

(1) Decision making at all levels.

(2) Mission planning and operations.

(3) Personnel and veteran services.

(4) Legal inquiries.

(5) Business continuity.

(6) Preservation of U.S. history.

d. Electronic records are also maintained in accordance with Office of Management and Budget (OMB) Circular No. A-130. These U.S. Government-wide requirements include:

(1) Managing all permanent electronic records electronically to the fullest extent possible for eventual transfer and accessioning to the National Archives and Records Administration (NARA) in an electronic format.

(2) Managing all records created via e-mail accounts or e-messaging accounts electronically and retaining them in appropriate electronic system(s) that support records management, information management, and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as legally required.

(3) Ensuring the ability to access, retrieve, and manage electronic records throughout their life cycle regardless of form or medium.

e. Federal records will be disposed of in a proper and timely manner in accordance with retention schedules approved by the Archivist of the United States pursuant to Chapter 33 of Title 44, U.S.C.

f. All personnel creating and receiving records and information within the WHS-serviced Components will be trained as appropriate regarding their Federal records management responsibilities.

g. Non-official e-messaging should not be used for the conduct of U.S. Government official business. If personnel use a non-official e-messaging account, they must:

(1) Copy the message to their official e-messaging account when the record is first transmitted; or

(2) Forward a complete copy of the record to their official e-messaging account within 20 days of the record's original creation or transmission pursuant to Section 2911 of Title 44, U.S.C.

1.3. TERMINOLOGY CLARIFICATION.

Throughout this issuance, the terms "must" and "will" denote a requirement with which management will comply in all cases. "Should" indicates a presumptively mandatory requirement except in circumstances where the requirement is not relevant or reason for not satisfying the requirement can rationally be explained to the involved leadership. "May" or "could" indicates best practices that may be adopted at the discretion of the involved leadership.

SECTION 2: RESPONSIBILITIES

2.1. DIRECTOR, WHS.

Under the authority, direction, and control of the Performance Improvement Officer/Director of Administration and Management (PIO/DA&M), the Director, WHS, designates the Director, Executive Services Directorate (ESD) to serve as the OSD Senior Agency Official for Records Management (SAORM).

2.2. DIRECTOR, ESD.

Under the authority, direction, and control of the PIO/DA&M, through the Director, WHS, and in their capacity as the OSD SAORM, the Director, ESD:

a. Has overall responsibility for the OSD RIM Program within the WHS-serviced Components in accordance with Chapters 31 and 33 of Title 44, U.S.C.; Part 102-193 of Title 41, CFR; Subchapter B of Chapter XII of Title 36, CFR; OMB Circular No. A-130; and OMB/NARA Memorandums M-19-21 and M-23-07.

b. Cooperates with NARA in:

(1) Developing and applying standards, procedures, and techniques designed to improve the management of records and information.

(2) Ensuring the maintenance, accessibility, and security of records of continuing value as defined in the NARA Guide to the Inventory, Scheduling, and Disposition of Federal Records.

(3) Facilitating the identification, segregation, and disposal of all records of temporary value and non-record information.

c. Designates the Chief, Records and Declassification Division (RDD) as the Federal Records Officer for the WHS-serviced Components.

d. Advocates for the OSD RIM Program, ensuring the WHS-serviced Components are documenting their activities and decisions.

e. Coordinates with the DoD Chief Information Officer (CIO) in their capacity as the DoD SAORM, as well as the DoD Component SAORMs (as necessary) on DoD-wide or other interdepartmental RIM policies or issues pertaining to information technology (IT) and electronic records, in accordance with OMB Circular No. A-130 and DoDI 5015.02.

f. Advocates for RIM as an integral component of information governance and information resource management.

g. Ensures the OSD RIM Program is adequately resourced to conduct its overall responsibilities including:

(1) Coordinating with related programs such as the DoD Risk Management Framework Program, legal and electronic discovery, information collections, privacy, and the DoD Freedom of Information Act Program, in accordance with OMB Circular No. A-130.

(2) Establishing internal policies regarding program objectives, responsibilities, and authorities for the creation, maintenance, and disposition of agency records.

(3) Overseeing OSD's transition to digital government, in accordance with OMB/NARA Memorandums M-19-21 and M-23-07, OMB Circular No. A-130, and NARA bulletins.

(4) Submitting reports to NARA supporting records management inspections and other oversight activities.

(5) Informing and training WHS-serviced Component personnel on their records management responsibilities in accordance with NARA regulations and guidance.

h. Consults with the WHS-serviced Component CIOs, data officers, and senior Component officials for privacy concerning information systems and components that cannot be appropriately protected or secured. Ensures that such systems are given a high priority for upgrade, replacement, or retirement.

i. Ensures the WHS-serviced Components' records and information are treated as information resources and national assets, in accordance with OMB Circular No. A-130 and DoDI 5015.02, respectively.

j. Ensures the WHS-serviced Components' ability to control disclosure of official information, including assertion of privileges against disclosure, is not impaired through unauthorized removal of non-record information.

2.3. CHIEF, RDD.

Under the authority, direction, and control of the PIO/DA&M, through the Director, WHS, via the Director, ESD, and in their capacity as the OSD Records Administrator, the Chief, RDD:

a. Directs, administers, and oversees the OSD RIM Program.

b. Serves as the Federal Records Officer for the WHS-serviced Components, in accordance with:

(1) Chapters 31 and 33 of Title 44, U.S.C.

(2) Parts 1220 through 1239 of Title 36, CFR.

(3) Part 102-193 of Title 41, CFR.

(4) The Federal Advisory Committee Act.

(5) OMB Circular No. A-130.

(6) DoDI 5015.02.

(7) DoD Manual (DoDM) 5230.30.

(8) DoDI 8170.01.

(9) Administrative Instruction 50.

c. Oversees the implementation of this issuance as the Federal Records Officer for the WHS-serviced Components.

d. Advises the OSD SAORM on records management issues that could have broad implications across OSD, DoD, or between DoD Components and other government agencies.

e. Acts as the liaison official with NARA, other government agencies, private industry, and private citizens on RIM matters involving the WHS-serviced Components.

f. In accordance with Parts 1220 through 1239 of Title 36, CFR; Part 102-193 of Title 41, CFR; and Executive Order (E.O.) 13526, institutes and oversees a records management evaluation program to:

(1) Ensure the WHS-serviced Components' compliance with this issuance and the OSD Records and Information Management Program Primer (also known and referred to in this issuance as the "OSD Primer").

(2) Provide for improvements and changes to existing procedures and records schedules to reflect current mission and the WHS-serviced Components' requirements.

(3) Coordinate with the Secretaries of the Military Departments and Chairman of the Joint Chiefs of Staff on the development and submission of OSD and DoD-wide records disposition schedules (RDSs) as appropriate.

g. Directs, administers, and provides oversight of the OSD RIM Program by ensuring the WHS-serviced Components:

(1) Maintain accurate and complete documentation of Federal Government policies and transactions.

(2) Implement a systematic process for the preservation and disposal of records.

(3) Ensure personnel (whether civilian, military, contractors, or volunteers) do not remove records and copies of government–owned non-record information (hard copy or electronic) from government custody that are not cleared for public use. See the OSD Primer and Section 10 of this issuance for additional guidance on RIM policies and procedures for removal of OSD records and information.

(4) Serve as the approval authority for the release and component to component of non-record copies of OSD records and information for all OSD Presidential appointees (PAs),

Presidentially appointed, Senate-confirmed (PAS) individuals, and senior officials designated as CAPSTONE officials in accordance with Part 1222.24(a)(6) of Title 36, CFR, and NARA General Records Schedule (GRS) 6.1.

(5) Initiate controls to protect DoD records and information from unauthorized disclosure, including DoD assertion of privilege, spillage, or personally identifiable information (PII) breaches.

(6) Provide guidance to their program offices on the creation, organization, maintenance, use, and disposition of records and information they produce and receive.

(7) Ensure positive control over the organization, maintenance, use, designation, and disposition of records and information, regardless of media (hard copy, electronic, audiovisual, etc.).

(8) Coordinate with the OSD CIO and WHS-serviced Components CIOs or IT service providers to ensure the implementation of capabilities to access, retrieve, and manage records throughout their lifecycle, regardless of format or medium.

(9) Report to the Archivist of the United States any actual, impending, or threatened unlawful removal, alteration, or destruction of Federal records.

h. Advises the WHS-serviced Components' RIM personnel, IT service providers, information system owners, and program managers on records management requirements and functionality when creating new or updating existing records, as well as Federal information systems (FISs), to ensure:

(1) The systems adequately document, secure, and access electronic records.

(2) Disposition instructions are established and implemented.

i. Develops and applies standards, procedures, and techniques for:

(1) Improving records management.

(2) Ensuring the maintenance and timely retirement of records of continuing value.

(3) Facilitating the segregation and disposal of all records of temporary value.

j. Provides WHS-serviced Component personnel with basic and content specific RIM training, in accordance with Chapters 31 and 33 of Title 44, U.S.C.; Parts 1220 through 1239 of Title 36, CFR; and NARA Bulletin 2017-01.

k. Advises and assists the WHS-serviced Components with the identification, segregation, retention, and disposition of all records, including personal files, in accordance with Chapters 31 and 33 of Title 44, U.S.C. and Subchapter B of Chapter XII of Title 36, CFR.

l. Coordinates, controls, and supervises access to OSD records essential for historical research, following appropriate safeguards for information security and personal privacy, in accordance with OMB Circular No. A-130, DoDM 5400.07, and DoD 5400.11-R.

m. Establishes and obtains the approval of the Archivist of the United States for RDSs by:

(1) Coordinating the review of the OSD RDS with the WHS-serviced Components to ensure program, functional, and mission offices are identifying new subject matter or updating and maintaining existing file numbers to reflect current business needs.

(2) Maintaining the OSD RDS at https://www.esd.whs.mil/RIM as NARA approves new or revised disposition schedules applicable to the WHS-serviced Components or revises the GRS citations.

n. Manages the transfer and retrieval of the WHS-serviced Components records and information to the Federal records centers (FRCs) and accessions permanent records to the U.S. National Archives.

o. Maintains a record of all current suspension actions to normal disposition instructions such as records holds, freezes, moratoriums, litigation holds, or preservation notices.

2.4. GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE (GC DOD).

The GC DoD will provide legal direction as needed to the WHS-serviced Components with regards to:

a. Compliance with legal and regulatory requirements applicable to RIM activities.

b. Issuing and processing moratoriums such as litigation holds or preservation notices; removal of personal and non-record copies of OSD records and information; and electronic records management as described in this issuance.

2.5. WHS-SERVICED COMPONENT HEADS.

The WHS-serviced Component heads:

a. Establish and sufficiently resource a RIM program within their program offices in accordance with Chapters 31 and 33 of Title 44, U.S.C.; Parts 1220 through 1239 of Title 36, CFR; and Part 102–193 of Title 41, CFR.

b. Use standards, procedures, and techniques to ensure the most economical, efficient, and reliable means for creation, retrieval, maintenance, preservation, and disposition of their records, regardless of media.

c. Institute measures to ensure that records of continuing value are preserved and inactive records receive appropriate disposition in accordance with the OSD RDS.

d. Identify appropriate officials responsible for implementing mandatory regulatory RIM compliance requirements as identified in Section 3 of this issuance.

e. Appoint personnel to serve in accountable records management roles within their components, divisions, and offices as follows:

(1) OSD Component heads will appoint a Component records management officer (CRMO); OSD RIM Program-serviced DAFA directors will appoint a DAFA records manager (RM); and DoD Advisory Committee heads will appoint a DoD Advisory Committee RM. These appointed individuals are referred to collectively in this issuance as the "WHS-serviced Component CRMOs and RMs."

(2) Appointments will be made in writing and a copy furnished to the OSD Records Administrator. Appointment memorandums are updated upon the departure or change of the individual(s).

(3) WHS-serviced Component CRMOs and RMs:

(a) Are responsible for coordinating and overseeing the implementation of the records management requirements throughout their WHS-serviced Component and serve as the accountable records custodian (RC) within their organization.

(b) Serve as their WHS-serviced Component's primary point of contact for the OSD RIM Program and the OSD Records Administrator.

(c) Maintain a list of personnel appointed to their reporting components, divisions, and offices in accordance with Paragraph 2.5.e.(4).

(d) Coordinate with training coordinators to ensure all OSD employees, Service members, and contract personnel assigned to their Component complete basic records management training annually to maintain compliance with Chapters 31 and 33 of Title 44, U.S.C.; Parts 1220 through 1239 of Title 36, CFR; Part 102–193 of Title 41 CFR; DoDI 5015.02; and this issuance.

(4) All WHS-serviced Components' reporting components, divisions, and offices will appoint RMs, records liaisons (RLs), or RCs to oversee their implementation and maintenance of the RIM Program.

(a) WHS-serviced Components' reporting components, directorates, and divisions levels will each assign an RM.

(b) WHS-serviced Components' program, function, or mission offices will assign RLs or RCs.

f. Implement records management functions and retention and disposition requirements into information life-cycle processes and stages. This includes the design, development, implementation, and decommissioning of FISs, to include storage solutions and cloud-based services such as software as a service, platform as a service, and infrastructure as a service. (See

Section 6 of the OSD Primer for records management functions and retention and disposition requirements).

g. Maintain OSD records and information posted to commercial and government-owned social networking sites (SNSs) or web 2.0 technology in accordance with Title 36, CFR, and the OSD RDS. Bring to the attention of the OSD Records Administrator any records and information created or received during the conduct of business and maintained in these systems that do not have an approved records disposition identified in the OSD RDS.

h. Plan and budget for the migration of records and their associated metadata maintained in FISs or database to new storage media or persistent formats to avoid loss of record data due to media decay or outdated technology.

i. Protect records and information against unauthorized removal or loss, and ensure all personnel are informed of their records management responsibilities in accordance with Section 3106 of Title 44, U.S.C.; Part 1230 of Title 36, CFR; and DoDI 5015.02. See Section 5 of the OSD Primer for unauthorized disposition reporting procedures.

j. Manage electronic records in accordance with NARA and DoD-wide requirements. This includes:

(1) Managing all permanent records electronically to the fullest extent possible for eventual transfer to and accessioning by NARA in an electronic format, in accordance with OMB/NARA Memorandums M-19-21 and M-23-07.

(2) Managing all e-mail and e-message records electronically and retaining them in an appropriate electronic system(s) that supports records management and litigation requirements, including the capability to identify, retrieve, and retain the records for as long as they are needed.

(3) Maintaining an inventory of all information systems the WHS-serviced Component has developed or acquired to support its programmatic responsibilities to meet the requirements of Section 3505(c) of Title 44, U.S.C., and Part 1236.26 of Title 36, CFR.

(4) Identifying the appropriate RDS when requesting the approval of DoD information collections in accordance with DoDM 8910.01.

k. In accordance with Section 552a of Title 5, U.S.C., also known and referred to in this issuance as the "Privacy Act of 1974"; OMB Circular No. A-130; DoD 5400.11-R; and DoDI 8510.01, ensure FISs containing PII are:

(1) Implementing appropriate privacy safeguards, including storage solutions and cloud-based services such as software as a service, platform as a service, and infrastructure as a service.

(2) Retained in accordance with the OSD RDS. See Paragraph 11.4. of this issuance and Section 8 of the OSD Primer for guidance on implementing appropriate privacy safeguards into OSD records and information.

l. Ensure that WHS-serviced Component functions, programs, and organizations identify and preserve essential documents and record information needed for continuity of operations in accordance with DoDD 3020.26 and Annex F of Federal Emergency Management Agency's Federal Continuity Directive 1.

m. Maintain and dispose of classified records and information in accordance with the applicable OSD RDS.

n. Annually remind and caution all employees:

(1) Not to transfer, destroy, remove, or release records in their custody, including e-mail and e-messages, except as allowed pursuant to:

(a) This issuance.

(b) The OSD RDS.

(c) The Privacy Act of 1974, as amended.

(d) OMB Circular No. A-130.

(e) DoD 5400.11-R.

(f) The Federal Advisory Committee Act.

(g) E.O. 13526.

(h) Section 3106 of Title 44, U.S.C.

(i) Part 1230 of Title 36, CFR.

(j) DoDD 5400.07.

(k) DoDM 5400.07.

(2) To report to the OSD Records Administrator any actual, impending, or threatened unlawful removal, alteration, or destruction of Federal records.

(3) To manage their personal files in accordance with Part 1222.18 of Title 36, CFR, the Privacy Act of 1974, and Section 8 of this issuance.

o. Serve as the approval authority for the release, Component to Component, of non-record copies of OSD records and information for all non-CAPSTONE officials in accordance with Part 1222.24(a)(6) of Title 36, CFR (see Section 10 of this issuance for additional guidance). Ensure the documentation created and received by employees, Service members, and contract personnel departing or transferring from a WHS-serviced Component are preserved in appropriate locations or transferred to appropriate RIM personnel. WHS-serviced Components must use one of the following to report record accountability:

(1) Secretary of Defense (SD) Form 821, "Separating Personnel Records Accountability Checklist –Senior Officials Of OSD, The OSD Components, Defense Agencies and DoD Field Activities."

(2) SD Form 822, "Separating Personnel Records Accountability Checklist – OSD Employees and Contractors."

(3) SD Form 833, "Departing Employee Checklist Transfer of Records Between DoD/OSD Components."

(4) Other WHS-serviced Component approved forms to document that records have been preserved.

SECTION 3: COMPLIANCE WITH RIM MANDATES

3.1. WHS-SERVICED COMPONENT HEADS.

The WHS-serviced Component heads will ensure the implementation of the mandatory regulatory compliance requirements as detailed in this section within their OSD Component, DAFA, or DoD Advisory Committee.

3.2. WHS-SERVICED COMPONENT CIOS AND IT SERVICE PROVIDERS.

Pursuant to Part 1222.24 of Title 36, CFR, and Chapter 35 of Title 44, U.S.C., the WHS-serviced Component CIOs and IT service providers:

a. In coordination with security managers and program managers, provide technical advice, assistance, and access controls to the head of their organization and the OSD RIM Program to support the inclusion of electronic records management functions into the design, development, enhancement, and implementation of FISs in accordance with Parts 1220 through 1239 of Title 36, CFR, and the OSD RDS.

b. Assist in the transfer of permanent electronic records to NARA in accordance with Parts 1220 through 1239 of Title 36, CFR, and the OSD RDS.

c. In accordance with OMB Circular No. A-130:

(1) Coordinate with the OSD SAORM, the OSD Records Administrator, the senior agency officials for privacy, and the appropriate WHS-serviced Component program manager when information systems and components' records, information, and data cannot be appropriately protected or secured.

(2) Ensure that such systems are given a high priority for upgrade, replacement, or retirement.

d. Protect OSD records, information, and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction to provide for their confidentiality, integrity, and availability. Provide information on how shared drives are managed at the back end and accessed on a case-by-case basis. See the OSD Primer for unauthorized disposition reporting procedures.

e. Implement capabilities required to provide integrated network operations to enable information access by any user across network and security domains. Network operations include processes and mechanisms for enterprise management, content management (which includes records management), and network defense pursuant to the DoD Architecture Framework.

f. Serve as the cognizant authority for all Federal-level IT and information management compliance and reporting pertaining to OSD enterprise IT efforts including, but not limited to,

responsibilities outlined in Chapters 31, 33, and 35 of Title 44, U.S.C., and Subtitle III of Title 40, U.S.C. (also known as the "Clinger-Cohen Act of 1996").

g. Implement and enforce applicable policies and procedures, including requirements for archiving information maintained in persistent formats (including within cloud platforms), particularly in the planning, design, and operation of information systems, in accordance with Chapter 35 of Title 44, U.S.C. As part of the capital planning and systems development life-cycle process, ensure DoD employees:

(1) Prepare information system inventories required for records management in accordance with Chapters 21, 29, 31, 33, and 35 of Title 44, U.S.C.

(2) Plan and implement in the system records management controls, in accordance with Chapters 21, 29, 31, 33, and 35 of Title 44, U.S.C., and Part 1236 of Title 36, CFR.

(3) Ensure all records in the system will be retrievable and usable for as long as needed to conduct DoD business and in accordance with the OSD RDS, whereupon they will be destroyed (temporary records) or transferred to NARA (permanent records). Where the records will need to be retained beyond the planned life of an FIS, WHS-serviced Component heads and their CIOs or IT service providers must plan and budget for the migration of records and their associated metadata to new storage media or persistent formats to avoid loss due to media decay or outdated technology.

3.3. WHS-SERVICED COMPONENT ACQUISITION AND PROCUREMENT OFFICERS.

In accordance with Part 1222.32(a)(2) of Title 36, CFR, and Parts 201 to 253 of Title 48, CFR, WHS-serviced Component acquisition and procurement officers will ensure the following records management requirements are included in contracts for services and products. These include, but are not limited to:

a. Records creation, retention, management, and disposition.

b. Privacy and security for protected health information (PHI), electronic protected health information (ePHI), PII, controlled unclassified information (CUI), and other classes of protected records and information.

c. The protection of intellectual property and national security information (NSI).

d. The preservation of records and information relevant to litigation or government proceedings.

e. Ensuring records retention, controls, and clauses are written to contract vehicles and vendors are complying with all applicable records management laws and regulations in accordance with Chapters 29 and 31 of Title 44, U.S.C.; Public Law 113-187; Parts 1220 through 1239 of Title 36, CFR; DoDI 5015.02; E.O. 13526 (for classified records); Volumes 1 through 3 of DoDM 5200.01; DoDI 5200.48; and this issuance.

f. In all contract vehicles, direct that contractor personnel supporting their program offices are to:

(1) Maintain records and information created and received during their day-to-day responsibilities. Ensure that each record set is complete, and that sections or related papers are retained or accounted for in both hard copy and electronic filing systems in accordance with the OSD RDS.

(2) Maintain e-mail, e-messages, and attachments that document work-related activities in accordance with the OSD RDS.

(3) Maintain personal files, non-record material, and contractor work-related records and information separately from U.S. Government records.

(4) Implement the policies and procedures in E.O. 13526, DoDI 5200.48, Volume 3 of DoDM 5200.01, DoDM 5230.30, the OSD RDS, and the OSD Primer.

(5) Comply with the procedures in the OSD Primer and Sections 8 and 10 of this issuance when personnel are requesting to remove personal files.

3.4. WHS-SERVICED COMPONENT RIM PERSONNEL.

In accordance with Parts 1220.34(d) and 1222.24(a)(7) of Title 36, CFR, WHS-serviced Component RIM personnel:

a. Complete the OSD Records Administrator-sponsored records management training within 3 months of their appointment. RIM personnel should also consider attending training at professional RIM organizations and using RIM resources available on NARA's website at https://www.archives.gov.

b. Assist DoD employees with the identification, maintenance, and retention of all OSD records, including those containing NSI, CUI, and PII, in accordance with the OSD Primer.

c. Develop and implement standard operating procedures documenting internal RIM roles and responsibilities specific to the WHS-serviced Component.

d. Brief incoming personnel (including Service members and contractors) concerning their duties and responsibilities when creating and maintaining OSD records and information. RIM personnel are required to document briefings of incoming personnel via memorandum for the record or the OSD Records Management Briefing acknowledgement memo. Briefing slides and memorandum are available on the OSD RIM program SharePoint portal.

e. Brief departing personnel (including Service members and contractors) concerning their responsibility to surrender all agency records to the appropriate personnel, including e-mail and e-messages related to ongoing projects. RIM personnel are required to document briefings of departing personnel via the SD Form 821 or SD Form 822. Briefing slides and memorandum are available on the OSD RIM program SharePoint portal.

f. Ensure each reporting office within their WHS-serviced Component has an office file plan. Annually review and approve the file plan for each office within their Component to ensure that records are accurately identified.

(1) RLs and RCs will prepare and submit file plans to their WHS-serviced Component CRMO or RM for approval. See Section 4 of the OSD Primer for additional guidance.

(2) When direct oversight is geographically or functionally impractical, the CRMO or DAFA RM may delegate approval of file plans to designated directorate or division RMs, RLs, and RCs within program offices.

g. Conduct records searches; implement moratoriums such as litigation holds, preservation notices, or court orders; and ensure component offices are aware of their responsibilities to safeguard records and information identified in existing moratoriums. See Section 7 of this issuance for additional guidance.

h. Assist their WHS-serviced Component with the application of disposition procedures, to include the destruction and retirement of their records.

i. Notify the OSD Records Administrator of any unauthorized destruction, damage, alienation, or removal of official records. See Section 5 of the OSD Primer for unauthorized disposition reporting procedures.

j. Ensure reporting components and offices are maintaining all records related to North Atlantic Treaty Organization (NATO) COSMIC and ATOMAL marked records on loan from their control points.

k. Receive and process requests to remove non-record copies submitted for approval by employees, Service members, or CAPSTONE officials.

(1) Coordinate these requests with office of primary responsibility and component security managers.

(2) Notify the OSD Records Administrator when CAPSTONE officials request to remove non-record copies of DoD records and information.

(3) Ensure DoD employee requests to remove non-record copies of records and information are documented using SD Form 821 or SD Form 822, as appropriate.

(4) Assist DoD employees with interagency requests to transfer e-mail or e-messaging accounts or other DoD records and information, ensuring they are documented and approved using SD Form 833.

l. Ensure the proper maintenance of records and non-record information generated by their program offices by reminding DoD employees, Service members, and contractors of the following:

(1) Do not mix personal and non-records materials with Federal records, including e-mail, e-messages, and DoD official SNS accounts.

(2) Dispose of records and information in accordance with the OSD RDS.

(3) Avoid the use of personal e-mail or e-messaging accounts, unauthorized internet applications, or SNSs to conduct official agency business, except when authorized by DoD 5500.07-R.

(4) Be responsible for the custody, maintenance, retirement, and disposition of current records and FIS created and maintained under office cognizance.

(5) Manage visual information pursuant to DoDI 5040.07 and the OSD RDS.

m. Coordinate with WHS-serviced Component training coordinators to ensure all employees and onsite contractors complete the OSD Annual Basic Records Management Training to maintain compliance with DoDI 5015.02 and this issuance.

n. Conduct internal evaluations of their reporting office(s) records management programs at least every 2 years or upon major reorganization to ensure compliance with this issuance.

(1) RIM personnel can use SD Form 823, "Division/Branch/Office Standardized Recordkeeping Checklist," or WHS Form 17, "OSD Records and Information Management (RIM) Pre-Evaluation," to assist.

(2) Evaluations must be documented in writing and include findings and recommendations. Documentation of RIM evaluations will be maintained by the WHS-serviced Component's RIM personnel.

o. Coordinate with program managers and officers on the development of records schedules for FIS. See Section 5 of the OSD Primer for procedural guidance on the development of records schedules.

p. Coordinate with component privacy officers on the identification of applicable file numbers for system of records notices (SORNs), privacy impact assessments (PIAs), or on the development of records schedules for submission to the OSD Records Administrator.

q. Ensure RIM procedures for the maintenance of component records are included in the development of standard operating procedures, internal issuances, and instructions that document business processes or procedures. At a minimum, these instructions will identify:

(1) Offices and program(s) for which the component is responsible.

(2) Whether office and/or program(s) files are maintained in a central or decentralized records file scheme.

(3) Records maintained to provide evidence of conformity, implementation of programmatic responsibilities, operations, oversight, and execution of policy, regulations, and

other business activities. For example, "supervisors' personnel files" include but are not limited to:

(a) Positions.

(b) Authorizations.

(c) Pending actions.

(d) Position descriptions.

(e) Training records.

(f) Individual development plans.

(g) Telework agreements.

(h) Award recommendations.

(i) Records on individual employees not duplicated in or not appropriate for the official personnel file.

(4) Responsibilities of DoD employees and contractors for maintaining complete, legible records and information that document work activities. For example, a contracting officer file may include but is not limited to:

(a) Metrics.

(b) Memorandums.

(c) Meeting minutes.

(d) Corrective and preventive actions.

(e) Complaints and feedback.

(f) Modifications.

(g) Audit and assessment results.

(h) Document change requests.

(i) Standard operating procedures.

(j) Training records.

(k) Purchasing records related to government-funded equipment.

(5) Formats and location of records.

(a) How and where the records are maintained.

(b) Whether the records in hard copy or electronic format. If electronic, identify location such as network share drives or FISs. This includes FISs maintained at contractor sites or facilities.

(6) Identification of applicable records disposition authorities for all records described within standard operating procedures, internal issuances, and instructions, regardless of format or classification.

r. Have documented procedures, approved by WHS-serviced Component head or delegated authority, to enable the migration of records and associated metadata to new storage media or persistent formats so that records are retrievable and usable if needed to conduct agency business and to meet NARA-approved dispositions.

s. Ensure OSD CAPSTONE officials are managing their records in accordance with NARA disposition authority N1-330-11-010 (File Number 212-01). See Section 4 of the OSD Primer for additional guidance.

(1) CAPSTONE officials' titles may vary across WHS-serviced Components and include, but are not limited to, the Secretary of Defense, Deputy Secretary of Defense, Principal Staff Assistants, Assistant Secretaries of Defense, and OSD RIM Program-serviced DAFA directors. See Section 4 of the OSD Primer for information about records of CAPSTONE officials.

(2) All RIM personnel will review and update their WHS-serviced Component CAPSTONE list upon arrival of new official(s) or annually, whichever is sooner, using the OSD RIM SharePoint site.

3.5. WHS-SERVICED COMPONENT PERSONNEL.

a. In accordance with Parts 1220.34(d) and 1222.24(a)(7) of Title 36, CFR, DoD employees and contractors of WHS-serviced Components will:

(1) Maintain records and information created and received during their day-to-day responsibilities. Ensure that each record set is complete and that enclosures, attachments, working files, documents, and related information (including audio and video records) are retained or accounted for in either a hard copy or electronic filing systems in accordance with this issuance and the OSD RDS.

(2) Preserve e-mail, e-messages, and attachments documenting work-related activities in accordance with the OSD RDS.

(3) Maintain files and filing materials, regardless of format, regularly and carefully in a manner that allows them to be safely stored and efficiently retrieved when necessary.

(4) Ensure personal files and non-record material are maintained separately from work-related records and information.

(5) Implement records management instructions issued by the OSD Records Administrator and WHS-serviced Component CRMOs and RMs, including guidelines on records creation and procedures for capturing records and information.

(6) Follow the procedures in Section 9 of this issuance for the processing of non-record material.

(7) Document the substance of meetings and conversations where decisions are made, issues are resolved, or policy is established.

(8) Complete records management training within 60 days of employment and must complete annual refresher training pursuant to Section 1220.34 of Title 36, CFR, and NARA Bulletin 2017-01.

(9) Avoid the use of personal e-mail, personal e-messaging, and non-official accounts (including SNS) to conduct official agency business, except when authorized by DoD 5500.07- R.

b. Pursuant to Section 2911 of Title 44, U.S.C., OSD employees, contractors, and Service members will not create or send work-related records and information using a non-official e-messaging or social media accounts unless such officer or employee:

(1) Copies their official e-messaging account in the original creation or transmission of the record.

(2) Forwards a complete copy of the record to an official e-messaging account of the officer or employee no later than 20 days after the original creation or transmission of the record.

(a) Individuals must forward or copy complete messages to their official e-messaging accounts.

(b) Coordinate with their IT service providers to ensure all records created on mobile devices are transferred to appropriate locations for storage or preservation. For archival purposes, actions such as screenshots, screen capture, and image capture do not provide an adequate documentation to the complete message.

(3) Exceptions to Section 2911 of Title 44, U.S.C, must be approved by the WHS-serviced Component head and meet all these conditions in accordance with DoDI 8170.01:

(a) Emergencies and other critical mission needs.

(b) When official communication capabilities are unavailable, impractical, or unreliable.

(c) It is in the interest of DoD or other U.S. Government missions.

SECTION 4: MANAGEMENT OF OSD RECORDS AND INFORMATION POLICY

4.1. OSD AND DOD POLICY.

In accordance with the DoD Data Strategy, it is OSD and DoD policy that the records and information created and received by OSD employees, contractors, and Service members are vital to mission success. Managing information as a resource is as important as managing any other vital resource.

a. Federal law, legislation, and DoD and OSD issuances require organizations to maintain many different types of records. For example, an OSD Component or WHS-serviced Component responsible for testing a weapons system can have volumes of records, including personnel training folders, official office correspondence, policy letters, awards, messages, reports, forms, publications, plans, budgets, orders, and contractual correspondence.

b. Every official action taken in OSD results in the creation of some type of record. Whether received using e-mail or e-message, analyzed and summarized in a report, or aggregated in an information system, the record created or received has a value. WHS-serviced Component employees and contractors have a duty to:

(1) Capture what is needed to explain transactions, processes, functions, business elements, etc., from start to finish.

(2) Capture information that provides evidence for accountability as to how the WHS-serviced Component operated.

(3) Ensure the integrity of records and information created and received by assuring the data:

(a) Has not been changed subsequently.

(b) Remains accurate and free from error or defect.

(c) Is consistent and uniform over its lifecycle.

(4) Certify authenticity of OSD records and information, ensuring they are an accurate account of an activity, transaction, or decision.

4.2. OSD RECORDS.

The maintenance of OSD records and information depends on establishing continuous and systematic control over the creation, maintenance, use, and disposition of agency records and information, in accordance with Chapters 31 and 33 of Title 44, U.S.C., and Subchapter B of Chapter XII of Title 36, CFR.

a. The establishment and maintenance of proper filing, guide cards, and filing materials help keep the files orderly and effectively manage information. This aids in retrieving the files, charging them out, and transferring or destroying inactive files in accordance with approved disposition schedules, regardless of media and format.

b. Procedural guidance on the maintenance of OSD records and information is captured in Sections 4, 5, and 6 of the OSD Primer.

4.3. FILE PLANS.

Subpart B of Part 1222 of Title 36, CFR, requires all Federal agencies to provide for adequate documentation of agency business. To meet this requirement, all program offices, divisions, and directorates for the WHS-serviced Components will establish and maintain a file plan that:

a. Will be reviewed and approved by their CRMO, DAFA RM, or DoD Advisory Committee RM annually to ensure compliance, consistency, and accuracy.

b. Meets the minimum requirements outlined in Paragraph 4.6. of the OSD Primer.

c. Identifies all records and information created and received by the WHS-serviced Components' program offices, divisions, and directorates.

4.4. ELECTRONIC RECORDS, INCLUDING MOBILE DATA.

a. DoD employees are responsible for complying with Part 1236 of Title 36, CFR, DoDI 5015.02, DoDM 8180.01, and this issuance regarding the management of records created or received in electronic formats, FIS or via social media, electronic messaging applications, including text messages, e-messaging accounts, messaging services provided on mobile devices, third-party applications, encrypted communications, messaging applications, and direct messages on social media platforms.

(1) Regardless of whether a mobile device is provided by a DoD IT service provider or privately owned, text messages and other information created on that device are considered records when relating to the conduct of government business. Accordingly, these messages and information must be preserved in accordance with Federal law and DoD policy.

(2) To the fullest extent possible DoD employees should not store records on mobile devices. WHS-serviced Component civilians and Service members will coordinate with their IT service providers to ensure all records created on mobile devices are transferred to appropriate locations for storage or preservation no later than 20 days after the creation or transmission of the record.

(3) IT service providers for the WHS-serviced Components will establish a mechanism with the capability to process and transfer records created via email, text, and social media to appropriate locations for preservation, retention, and disposition.

(4) Records created via a text message or an e-messaging account of a CAPSTONE official will be retained in accordance with the current version of the OSD CAPSTONE disposition schedule and Part 1236 of Title 36, CFR. Accounts of Non-CAPSTONE officials will be retained pursuant to GRS 5.2. Item 010. Such records are normally required for only a short time (generally less than 180 days) and are not required to meet legal or fiscal obligations or to initiate, sustain, evaluate, or provide evidence of decision-making.

b. See the OSD Primer and Section 11 of this issuance for additional guidance on maintenance and retention of electronic records.

SECTION 5: RIM POLICY FOR DOD ADVISORY COMMITTEES

5.1. PURPOSE.

a. Generally, advisory committees are a collection of individuals from DoD Components, non-DoD Federal agencies, or public, private, or commercial entities who bring unique knowledge and skills that augment the knowledge and skills of a DoD Component or program office, make recommendations, or provide key information and materials. DoD Advisory Committees do not perform inherently governmental functions such as deciding DoD policy or implementing DoD policy.

b. DoD Advisory Committees may:

(1) Evaluate the performance of and review, monitor, and assess a specific program(s).

(2) Serve as an advocate for an identified subject, function, the sponsoring DoD activity, DoD Component, Congress, or the President of the United States.

(3) Gather input from or serve as a liaison with relevant constituencies.

(4) Provide feedback from the public to the sponsoring DoD Component or program office.

(5) Provide technical expertise and act as an independent and unbiased sounding board to the sponsoring DoD Component or program office.

(6) Assist the sponsoring DoD Component or program office staff to determine important activities.

(7) Provide independent advice and recommendations to DoD leadership.

c. DoD Advisory Committees include but are not limited to:

(1) DoD- or OSD-wide Federal advisory committees, whether statutory or discretionary, established pursuant to the Federal Advisory Committee Act.

(2) OSD Component or OSD RIM Program-serviced DAFA committees, special study groups, task forces, boards, commissions, councils, and similar groups established to provide advice, ideas, options, and opinions to the Federal Government, established pursuant to their general Title 10, U.S.C., authorities or as directed by Congress or Federal law and not subject to the Federal Advisory Committee Act.

(3) Internal, multi-functional, and cross-component advisory committees established under the authority of the Secretary of Defense, Deputy Secretary of Defense, OSD Principal Staff Assistants, or the Assistant Secretaries of Defense.

(4) Interagency advisory committees established by the President of the United States, Congress, or the Secretary of Defense.

(5) A DoD Component whose head is designated as the DoD Executive Agent for a DoD Advisory Committee pursuant to DoDD 5101.01.

5.2. DOD ADVISORY COMMITTEES.

DoD Advisory Committees may be tasked with addressing specific issues related to DoD capabilities or multitude of subjects.

a. DoD Advisory Committees create and collect records and information from across the DoD and OSD, other Federal agencies, or non-governmental organizations such as think tanks or colleges and universities. This collection of information is used to review, analyze, and provide advice and recommendations on DoD or OSD policy or procedures on a variety of subjects, including but not limited to reorganization, base realignments, or recommending new actions. The records and information gathered by these advisory committees represent unique collections that are not available elsewhere within the DoD or OSD.

b. The DoD Advisory Committee heads will assign an RM to coordinate with the OSD Records Administrator and maintain all committee records, regardless of format, in accordance with this issuance and the OSD Primer, as applicable. See Section 3 of this issuance for RIM personnel responsibilities.

c. Employees and contractors will manage and archive records of these advisory committees in accordance with this issuance, the OSD Primer, GRS 6.2, or NARA-approved disposition schedule via the OSD Records Administrator no later than 120 days before termination. These records include but are not limited to:

(1) Memorandums, organizational charts, and directives establishing, changing, continuing, or dissolving the committee.

(2) Agenda, meeting minutes, briefing books, appointment letters, rosters, and membership balance plans.

(3) Copies of interim, final reports, studies, pamphlets, posters, and other publications produced by the advisory committee.

(4) Substantive drafts of the final report and research materials.

(5) Questionnaires, surveys, and other raw data accumulated in connection with the study or work of the advisory committee.

(6) Documentation of subcommittees, working groups, or other subgroups that support the reports and recommendations of the full or parent advisory committee.

(7) Other related records documenting the accomplishments of the advisory committee.

d. DoD Advisory Committees operational for more than 1 year will be subject to RIM evaluations. See the OSD Primer and Section 12 of this issuance for procedural guidance.

5.3. MANAGING DOD ADVISORY COMMITTEE RECORDS AND INFORMATION.

See Section 10 of the OSD Primer for procedures regarding the management of DoD Advisory Committees records and the roles and responsibilities of committee heads and members.

SECTION 6: DISPOSITION OF RECORDS AND INFORMATION POLICY

6.1. GENERAL.

a. Section 3303 of Title 44, U.S.C., requires all Federal agencies to submit disposition schedules to address the retention and disposal of records and information created and received. Disposition schedules also describe the subject matter and value of the records and once approved by the Archivist of the United States, are published in the OSD RDS available at https://www.esd.whs.mil/RIM.

b. Pursuant to Section 3303a of Title 44, U.S.C., all approved disposition schedules are mandatory, regardless of form, format, function, classification, or location. The WHS-serviced Components will execute the disposition schedules and ensure the records and information are properly disposed of in accordance with approved disposition schedules. For example:

(1) Records monitoring expenditures under approved budget allocations are retained for 3 years after execution of the funds. The mandatory retention is 3 years, regardless of whether these records are retained in hard copy or persistent electronic formats or on Secret Internet Protocol Router Network (SIPRNET) or Joint Worldwide Intelligence Communications System (JWICS) networks.

(2) RIM personnel will, with their program offices, coordinate the review of WHS-serviced Component-specific disposition schedules annually. The purpose of this review is to identify new program records and information systems to be scheduled and to identify changes in recordkeeping practices that require records schedule revision. Disposition schedules that are 10 years or older must be certified current or updated. Section 5 of the OSD Primer establishes procedures for modifying existing schedules.

c. OSD records, information, and FISs without an approved disposition schedule are considered unscheduled records. OSD records and information cannot be destroyed without an approved disposition schedule. Section 5 of the OSD Primer establishes procedures for submitting new disposition schedules.

6.2. PURPOSE OF DISPOSITION SCHEDULES.

Disposition schedules identify the content and provide instructions on the lifecycle, retention, and disposition of records and information and are intended to ensure:

a. OSD records are retained in a manner consist with their legal, fiscal, and administrative operational value to the office of primary responsibility.

b. The records are being properly managed and maintained in both electronic and physical formats.

c. Records and information of historical value are preserved and archived.

d. Redundant, trivial, and obsolete records are disposed of in a timely manner.

e. RIM controls are incorporated in the design, funding, and operation of OSD internal and enterprise FISs or the content is integrated into a recordkeeping system that is external to the FIS pursuant to Part 1236 of Title 36, CFR.

6.3. REQUESTS TO DEVIATE FROM OR MODIFY DISPOSITION SCHEDULES.

The WHS-serviced Components are not authorized to deviate from authorized disposition schedules without permission of the OSD Records Administrator. Requests to deviate or modify disposition schedule(s) are submitted to the OSD RIM Program for approval by the OSD Records Administrator. Depending on the extent of the requested deviation(s) or modification(s), the OSD Records Administrator may submit the request to NARA for approval. See Section 5 of the OSD Primer for guidance on modifying RDS.

SECTION 7: RECORD DISPOSITION AUTHORITY MORATORIUMS

7.1. GENERAL.

a. Protecting OSD records and information does not stop at implementing appropriate controls within your components, directorates, and reporting offices. WHS-serviced Components, OSD employees, contractors, and Service members also have the responsibilities to preserve, search, and produce records and information when directed by general counsel (GC), attorneys, or RIM personnel. When directed, WHS-serviced Components must take steps to preserve potentially relevant evidence in any form when a party reasonably anticipates litigation of a matter or as directed. The consequences of a failure to preserve may vary depending on the circumstances, but may include:

(1) Regulatory fines and penalties.

(2) Civil litigation consequences, such as increased litigation costs, fines, adverse inference instructions, default judgment, and civil contempt.

(3) Vicarious liability for responsible senior management.

(4) Criminal liability for organizations and individuals.

(5) Termination.

b. Record disposition authority moratoriums, defined in the Glossary and referred to as "moratoriums" in this issuance, ensure that records relating to the litigation are not destroyed and are available for the discovery process before and during litigation. Agency GC or attorneys are generally responsible for issuing litigation holds to:

(1) Individual WHS-serviced Component(s).

(2) OSD- or DoD-wide.

(3) Military Departments or other DoD agencies.

(4) Individual Federal employees.

c. Moratoriums may also be issued via the OSD Records Administrator, OSD Component attorneys, DAFA GC, Congress, or the Office of the President.

d. The moratoriums can generally be separated into four types:

(1) Search and Production Request.

(a) A search and production request notifies the WHS-serviced Component(s) concerned to identify and locate records or subject matter pertinent to the moratorium.

(b) When notified, the WHS-serviced Component(s) concerned are required to search for information related to the litigation hold regardless of format and location.

(c) The WHS-serviced Component(s) are to ensure that records relevant to the search remain unaltered and unadulterated.

(d) These moratoriums will provide details on search criteria, subject matter, formats, and instructions for producing relevant information to a point of contact.

(2) Search and Hold Request.

(a) Search and hold requests can involve the examination of all types of hard copy and electronic records and information, including DoD employee e-mail and e-messaging accounts.

(b) Examples of electronic records and information include text, images, calendar files, databases, spreadsheets, audio files, animation, websites, e-mails, e-messages, voice mails, chat, chat transcripts, and computer programs.

(c) The WHS-serviced Component(s) are to ensure that records relevant to the search remain unaltered and unadulterated.

(d) These moratoriums will provide details on search criteria, subject matter, and formats and will ask the recipients to hold the information in their possession, custody, or control until further notice.

(3) Pending Litigation.

(a) The WHS-serviced Component(s) or individual employees or Service members of a WHS-serviced Component(s) can be the subject of litigation. Whether an individual, group of employees, or WHS-serviced Component, the parties identified pursuant to litigation may receive documentation notifying them of a pending lawsuit and actions required to be taken from the Department of Justice, GC DoD, OSD Component attorneys, or OSD RIM Program-serviced DAFA GC.

(b) When notified, the individual, group of employees, or the WHS-serviced Component may be required to search for, preserve, or produce information related to the litigation regardless of format and location.

(c) The WHS-serviced Components have an obligation to identify and preserve relevant electronic information and hard copy documents when a reasonable anticipation of litigation arises or when they receive a litigation hold or preservation notice.

(4) Government Accountability Office or Inspector General Audits.

The Government Accountability Office and Office of Inspector General of the Department of Defense may require access to records and documents related to the WHS-serviced Component programs or functions as needed to conduct the audit or inspection. Upon

notification, the WHS-serviced Component will suspend disposition of records and information to complete the audit or inspection.

e. Notifications may be sent using official correspondence, either by e-mail, e-message, or official tasking system.

7.2. PROCESSING MORATORIUMS.

a. The Office of the GC DoD will:

(1) Notify the OSD Records Administrator of litigation holds relevant to the WHS-serviced Components by sending a copy of the litigation hold to the OSD Records Administrator organizational e-mail address.

(2) Identify a lead attorney to coordinate with the OSD Records Administrator.

(3) Request any WHS-serviced Components subject to a litigation hold identify a point of contact to act as central point of contact for preservation issues and responses for their respective Component.

(4) Notify the OSD Records Administrator when a litigation hold(s) is lifted or terminated.

b. GC and attorneys assigned to the WHS-serviced Component will review records and information for privilege before release outside of DoD. The review must ensure records that may be classified, privileged, or otherwise protected from disclosure are treated appropriately.

c. The OSD Records Administrator will:

(1) Review litigation holds to determine affected WHS-serviced Component(s) and the scope or date span of the request. If necessary, issue additional guidance on the preservation or processing of records or materials implicated in the hold.

(2) As necessary:

(a) Coordinate with the WHS-serviced Component CIOs or IT service providers to identify content and locations for electronic searches on the network, enterprise e-mail, e-messaging accounts, or other IT systems as appropriate.

(b) Conduct a search of records of the affected WHS-serviced Component(s) held within FRCs.

(c) Provide oversight, training, and guidance to WHS-serviced Component CRMOs and RMs on implementing litigation holds, including issuing periodic reminders.

(d) Notify the RIM personnel, NARA, and other affected WHS-serviced Components when a litigation hold has lifted or terminated.

d. WHS-serviced Component CIOs or IT service providers will:

(1) Coordinate with the assigned lead attorney to determine scope and search terms requested in the litigation hold.

(2) Coordinate with their GC, attorney, or the assigned lead attorney for the legal sufficiency review of search requests, including but not limited to:

(a) Ensuring notices are distributed and an appropriate level of detail provided to identify potentially relevant information.

(b) Determining whether a separate litigation notice should be sent to information system owners who may be maintaining information systems that house data that the records management personnel do not control or to which they do not have access.

(c) Ensuring the preservation of records and documents (including e-mails, e-messages, social media, and those in electronic formats) that may be relevant to the litigation or potential litigation.

(3) Conduct searches of shared network drives, cloud service providers and FISs owned by the affected WHS-serviced Component residing on the OSD.mil domains (including Non-classified Internet Protocol Router Network (NIPRNET), SIPRNET, and JWICS as appropriate), enterprise mail, mobile devices, or affected individual employee accounts.

(4) Ensure that records and information responsive to the litigation hold are maintained in native formats until notified of production or cancellation of the litigation hold.

(5) Ensure that potential electronically stored information sources are properly addressed, including online and offline devices, software, cloud-based electronically stored information, and applications.

e. As the records and information owners, the WHS-serviced Components are responsible for the accuracy, completeness, and timeliness of responses to the litigation hold, including the location, preservation, review, and production tasking in response to litigation hold memorandum direction. As such, each WHS-serviced Component will:

(1) Identify reporting offices and key custodians (e.g., former retired civilian, military, or U.S. Government contractor personnel) who may possess potentially relevant electronically stored information or documents other tangible things related to the litigation.

(2) Ensure that processes are in place to effectively search for, locate, preserve, review, and produce records and information. These plans must account for records and information not located on the OSD.mil domain including, but not limited to:

(a) Information systems.

(b) E-mail or e-messages with attachments.

(c) All other types of electronic files (e.g., text messages or files generated on a mobile device).

(d) All holdings of hard copy materials not directly supported by the WHS-serviced Component CIO or IT service providers.

(3) Designate personnel to act as a hub for coordination with GC and the OSD Records Administrator to execute litigation hold requirements.

(4) Comply with Paragraphs 7.2.f. and 7.2.g. if a litigation hold is received directly by the WHS-serviced Component.

(5) Notify affected subordinate components, program offices, and personnel of litigation holds.

(6) Be responsible for notifying subordinate component activities that a litigation hold exists or has been lifted.

f. Designated WHS-serviced Component points of contact will:

(1) Acknowledge receipt of litigation hold memorandum to the assigned lead attorney.

(2) Suspend the retention period(s) of all affected relevant records and information and retain them until notified that the litigation or disputes are resolved.

(3) Provide the assigned lead attorney with the names of the offices and individuals who coordinated conducted the search and an inventory list of records and information affected responsive to the categories listed in by the litigation hold or preservation notice. The inventory list will contain the number of records identified and an estimate of the number of documents or volume of data.

(4) Provide the requestor assigned lead attorney with copies of the records and information in question, as appropriate and authorized for release.

g. A moratorium can be addressed to an employee. When coordinating with the WHS-serviced Components, this employee should be considered a key custodian.

(1) When notified, WHS-serviced Component employees, including Service members or contractors, will:

(a) Suspend routine destruction of records as identified in the litigation hold or preservation notice.

(b) Discontinue WHS-serviced Component reporting office practices for destruction of records.

(c) Preserve records in their original electronic or hard copy formats.

(d) Preserve new responsive records generated or received after notification of moratorium.

(e) Follow instructions specified by the moratorium.

(f) Consult with the designated contact point of contact person with questions.

(g) Inform their WHS-serviced Component CRMO or RM, as appropriate, including any received moratoriums and actions taken in response.

(2) All departing employees in receipt of a moratorium(s) are under an obligation to inform their assigned RIM personnel and their supervisor about impending departure to provide time to arrange for preservation of potential evidence.

7.3. RESPONSIVE RECORDS.

When an individual, the WHS-serviced Component, or their reporting office has responsive records, they must execute the instructions provided in the records litigation hold or freeze preservation notification. If instructions are not provided, the affected parties will coordinate with RIM personnel to:

a. Create a "Records Moratorium" folder on the shared drive and name the folder with the subject of the moratorium. Identify appropriate personnel with "need to know" and coordinate with their IT service provider to restrict or limit access to these folders.

b. Search records storage locations, including but not limited to file cabinets, safes, cloud computing solutions, network shared drives, personal drives, FISs, mobile devices, and applicable e-mail or e-messaging accounts for documents responsive to the moratorium.

c. If the responsive records are in hard copy, the affected parties must scan records in accordance with current NARA standards and retain images in designated folders on the shared drive to ensure they are appropriately preserved. RIM personnel will ensure retention of the paper versions until the litigation hold or preservation notice is rescinded.

d. To the extent practicable, or as directed by the assigned attorney, convert responsive e-mail, e-messages, and electronic records to a portable document format (PDF) and copy them to the designated folders on the shared drive to ensure they are appropriately preserved. Instructions for converting e-mail and e-messages to PDF or other sustainable formats are available on the OSD RIM website.

e. Place appropriate access restrictions to prevent the deletion or alteration of records.

f. The WHS-serviced Component will provide the name of offices, locations, and personnel who conducted the search and identify whether any responsive records or non-responsive records were found, in a memorandum for the record, in accordance with the Federal Rules of Civil Procedure.

SECTION 8: PROTECTION OF OSD RECORDS AND INFORMATION

8.1. GENERAL.

Classification formalizes the process of defining what information is classified, defining, and implementing different levels of protection based on the expected damage to national security the information would cause if compromised.

a. In accordance with E.O. 13526, classification may be applied only to records and information owned by, produced by or for, or under the control of the U.S. Government, to include products created by government contractors.

b. Information may be considered for classification only if its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security and it concerns one of the categories specified in Section 1.4 of E.O. 13526.

8.2. PROTECTION OF NSI AND CUI.

a. All WHS-serviced Components must ensure NSI and CUI are protected in accordance with DoDI 5200.01, DoDI 5200.48, and Volumes 1 through 3 of DoDM 5200.01.

b. For NATO security documents, the DoD plays a vital role within NATO and member organizations on intergovernmental military alliance issues.

(1) DoDD 5100.55 outlines the WHS-serviced Components' responsibilities for formulating policy and issuing guidance, criteria, instructions, and procedures required for ensuring compliance with and implementation of NATO security policy.

(2) United States Security Authority for NATO Affairs Instruction 1-07 identifies procedures for protection and disposition of NATO classified and unclassified records and information created and maintained by the WHS-serviced Components.

8.3. DECLASSIFICATION OF OSD RECORDS AND INFORMATION.

a. Pursuant to DoDI 5200.01, declassification of information will receive the same level of attention as the classification of information so that information remains classified only if required by national security considerations.

b. Only classified records and information identified as permanent pursuant to the OSD RDS are eligible for declassification review in accordance with Section 3.3 of E.O. 13526, Volume 3 of DoDM 5200.01, and DoDM 5230.30.

c. Before being transferred to NARA, all classified NSI will receive a Kyl-Lott review, pursuant to Public Law 105-261. Only personnel certified pursuant to Chapter 23 of Title 42,

U.S.C., also known and referred to in this issuance as the "Atomic Energy Act of 1954, as amended," are authorized to conduct Kyl-Lott reviews.

d. If an original classification authority (OCA) identifies a series of OSD records and information that requires an encompassing exemption from declassification, the OCA may submit for a "File Series Exemption" in accordance with Section 3.3 of E.O. 13526. The OCA will provide:

(1) A detailed description of the information (including applicable OSD RDS file numbers), either by reference to information in specific records or in the form of a classification guide, to the OSD Records Administrator for review and concurrence.

(2) An explanation of why the information should be exempt from automatic declassification, public release and must remain classified for a longer period.

(3) A specific date or a specific and independently verifiable event when the exempted file series can be reviewed for declassification.

e. Requests for file series exemption will be submitted in writing to the Office of the Under Secretary of Defense for Intelligence and Security and the OSD Records Administrator for concurrence.

(1) Upon concurrence, the Office of the Under Secretary of Defense for Intelligence and Security will coordinate submission to the Secretary of Defense for signature and submission to the Interagency Security Classification Appeals Panel requesting the file series exemption, in accordance with Volume 1 of DoDM 5200.01.

(2) Series are not considered exempt from declassification until approved by the Interagency Security Classification Appeals Panel.

f. NSI and CUI records and information identified as temporary records pursuant to the OSD RDS will be destroyed in accordance with their applicable file number.

8.4. DE-CONTROL OF CUI.

Neither the OSD RIM Program nor the OSD Declassification Program is authorized to de-control CUI. In accordance with DoDI 5200.48, the office of primary responsibility or the controlling DoD office will include dissemination statements on OSD records and information to facilitate control, secondary sharing, de-control, and release.

8.5. PROTECTION OF PII AND PHI.

The WHS-serviced Components will ensure FISs, applications, databases, cloud computing solutions, and emerging technologies authorized for deployment on the DoD information network (DODIN) that contain, manage, and retain PII, PHI, and ePHI are compliant, as applicable, with:

a. The Privacy Act of 1974.

b. DoDIs 5400.11, 6025.18, and 8580.1.

c. DoD 5400.11-R.

d. Volume 2 of DoDM 5400.11.

e. DoDM 6025.18.

f. Applicable editions of National Institute of Standards and Technology publications for relating to privacy and PII records.

8.6. PRIVACY IMPACT ASSESSMENTS

a. A PIA is designed to accomplish three goals:

(1) Ensure conformance with applicable legal, regulatory, and policy requirements for privacy.

(2) Determine the risks and effects.

(3) Evaluate protections and alternative processes to mitigate potential privacy risks.

b. PIAs will be prepared using Department of Defense (DD) Form 2930, "Privacy Impact Assessment (PIA)," and in accordance with DoDI 5400.16.

c. WHS-serviced Component CRMOs and RMs will ensure the RDS cited by the program manager or designee are correct and updated as appropriate.

(1) If a records disposition authority does not exist or needs to be updated, the WHS-serviced Component CRMO or RM will submit a Standard Form (SF)-115, "Request for Records Disposition Authority" to the OSD Records Administrator. See Section 5 of the OSD Primer for guidance on developing and submitting an SF-115.

(2) Upon verification or submission of an SF-115, the WHS-serviced Component CRMO or RM is authorized to sign the PIA.

(3) Records disposition information on the PIA and SORN, including the applicable retention period, should be consistent with the records disposition authority cited on the PIA and must match the applicable SORN.

8.7. SORN.

a. In accordance with DoDI 5400.11 and the procedures in DoD 5400.11-R, each WHS-serviced Component maintaining records and information about individuals will ensure that this data is protected from unauthorized collection, use, dissemination, or disclosure of PII. Records

containing PII records will be maintained pursuant to DoDI 5400.11 and the Privacy Act of 1974.

b. A SORN is required when all the following apply:

(1) The records are maintained by a Federal agency.

(2) The records contain information about an individual.

(3) The records are retrieved by a personal identifier.

c. WHS-serviced Component CRMOs and RMs will assist the program manager or designee with identifying the correct records disposition authority applicable to the group(s) of records identified in the SORN. If a records disposition authority does not exist or needs to be updated to meet mission or operational needs, the WHS-serviced Component CRMOs and RMs will submit an SF-115 to the OSD Records Administrator. Records disposition information on the PIA and SORN, including the applicable retention period, should be consistent.

SECTION 9: TRANSFER OR DECOMMISSIONING OF OSD FUNCTIONS AND PROGRAMS

9.1. TRANSFER OF FUNCTIONS AND PROGRAMS.

a. In accordance with Title 10, U.S.C., the Secretary of Defense is authorized to reassign functions and programs as necessary to meet operational requirements or to implement actions authorized by the President or Congress.

b. Each WHS-serviced Component must ensure records and information necessary for Component operations and records of permanent historical value are identified and documented, regardless of format.

(1) At a minimum, each reporting office within the WHS-serviced Components must:

(a) Identify the office(s), functions, or programs to be transferred.

(b) List the file numbers, subject matter, quantity, media or format, classification, and location of the records they will retain.

(c) Identify any records to be transferred along with the function to another office.

(2) The SD Form 832 may be used to facilitate this process and document records required to be retained.

(3) The SF 135, "Records Transmittal and Receipt," should be used to document hard copy records being transferred to another WHS-serviced Component or closed records no longer required for current business or historical value. The latter may be archived offsite via the OSD Records Administrator.

c. DoD Advisory Committees disestablished by order of the President of the United States, Congress, the Secretary of Defense, Deputy Secretary of Defense, Principal Staff Assistants, or the Assistant Secretaries of Defense will transfer their records to the OSD Records Administrator in accordance with Section 7 of the OSD Primer.

d. The head of the reporting office and the assigned RIM personnel are responsible for maintaining custody of and accountability for OSD records and information until they are transferred to the gaining WHS-serviced Component, FRC, or the OSD Records Administrator. When transferring records and information, RIM personnel must:

(1) Transfer copies of all inventory documentation to the WHS-serviced Component CRMO or RM for the gaining WHS-serviced Component.

(2) Coordinate with security managers before transferring classified records and information.

(3) Notify the gaining WHS-serviced Components of any record freezes, preservation orders, or moratoriums.

(4) Ensure that personal materials (non-work-related) are separated from official records, working papers, and drafts.

(5) Oversee the packaging and transfer of hard copy records to gaining WHS-serviced Components or to the Washington National Records Center.

(6) Coordinate with IT service providers to identify network space(s) for WHS-serviced Component records, including identifying restrictions on access such as those containing PII or national security classifications, to the gaining WHS-serviced Component.

(7) Ensure all permanent records of disestablished WHS-serviced Components or records eligible for retirement are properly prepared and transferred to the OSD Records Administrator via the WHS-serviced Component CRMO or RM.

(8) Dispose of personnel records in accordance with Chapter 7 of the Office of Personnel Management's Guide to Personnel Recordkeeping and the OSD RDS.

(9) Report any actual, impending, or threatened unlawful removal, alteration, or destruction of records and information to the OSD Records Administrator (see Paragraph 5.8 of the OSD Primer for reporting instructions). In the event of unlawful removal or inappropriate destruction of records containing PII, report the violation in accordance with Volume 2 of DoDM 5400.11.

(10) Notify the OSD Records Administrator of all programs, functions, and related records, information systems, and SNS accounts being transferred or disestablished and provide a copy of the SD Form 832, SF-135, or other documentation used to detail those records.

e. In the case of classified records transferred in conjunction with a transfer of functions, and not merely for storage purposes, the receiving WHS-serviced Component(s) will be deemed to be the originating agency pursuant to E.O. 13526.

f. Classified records received by DoD Advisory Committees established pursuant to the Federal Advisory Committee Act will be transferred to the OSD Declassification Program (WHS/RDD) for automatic declassification review in accordance with the procedures identified in Section 7 of the OSD Primer.

9.2. TRANSFER OF RECORDS TO OTHER EXTERNAL ORGANIZATIONS.

a. Transfers of OSD functions and programs, regardless of classification, to non-DoD Components because of a transfer of functions, programs, or similar reasons will be coordinated with the OSD Records Administrator and documented using the SF 135 or SD Form 832, "OSD Records Inventory Form." See Section 7 of the OSD Primer for documenting transfers of records.

b. Distribution of the SF-135 is as follows.

(1) The original is forwarded to the receiving organization.

(2) A copy is provided to the OSD Records Administrator.

9.3. DISESTABLISHMENT OR CLOSURE OF OSD FUNCTIONS AND PROGRAMS.

a. Hardcopy, electronic records, databases, and FISs cannot be destroyed or decommissioned if the records are within their established retention periods. For example, MYPAY maintains the master pay record data for civilian and Service members. The established retention for the master pay records is 99 years. If the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense, decommissioned MYPAY before all the records within it has reached the end of their retention, that office would be responsible for ensuring the records within MYPAY remain accessible, readable, and secure for the remainder of the retention period.

b. The WHS-serviced Component heads are advised to provide guidance in preparing and transferring of hard copy records to program offices with the capability to retain them or to FRCs via the OSD Records Administrator.

(1) Retention of FISs must be coordinated with IT service providers with responsibility delegated to a reporting office for oversight.

(2) The WHS-serviced Component heads must consider records needed for operational and mission, human resources, and legal requirements.

c. RIM personnel should coordinate with their action officer or program manager to inventory shared drives and hard copy records to determine their status, disposition, and classification. Other issues that may need to be addressed are:

(1) Naming conventions.

(2) Version control.

(3) Unprotected folders containing PII.

(4) Access controls.

(5) The destruction of personal, reference, and non-record materials.

d. IT service providers must assist with transferring the disestablished WHS-serviced Components' electronic records and FISs to the gaining office or Component identified locations, and ensure they remain:

(1) Reliable. Records present a full and accurate representation of the transactions, activities, or facts.

(2) Authentic. Records are protected against unauthorized addition, deletion, alteration, use, and concealment.

(3) Complete. Records are complete and unaltered.

(4) Usable. Records can be located, retrieved, presented, and interpreted.

(5) Accurate in content. The information within the record itself is preserved.

(6) Accurate in context. Any related records that show organizational, functional, and operational circumstances about the record are properly cross-referenced.

(7) Accurate in structure. Controls are in place to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

(8) Retained. Records are retained in a usable format until their authorized disposition date.

SECTION 10: REMOVAL OF PERSONAL AND NON-RECORD COPIES OF OSD RECORDS AND INFORMATION

10.1. NON-RECORDS MATERIALS.

a. Non-record materials are U.S. Government-owned materials (regardless of format) excluded from the legal definition of records in accordance with Section 3301 of Title 44, U.S.C. They include but are not limited to:

(1) Extra copies of documents preserved only for convenience of reference.

(2) Stocks of publications and of processed documents. However, each agency needs to create and maintain record sets of processed documents and of publications, including annual and special reports, special studies, brochures, pamphlets, books, handbooks, manuals, posters, and maps.

(3) Library and museum material made or acquired and preserved solely for reference or exhibition purposes.

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

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

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

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

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

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

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

b. Non-record materials may be removed from U.S. Government custody only with the agency's approval.

10.2. PROCESSING REQUESTS TO REMOVE NON-RECORD COPIES OF OSD RECORDS AND INFORMATION FROM GOVERNMENT CUSTODY.

a. In accordance with Chapters 31 and 33 of Title 44, U.S.C., and Parts 1220 through 1239 of Title 36, CFR, records and information created and received by OSD employees in the conduct of government operations are the property of the Federal Government.

b. DoDI 5015.02 requires all WHS-serviced Components to implement measures to maintain accountability of the records and information, including copies, the Components create and receive. This includes but is not limited to:

(1) Copying or removing records from government custody, except as authorized by this issuance, DoDIs 5200.01 and 5200.48, Volumes 1 through 3 of DoDM 5200.01, and the OSD RDS.

(2) Ensuring OSD employees, Service members, and contractors are aware they are not authorized to remove original hard copy records.

(3) Reminding OSD employees, Service members, and contractors that unclassified records and information are not automatically releasable. The classification "Unclassified" is not the same as being cleared for public release.

c. DoD e-mail, e-messages, SNSs, web 2.0 technology, or social media accounts are provided for the conduct of government business and DoD operations and:

(1) Are not considered personal files.

(2) Are not authorized for transfer or removal without review and approval. This includes but is not limited to complete copies of e-mail inboxes, sent e-mails, outboxes, e-messages, e-messaging accounts, or Microsoft Outlook personal storage table (.PST) files.

(3) Users are prohibited from using non-approved third-party e-mail systems, e-messaging applications, storage servers, file-sharing services, SNSs, web 2.0 technology, or social media applications to conduct government business. This includes but is not limited to Google Drive, Yahoo mail, iCloud, Whatsapp, or SnapChat.

(4) OSD employees may request to transfer non-record copies of OSD records and information (including e-mails or e-messages) when transferring to new DoD duty stations or assignments, if it does not:

(a) Diminish the official record or impact the WHS-serviced Component's ability to conduct business.

(b) Contain PII not related to the requestor.

(c) Contain NSI, CUI, or unclassified information that may, individually or combined, lead to the compromise of classified information or disclosure of operations or security.

(d) Contain subject matter pertinent to current and pending litigation or moratoriums.

(e) When reviewing transfer requests, the OSD Components and OSD RIM Program-serviced DAFAs must ensure the requestor has been deemed to have a mission-related purpose or lawful government purpose for the transaction of the gaining office or components' activity, mission, function, or operations.

d. Members and personnel of DoD Advisory Committees are not authorized to remove or transfer records and information created or received by the committee.

e. See Paragraph 10.6. of this issuance for the removal or transfer authorization and approval process.

10.3. REVIEW OF RECORDS REQUESTED.

a. During their tenure in office, many government officials, employees, and Cabinet officials accumulate substantial collections of personal files and non-record copies of official documents (including electronic files, e-messages, and e-mail) created solely for convenience of reference. See Glossary for definition of non-record material.

b. OSD Components and OSD RIM Program-serviced DAFAs must review the requested non-record materials to determine releasability.

(1) OSD Components and OSD RIM Program-serviced DAFAs will conduct a review in accordance with DoDI 5200.48 and Volumes 1 through 3 of DoDM 5200.01 to ensure protected records and information is not released without authorization.

(2) The non-record copies will be reviewed to identify CUI or unclassified information that may, individually or combined, lead to the compromise of classified information or disclosure of operations or security. Non-record copies that cannot be decontrolled pursuant to DoDI 5200.48 or redacted must not be authorized for release or transfer.

(3) Personal files and non-record copies will be reviewed by the office of primary responsibility of the requested materials for foreseeable harm to DoD in compliance with the Department of Justice Office of Information Policy's Foreseeable Harm Standard or superseding guidance.

(4) Additional guidance for transfers or removal of OSD records and information is provided in Section 9 of the OSD Primer.

c. When reviewing transfer requests, the OSD Components and OSD RIM Program-serviced DAFAs must ensure the requestor has been deemed to have a mission-related purpose or lawful government purpose for the transaction of the gaining office or components' activity, mission, function, or operations.

10.4. REMOVAL OF NON-RECORD COPIES BY POLITICAL APPOINTEES.

a. OSD PAs and PAS officials will:

(1) Sign a non-disclosure agreement provided by the OSD Records Administrator for the removal of approved non-record copies.

(2) Agree not to release or publish the information orally or in writing (hard copy or electronically) without written DoD approval.

(3) Complete the SD Form 821 for the removal of non-record material. The SD Form 821 and materials will be submitted to the OSD Records Administrator for review and approval via their WHS-serviced Component CRMO or RM.

b. The OSD SAORM serves as the appellate authority to any denials or redactions that may be contested.

c. See Paragraph 10.6. for approval authorities.

10.5. DONATION OF NON-RECORD COPIES AND PERSONAL FILES.

a. Only Cabinet-level officials may donate unclassified non-record material to a Presidential Library, U.S. National Archives, Library of Congress, or to a private institution (college, library, historical society, etc.) in accordance with Part 1226.26 of Title 36, CFR.

b. Any transfer of non-record copies of official documents to any government or private institution must be affected in writing by a deed of gift or other form of legal conveyance.

(1) The written instrument must clearly explain the terms under which the institution accepts the papers and the protection they will be afforded while in its care, to include mandatory restrictions on access.

(2) These restrictions pertain to any of the following:

(a) Potential violations of personal privacy.

(b) Protection of DoD information of public business, as well as nonpublic and privileged, information exempted from release in the collection.

(c) Materials or information that might prove prejudicial to the conduct of U.S. foreign relations.

(d) Material relating to law enforcement investigations.

(3) Any such conveyance must be reviewed by the GC DoD and the OSD Records Administrator before the donor signs it.

c. It is the responsibility of the donor and their immediate staff to:

(1) Coordinate with the GC DoD and the OSD Records Administrator regarding the donation.

(2) Complete the SD Form 821. The SD Form 821 will be submitted to the OSD Records Administrator via their WHS-serviced Component CRMO or DAFA RM.

(3) Provide to the OSD Records Administrator:

(a) The name and address of the proposed recipient of the records.

(b) A list containing:

1. Identification of the documents or files.

2. The inclusive dates.

3. The volume and media of the materials to be donated.

d. Access to personal files and non-record material donated by an official to an institution for historical preservation will be in accordance with the instrument of gift signed by the official and the institution.

e. Access to Federal records by former officials which they originated, reviewed, signed, or received while serving as PAs can be granted in accordance with Administrative Instruction 50.

10.6. AUTHORIZATION TO TRANSFER OR REMOVE.

a. Transfers or removal requests for records and information between OSD and DoD Components by non-CAPSTONE officials will be approved by an authorizing official from the gaining and losing OSD Components or WHS-serviced Components or the Federal records officer for the DoD Component.

(1) Requests to transfer records will be documented on the SD Form 833.

(2) Requests to remove personal files and non-record materials will be documented on the SD Form 822. Upon approval, Non-CAPSTONE officials will sign a non-disclosure agreement provided by their CRMO or DAFA RM for the removal of approved non-record copies.

b. In accordance with Paragraph 10.1. of this issuance, the procedures contained in Section 9 of the OSD Primer, and the OSD RDS, authorizations for removal or transfers are the sole discretion of the gaining and losing OSD Component heads or OSD RIM Program-serviced DAFAs directors or their authorized delegates.

c. The OSD Records Administrator serves as the approval authority for OSD CAPSTONE officials. The OSD SAORM serves as the appellate authority to any denials or redactions that may be contested concerning the review of unclassified non-record information or materials for the purposes of removal from DoD custody.

d. DoD Advisory Committee members, Service members, employees, and contractors or staff of DoD Advisory Committees are not authorized to transfer or remove the records and information created or received while assigned or employed by the committee.

SECTION 11: ELECTRONIC RECORDS MANAGEMENT

11.1. PRINCIPLES.

a. The WHS-serviced Components will implement appropriate measures and standards to ensure that OSD records and information remain authentic, secure, and confidential, regardless of format, classification, or location.

b. The WHS-serviced Components will ensure all records and information created, received, and stored in FISs, cloud computing platforms, and the DODIN (including all classified networks, e-mail, e-messages, or future technologies) adhere to these principles:

(1) The records and information are:

(a) Reliable. Present a full and accurate representation of the transactions, activities, or facts.

(b) Authentic. Protected against unauthorized addition, deletion, alteration, use, and concealment.

(c) Complete and unaltered.

(d) Usable. Records and information can be located, retrieved, presented, and interpreted.

(e) Accurate in content. Preservation of the information within the record itself.

(f) Accurate in context. Cross-references to related records show the organizational, functional, and operational circumstances about the record.

(g) Accurate in structure. Controls are in place to ensure the maintenance of the physical and logical format of the records and the relationships between the data elements.

(2) The records and information are retained until their authorized disposition date.

(3) FISs, cloud computing platforms, and the DODIN implement appropriate physical and logical methods to protect records and information from accidental or intentional alteration or destruction.

(4) WHS-serviced Component employees:

(a) Maintain and safeguard records and information containing NSI or PII by only accessing and using information that is minimally necessary to perform their job duties.

(b) Are informed of applicable legal mandates and industry standards for protecting information and use the information with consideration and ethical regard for others.

11.2. MAINTENANCE AND RETENTION OF RECORDS AND INFORMATION ON OSD NETWORK SHARE DRIVES.

The WHS-serviced Components may maintain their records on DoD-provided network share drives. Network share drives do not provide the functionality of an electronic recordkeeping system. Through a combination of manual and automated policies and procedures, a network share drive may act as a recordkeeping system. The WHS-serviced Component establishing share drives as a recordkeeping system will:

a. Establish formal procedures that address retention and disposition of records stored on network share drives.

b. Develop a clear and understandable naming convention for records and information. It is highly recommended the WHS-serviced Components use established acronyms and terminology developed in the DoD Dictionary of Military and Associated Terms. Additionally, Appendix B of the OSD Primer provides examples of standardized naming conventions.

c. Develop and implement RIM structure in accordance with Sections 6 and 7 of the OSD Primer.

11.3. E-MAIL AND E-MESSAGE MANAGEMENT.

It is OSD RIM policy, pursuant to Section 2912 of Title 44, U.S.C. and Part 1236.22 of Title 36, CFR and regardless of classification, that the IT service providers for the WHS-serviced Component will implement the approved NARA disposition authority using the current version of the OSD CAPSTONE disposition schedule for e-mail, text and e-messaging accounts established within the DODIN domains. The OSD CAPSTONE disposition schedule provides the approved disposition authority for the retention and disposition of e-mail and e-messaging accounts.

a. The OSD RIM Program is responsible for:

(1) Defining the scope of CAPSTONE positions with OSD Components and OSD RIM Program-serviced DAFAs.

(2) Coordinating updates to the OSD List of CAPSTONE Officials with the OSD Components and OSD RIM Program-serviced DAFAs to submit updates to NARA pursuant to GRS 6.1.

(3) Archiving of OSD records and information in accordance with the current version of the OSD CAPSTONE disposition schedule.

b. E-mail and e-messaging accounts for CAPSTONE equivalents at DoD Advisory Committees (e.g., Advisory Committee management officer, Designated Federal officer, or Advisory Committee organization mailboxes) are archived to NARA pursuant to GRS 6.2.

c. Employees, Service members, and contract personnel at WHS-serviced Components will maintain e-mail, text, and e-message records created and received in accordance with this issuance, the OSD Primer, and the OSD RDS.

d. Records created via a text message or an e-messaging account of a CAPSTONE official will be retained in accordance with the current version of the OSD CAPSTONE disposition schedule and Part 1236 of Title 36, CFR. Accounts of Non-CAPSTONE officials will be retained pursuant to GRS 5.2. Item 010 except as noted in Paragraph 4.4. of this issuance.

e. IT service providers for the WHS-serviced Components will establish a mechanism to retain and disposition e-mail, text messages, and e-messaging accounts of CAPSTONE officials pursuant to Part 1236 of Title 36, CFR, and the current version of the OSD CAPSTONE disposition schedule.

(1) This mechanism will include records management functionality and archival requirements pursuant to Part 1236 of Title 36, CFR, OMB Circular A-130, and DoDI 5015.02.

(2) WHS-serviced Components' IT service providers will also ensure OSD personnel are not using personal e-mail, e-messaging accounts, unauthorized internet applications, or social media to conduct official agency business pursuant to DoDI 8510.01.

11.4. FIS.

a. WHS-serviced Components' IT service providers will ensure RIM controls and recordkeeping functionality for retention, disposition, and migration are built into:

(1) FIS, applications, databases, cloud computing solutions, and emerging technologies authorized for deployment on the DODIN.

(2) Applicable editions of National Institute of Standards and Technology publications.

b. In accordance with DoD 5010.12-M, the WHS-serviced Components will ensure records management requirements are included in the contracts for goods or services and integrate records management obligations into their existing procurement processes. NARA has provided basic language that can be added to contracts at https://www.archives.gov/records-mgmt/policy/records-mgmt-language; however, WHS-serviced Components may include OSD-specific terms and conditions into contracts.

c. When a WHS-serviced Component stores and manages an FIS on behalf of one or more DoD Components, the information system owner and the program manager of the DoD Component's FIS will coordinate with the OSD Records Administrator on proposing a joint, OSD, or DoD-wide RDS for submission to NARA for its approval.

d. For FISs scheduled for upgrade or replacement, the WHS-serviced Components will ensure the records, information, and data maintained in it are transferred or transitioned to the new FIS in its totality and pursuant to its approved disposition authority. Otherwise, the legacy

system will retain a copy to ensure the records, information, and data are accessible until the end of its mandatory disposition period.

e. For FISs scheduled for decommissioning or retirement, the WHS-serviced Components will ensure the records, information, and data are retained until the end of its mandatory disposition period or the records are transferred to the ownership of the National Archives.

f. Additional information on RIM controls can be found in Section 6 of the OSD Primer.

11.5. DIGITIZING AND REVIEWING RECORDS.

a. Part 1236 of Title 36, CFR, covers the standards and procedures the WHS-serviced Components must apply when digitizing (scanning) records of either permanent or temporary value. Such records include hard copy documents, prints, bound volumes, photographic prints, and mixed-media records.

b. Before digitizing any records, the WHS-serviced Component will:

(1) Prepare draft project plans as required for the organization (not individual offices), digitizing 150 cubic feet or more to identify scope, organization background, host environment, digitization requirements, and procedures for scanning records, retention, and disposition. For additional information, see Section 6 and Appendix D of the OSD Primer.

(2) Before submitting to the OSD RIM Program, the WHS-serviced Components will coordinate the project plans with their internal attorneys or GC, or Office of GC DoD and Component security office, for review and concurrence.

(3) For WHS-serviced Components' digitalization projects of under 150 cubic feet, offices must coordinate with their RIM personnel and document that scans meet the requirements of Part 1236 of Title 36, CFR. WHS-serviced Components' digitalization projects will be approved by the WHS-serviced Component head.

c. RIM personnel will retain approved project plans. Project plans and documentation for all digitization projects are subject to OSD RIM Program inspection, regardless of classification. Failure to meet standards can result in rescanning records. Destruction of original records before verification of meeting scanning standards will result in an unauthorized destruction of records pursuant to Section 1228 of Title 36, CFR.

d. The WHS-serviced Components are not authorized to destroy original sources (hard copy or print photos) for records without validation of meeting standards cited in Part 1236 of Title 36, CFR. Offices may use Appendix D of the OSD Primer as a draft project plan template. Sections 4 and 5 of the project plan, as shown in Appendix D of the OSD Primer, provides quality control criteria necessary to validate compliance with Part 1236 of Title 36, CFR.

SECTION 12: OSD RIM PROGRAM EVALUATION POLICY

12.1. GENERAL.

Pursuant to Part 1220.34(j) of Title 36, CFR, OMB Circular A-130, and DoDI 5015.02, the OSD Records Administrator is charged with conducting formal evaluations to measure the effectiveness of records management programs and practices, and to ensure compliance with NARA and DoD regulations.

a. The purpose of these evaluations is to:

(1) Provide the OSD Records Administrator and WHS-serviced Component heads with an assessment of compliance with OSD RIM processes, procedures, and policies and specific records management topics.

(2) Identify material weakness within the WHS-serviced Components or with OSD RIM policies and procedures.

b. Evaluations are conducted through on-site meetings, using teleconferences or web conferences, surveys, and authorized web collaboration tools or any combination as necessary.

12.2. APPLICABILITY AND CRITERIA.

All WHS-serviced Components are subject to evaluation and assessment pursuant to Part 1220.34(j) of Title 36. The WHS-serviced Components will be evaluated on their compliance with this issuance, the OSD Primer, the OSD RDS, and RIM requirements as issued by OMB, NARA, or the Government Accountability Office.

a. All records and information will be made available for evaluation, regardless of form, format, location, or classification. The OSD RIM Program will provide appropriate documentation for access to NSI. This includes records and information created, maintained, and received within DoD classified networks, FISs, websites and social media, cloud services platforms, and emerging technologies.

b. Upon request, the WHS-serviced Components will provide the OSD RIM Program with documentation including, but not limited to:

(1) RIM standard operating procedures.

(2) Training programs.

(3) WHS-serviced Component RIM personnel roles in the design and development of information systems.

(4) Internal assessments.

(5) Copies of SF-135s.

(6) FIS migration plans.

(7) File plans.

(8) Intro and exit briefing materials.

c. Within 60 days of completion of evaluation, the OSD RIM Program will provide a written report and identifying status (compliance or non-compliance), results, findings, and recommendations for the WHS-serviced Components evaluated.

d. WHS-serviced Components found non-compliant will develop a plan of actions and milestones (POAM) and submit it to the OSD Records Administrator for approval. The WHS-serviced Components will submit quarterly status reports to the OSD Records Administrator until all findings and recommendations are closed. The OSD RIM Program will conduct a follow up evaluation 6 months after approval of the POAM.

12.3. INTERNAL RIM EVALUATIONS.

In accordance with DoDI 5015.02 and this issuance, the WHS-serviced Components will conduct internal RIM evaluations.

a. Section 10 of the OSD Primer provides criteria and procedures for execution of internal RIM evaluations.

b. Internal RIM evaluations will be in writing and identify recommendations, findings, and remediation.

c. RIM personnel for the WHS-serviced Components evaluated will develop a POAM to resolve all recommendations and findings. The WHS-serviced Component head will sign the POAM.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
ATOMAL	NATO security category
CFR	Code of Federal Regulations
CIO	chief information officer
COSMIC	NATO security category
CRMO	Component records management officer
CUI	controlled unclassified information
DAFA	Defense Agency and DoD Field Activity
DD	Department of Defense (form)
DoDD	DoD directive
DoDI	DoD instruction
DODIN	DoD information network
DoDM	DoD manual
E.O.	Executive order
ePHI	electronic protected health information
ESD	Executive Services Directorate
FIS	Federal information system
FRC	Federal records center
GC	general counsel
GC DoD	General Counsel of the Department of Defense
GRS	General Records Schedule
HIPAA	Health Insurance Portability and Accountability Act
IT	information technology
JWICS	Joint Worldwide Intelligence Communications System
NARA	National Archives and Records Administration
NATO	North Atlantic Treaty Organization
NIPRNET	Non-classified Internet Protocol Router Network
NSI	national security information
OCA	original classification authority
OMB	Office of Management and Budget

ACRONYM	MEANING
PA	Presidential appointee
PAS	Presidentially appointed, Senate-confirmed
PDF	portable document format
PHI	protected health information
PIA	privacy impact assessment
PII	personally identifiable information
PIO/DA&M	Performance Improvement Office/Director of Administration and Management
POAM	plan of actions and milestones
.PST	personal storage table
RC	records custodian
RDD	Records and Declassification Division
RDS	records disposition schedule
RIM	records and information management
RL	records liaison
RM	records manager
SAORM	Senior Agency Official for Records Management
SD	Secretary of Defense (form)
SF	standard form
SIPRNET	Secret Internet Protocol Router Network
SNS	social networking site
SORN	system of records notice
U.S.C.	United States Code
WHS	Washington Headquarters Services

G.2. DEFINITIONS.

Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

TERM	DEFINITION
access	The availability of or the permission to consult records, archives, or manuscripts. The ability and opportunity to obtain classified or administratively controlled information or records.
accession	The transfer of the legal and physical custody of permanent records from an agency to the National Archives.

TERM	DEFINITION
agency	Defined in Section 551 of Title 5, U.S.C.
ATOMAL	The NATO classification given to U.S. Restricted Data or Formerly Restricted Data, or United Kingdom atomic nuclear-energy information released to NATO.
audiovisual files	Files in pictorial or aural form, regardless of format. This includes still photos, graphic arts such as posters and original art, motion pictures, video recordings, audio or sound recordings, microform, and related records.
authenticity of OSD records and information	The quality of being genuine, not a counterfeit, and free from tampering. This is typically inferred from internal and external evidence, including its physical characteristics, structure, content, and context.
CAPSTONE	NARA approach to managing Federal record e-mails, instant messages, text messages, and chat messages that serve a similar purpose as email to facilitate communication and information sharing.
closed file or records	File unit or series containing documents on which action has been completed and to which additional documents are not likely to be added.
cloud computing	Defined in National Institute of Standards and Technology Special Publication 800-145.
contracting agency	Defined in Part 60-1.3 of Title 41, CFR.
contract	A mutually binding legal relationship obligating the seller to furnish the supplies or services (including construction) and the buyer to pay for them. It includes all types of commitments that obligate the U.S. Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing. In addition to bilateral instruments, contracts include (but are not limited to) awards and notices of awards; job orders or task letters issued under basic ordering agreements; letter contracts; orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance; and bilateral contract modifications. Contracts do not include grants and cooperative agreements covered by Chapter 63 of Title 31, U.S.C.

TERM	DEFINITION
contract personnel	A contractor's employees or other personnel (including officers, agents, and subcontractors) provided by the contractor to render services under this contract.
convenience file	A file containing duplicates of records kept near the point of use for ease of reference.
COSMIC	The NATO classification for Top Secret information.
copy	A reproduction of the contents of an original document, prepared simultaneously or separately, and usually identified by function or by method of creation. Copies identified by function may include action copy, file copy, or record copy, information or reference copy, official copy, and tickler copy. For 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. See "non-record material" and "records."
CRMO	The official who: Coordinates the records management activities of an OSD Component, including headquarters or in regional offices. Serves as the primary Component official who coordinates records management matters with the Federal records officer and any other local oversight agencies. Coordinates changes to the records schedule with the Federal records officer and local program managers overseeing an organization's records from their creation and preservation through to disposal. Typical responsibilities include: Establishing new records management systems. Developing, maintaining, verifying, and evaluating existing systems. Overseeing the switch from paper to electronic record-keeping.
current records	Records necessary to conduct the current business of an office and therefore generally maintained in office space and equipment. Also called "active records."

TERM	DEFINITION
DAFA RM or DoD Advisory Committee RM	The official who: Coordinates the records management activities of an OSD RIM Program-serviced DAFA or DoD Advisory Committee, including headquarters or in regional offices. Serves as the primary WHS-serviced Component official who coordinates records management matters with the Federal records officer and any other local oversight agencies. Coordinates changes to the records schedule with the Federal records officer and local program managers overseeing an organization's records from their creation and preservation through to disposal. Typical responsibilities include: Establishing new records management systems. Developing, maintaining, verifying, and evaluating existing systems. Overseeing the switch from paper to electronic record-keeping.
department	One of the executive departments listed in Section 101 of Title 5, U.S.C.
DoD Advisory Committee	A group of people appointed for a specific function pursuant to the authorities of the President of the United States, as directed by Congress, Federal law, or the Title 10, U.S.C., authorities of the Secretary of Defense, Deputy Secretary of Defense, Under Secretaries of Defense, Assistant Secretaries of Defense, Assistants to the Secretary of Defense, Secretary of Defense, and DAFA directors. These groups augment the knowledge and skills of a DoD Component or program office; provide recommendations or key information and materials; and may be referred to as Federal Advisory Committees, committees, special study groups, task forces, boards, commissions, councils, and similar groups established to provide advice, ideas, options, and opinions to the Federal Government. Such groups may or may not be subject to the Federal Advisory Committee Act.

TERM	DEFINITION
DoD Advisory Committee head	An individual or individual(s) assigned overall responsibility for the establishment, oversight, or execution of a committee, special study group, task force, board, commission, council, and similar groups, whether or not it is subject to the Federal Advisory Committee Act. This includes but is not limited to the Designated Federal Officer for an advisory committee subject to the Federal Advisory Committee Act or, if the group is not subject to the Federal Advisory Committee Act, the individual(s) designated pursuant to the authorities granted by the Secretary of Defense, Deputy Secretary, Under Secretaries, Assistant Secretaries, or DAFA heads pursuant to their general Title 10, U.S.C., authorities, or as directed by Congress or Federal law.
DoD Component	Unless otherwise noted, includes the OSD; Military Departments, including the Coast Guard when assigned to the Department of the Navy; DAFAs; Combatant Commands; WHS; the Uniformed Services University of the Health Sciences; and all non-appropriated fund instrumentalities.
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 under the Federal Records Act. The term includes both record content and associated metadata that the agency determines is required to meet agency business needs.
e-messages	Short for electronic messages; refers to e-mail and other e-messaging systems that are used for purposes of communicating between individuals.
e-messaging accounts	Accounts that allow users to send communications in real-time or for later viewing. They are used to send messages from one account to another account or from one account to many accounts. Many e-messaging systems also support the use of attachments. They can reside on agency networks and devices, on personal devices, or be hosted by third party providers.

TERM	DEFINITION
employee	For purposes of determining the individuals subject to Section 207 of Title 18, U.S.C., any officer or employee of the executive branch or any independent agency that is not a part of the legislative or judicial branches. The term does not include the President or the Vice President, an enlisted Service member, or an officer or employee of the District of Columbia. The term includes an individual appointed as an employee or detailed to the Federal Government under Chapter 62 of Title 42, U.S.C., also known as the "Intergovernmental Personnel Act," or specifically subject to Section 207 of Title 18, U.S.C., under the terms of another statute. It encompasses senior employees, very senior employees, special U.S. Government employees, and employees serving without compensation.
ePHI	Individually identifiable health information that is created, received, maintained, or transmitted in electronic form by a covered entity or business associate. It does not include individually identifiable health information in paper or oral form.
essential or vital records	Records that are needed to meet operational responsibilities under national security emergencies or other emergencies or disaster conditions (i.e., emergency operating records) or to protect the legal and financial rights of the U.S. Government and those affected by U.S. Government activities, such as legal and financial rights records.
evidential value	The usefulness of records in documenting the organization, functions, and activities of the agency creating or receiving them. See "historical value."

TERM	DEFINITION
Federal records officer	An individual who serves as the official responsible for overseeing their agency's records management program. A Federal records officer: Ensures that their agency has an up-to-date records management directive. Creates and maintains a network of RLs responsible for overseeing the program in headquarters and field offices in cooperation with the Federal records officer. Serves as the primary agency official who coordinates records management matters with NARA and other oversight agencies. Coordinates the development of a records schedule with NARA, IT, program, and agency officials. The records schedule identifies records as either temporary or permanent. All records schedules must be approved by NARA.
file numbers	The OSD alpha-numeric coding for identification of subject matter and related content. An index or file plan to associate concepts with specific numbers, which are then applied to the materials being filed.
file series exemption	Exemptions from automatic declassification that are intended for records that, during their review by the agency, have been determined to require further classification beyond the 25-year mark.
FIS	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
FRC	A facility, sometimes specially designed and constructed, for the low-cost, efficient storage and furnishing of reference service on semi-current records pending their ultimate disposition. Generally, this term refers to the FRCs maintained by NARA; but provisions exist, providing stringent criteria are met, to permit individual Federal agencies to create their own records centers or to contract this service out to civilian enterprises.
government control	The ability of the originating government agency to regulate access to documentary materials, especially classified information.

TERM	DEFINITION
GRS	A schedule issued by the Archivist of the United States governing the disposition of specified recurring series common to several or all agencies of the Federal Government. These series include civilian personnel and payroll records, procurement, budget, travel, electronic, audiovisual, and administrative management records. When records described in the GRS are used by any Federal agency, their disposition is governed by the GRS. Exceptions may be granted only by the Archivist of the United States. The GRS does not apply to an agency's program records.
hard copy records	Records consisting primarily of written words on paper or other hard copy surfaces.
historical value	The usefulness of records for historical research concerning the agency of origin.
inactive records	Records that are no longer required in the conduct of current business and therefore can be transferred to an FRC or destroyed, per approved disposition schedule.
information system	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
IT service provider	Defined in DoDI 5015.02 as "IT service."
Kyl-Lott review	An evaluation of all permanent classified records and information eligible for declassification to potentially identify and protect from declassification and release all marked and unmarked Restricted Data, Formerly Restricted Data, and Trans-classified Foreign Nuclear Information.
life cycle of records	The concept that records pass through three stages: creation and receipt, maintenance and use, and disposition. Records should be managed properly during all three phases of the life cycle.
litigation hold	A temporary suspension of the agency's document retention destruction policies for the paper documents and electronically stored information that may be (or are reasonably anticipated to be) relevant to a lawsuit. Also known as a "legal hold," "preservation order," "records freeze," or "hold order."
metadata	Defined in National Institute of Standards and Technology Special Publication 800-53 Revision 5.

TERM	DEFINITION
non-record materials	U.S. Government-owned documentary materials that do not meet the conditions of records status or that are specifically excluded from the statutory definition of records (see "records"). An agency's records management program also needs to include managing non-record materials. There are three specific categories of materials excluded from the statutory definition of records: Library and museum material (but only if such material is made or acquired and preserved solely for reference or exhibition purposes), including physical exhibits, artifacts, and other material objects lacking evidential value. Extra copies of documents, but only if the sole reason such copies are preserved is for convenience of reference. Stocks of publications and of processed documents. Stocks do not include serial or record sets of agency publications and processed documents, including annual reports, brochures, pamphlets, books, handbooks, posters, and maps.
NSI	Information that has been determined pursuant to E.O. 13526, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status.
OSD CAPSTONE officials	Officials (e.g., personnel identified in the United States Government Policy and Supporting Positions, commonly known as "the Plum Book") generally responsible for agency-, program policy-, or mission-related actions designated pursuant to NARA GRS 6.1.
OSD RIM Program-serviced DAFAs	Defined in Section 2 of the OSD Primer.
permanent records	Records appraised by the Archivist of the United States as having enduring value because they document the organization and functions of the agency that created or received them, or they contain significant information on persons, things, problems, and conditions with which the agency deals.
persistent format	An encoding format used to preserve digital data because it is expected to remain usable, reliable, and accessible over a long period of time. Also referred to as "sustainable format."

TERM	DEFINITION
personal files	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 government. Personal files are required to be filed separately from official records of the office.
PHI	Pursuant to Public Law 104-191, also known and referred to in this issuance as the "Health Insurance Portability and Accountability Act (HIPAA)", information considered to be individually identifiable information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations (e.g., PHI healthcare business uses). Under HIPAA, PHI includes health information such as diagnoses, treatment information, medical test results, and prescription information; and national identification numbers and demographic information such as birth dates, gender, ethnicity, and contact and emergency contact information.
PII	Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. For purposes of this issuance, the term "PII" is personal information in any identifiable form.
positive control	Policies and procedures that control the creation, transmission, receipt, and maintenance and disposition of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion, and alteration (e.g., via hacking, use, and concealment).
prime contractor	Defined in Section 8701 of Title 41, U.S.C.
Principal Staff Assistant program offices	Defined in Paragraph c. of Enclosure 2 of DoDD 5100.01. Organizations within an OSD Component or DAFA that develop, implement, and manage appropriate policies and procedures regarding specified functions. Program offices also perform oversight and periodic review of operating offices to ensure their compliance with Federal law, regulations, and DoD issuances.

TERM	DEFINITION
program records	Records created or received and maintained by an agency in the conduct of the substantive mission functions (as opposed to administrative or housekeeping functions). Sometimes called "operational records."
RC or RL	Interchangeable title used for individuals designed to work directly with OSD employees, Service members, and contract personnel to implement OSD RIM guidance, develop standard operating procedures, or implement guidance created or received from the OSD Components and OSD RIM Program-serviced DAFAs as applicable.
RDS	The administrative document used by OSD to obtain legal disposal authority for categories of its records. When authorized by the Archivist of the United States, these schedules grant continuing authority to dispose of identifiable categories of OSD records that already have accumulated and that will accumulate in the future. Sometimes called a "records control schedule," "records retention schedule," or a "records schedule."
reasonable anticipation of litigation	A legal standard state in which an organization is on notice of a credible probability that it will become involved in litigation or it seriously contemplates initiating litigation or takes specific actions to commence litigation.
record disposition authority moratorium	A temporary suspension of OSD record retention policies for documents that may be relevant to a lawsuit or that are reasonably anticipated to be relevant. Also known as a "litigation hold," "preservation order, notice," or "records freeze."
records	Includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the U.S. Government or because of the informational value of data in them. This 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.

TERM	DEFINITION
records management	Defined in Section 2901 of Title 44, U.S.C.
reference files	Also known as "technical reference files," "reference copies," or "information copies," reference files may appear in these forms: A copy of a record kept for easy access to the information it contains, as opposed to its intrinsic or evidential value. A copy of a record distributed to make recipients aware of the content but not directing the recipient to take any action on the matter. A specific copy used as a benchmark for purposes of checking the quality of other copies.
responsive records	Documents or electronic records determined to be within the scope of a Freedom of Information Act request or litigation.
reporting office	A business unit with the responsibility for maintaining the authoritative version of a specific series of records that support the functions and operations of such unit.
retention	The period that a specific series of records or collection(s) of data or information is to be kept. Also referred to as a "retention period."
retention schedule	A document that identifies and describes an organization's records, usually at the series level, and provides instructions for the disposition of records throughout their life cycle. Also referred to as an RDS, "records schedule," "records retention schedule," or "transfer schedule." The schedule may take the form of: An SF-115 that has been approved by NARA to authorize the disposition of Federal records; A GRS issued by NARA; or A printed agency manual or directive containing the records descriptions and disposition instructions approved by NARA on one or more SF-115(s) or issued by NARA in the GRS.
retirement	The movement of inactive files having a permanent or long-term value to an FRC for storage, servicing, and ultimate disposition. See "transfer or transferring" or "accession."

TERM	DEFINITION
RIM	The field of management responsible for establishing and implementing policies, systems, and procedures to capture, create, access, distribute, use, store, secure, retrieve, and ensure disposition of an organization's records and information.
RM	An individual overseeing the records management compliance of reporting components, directorates, and divisions within a WHS-serviced Component. Typical responsibilities include establishing new records management systems; developing, maintaining, verifying, and evaluating existing systems; and overseeing the switch from paper to electronic record-keeping. RMs coordinate with office RC and RLs on the oversight, implementation, and management of records and information created in accordance with their programmatic responsibilities.
subcontractor	Defined in Part 60-1.3 of Title 41, CFR.
temporary records	Records determined by NARA to be disposable or nonpermanent. NARA approves such records for destruction or occasionally for donation to an eligible person or organization.
transfer or transferring	Moving records into the physical custody of a NARA FRC. The transferring agency retains the legal custody of transferred records until final disposition.
unauthorized disposal	The improper removal of records without NARA approval or the willful or accidental destruction of records without regard to a NARA-approved records schedule. Unauthorized disposition of Federal records is against the law and punishable by up to $250,000 in fines and imprisonment pursuant to Section 3106 of Title 44, U.S.C., and Section 2071 of Title 18, U.S.C.
unscheduled records	Records whose final disposition has not been approved by NARA. Unscheduled records may not be destroyed or deleted.
vicarious liability	Liability that a supervisory party (e.g., an employer) bears for the actionable conduct of a subordinate or associate (e.g., an employee) based on the relationship between the two parties.
WHS-serviced Component CRMOs and RMs	CRMOs appointed by OSD Component heads; DAFA RMs appointed by OSD RIM Program-serviced DAFA directors; and DoD Advisory Committee RMs appointed by their committee heads.

TERM	DEFINITION
WHS-serviced Components	The OSD Components, OSD RIM Program-serviced DAFAs, and DoD Advisory Committees.
working files	Documents such as rough notes, calculations, or drafts assembled or created and used to prepare or analyze other documents. Also called "working papers."

REFERENCES

Administrative Instruction 50, "Historical Research in the Files of the Office of the Secretary of Defense," May 20, 2015, as amended

Code of Federal Regulations, Title 36, Chapter XII, Subchapter B

Code of Federal Regulations, Title 41

Code of Federal Regulations, Title 48

Department of Justice, Office of Information Policy, "OIP Guidance: Applying a Presumption of Openness and the Foreseeable Harm Standard," current edition[1]

Deputy Secretary of Defense, "DoD Data Strategy," September 30, 2020[2]

DoD Architecture Framework, current version[3]

DoD 5010.12-M, "Procedures for the Acquisition and Management of Technical Data," May 14, 1993, as amended

DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007

DoD 5500.07-R, "Joint Ethics Regulation (JER)," August 30, 1993, as amended

DoD Directive 3020.26, "DoD Continuity Policy," February 14, 2018

DoD Directive 5100.01, "Functions of the Department of Defense and its Major Components," December 21, 2010, as amended

DoD Directive 5100.55, "United States Security Authority for North Atlantic Treaty Organization Affairs (USSAN)," February 27, 2006

DoD Directive 5101.01, "DoD Executive Agent", February 7, 2022

DoD Directive 5110.04, "Washington Headquarters Services (WHS)," March 27, 2013

DoD Directive 5400.07, "DoD Freedom of Information Act (FOIA) Program," April 5, 2019

DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015, as amended

DoD Instruction 5025.01, "DoD Issuances Program," August 1, 2016, as amended

DoD Instruction 5040.07, "Visual Information (VI) Productions," February 21, 2013, as amended

DoD Instruction 5200.01, "DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI)," April 21, 2016, as amended

DoD Instruction 5200.48 "Controlled Unclassified Information (CUI)," March 6, 2020

DoD Instruction 5400.11, "DoD Privacy and Civil Liberties Programs," January 29, 2019, as amended

[1] Available at https://www.justice.gov/oip/oip-guidance-applying-presumption-openness-and-foreseeable-harm-standard

[2] Available at https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF

[3] Available at https://dodcio.defense.gov/Library/DoD-Architecture-Framework/

DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," July 14, 2015, as amended

DoD Instruction 6025.18, "Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule Compliance in DoD Health Care Programs," March 13, 2019

DoD Instruction 8170.01, "Online Information Management and Electronic Messaging," January 2, 2019, as amended

DoD Instruction 8510.01, "Risk Management Framework for DoD Systems," July 19, 2022

DoD Instruction 8580.1, "Information Assurance (IA) in the Defense Acquisition System," July 9, 2004

DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended

DoD Manual 5200.01, Volume 2, "DoD Information Security Program: Marking of Information," February 24, 2012, as amended

DoD Manual 5200.01, Volume 3, "DoD Information Security Program: Protection of Classified Information," February 24, 2012, as amended

DoD Manual 5230.30, "DoD Mandatory Declassification Review (MDR) Program," December 22, 2011, as amended

DoD Manual 5400.07, "DoD Freedom of Information Act (FOIA) Program," January 25, 2017

DoD Manual 5400.11, Volume 2, "DoD Privacy and Civil Liberties Programs: Breach Preparedness and Response Plan," May 6, 2021

DoD Manual 6025.18, "Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule in DoD Health Care Programs," March 13, 2019

DoD Manual 8910.01, "DoD Information Collections Manual," June 30, 2014, as amended

Executive Order 13526, "Classified National Security Information," December 29, 2009

Federal Emergency Management Agency Federal Continuity Directive 1, "Federal Executive Branch National Continuity Program and Requirements," January 17, 2017

General Records Schedule 6.1, "Email and Other Electronic Messages Managed under a Capstone Approach," January 2023

General Records Schedule 6.2, "Federal Advisory Committee Records," August 2015

National Archives and Records Administration Bulletin 2017-01, "Agency Records Management Training Requirements," November 29, 2016

National Archives and Records Administration Guide to the Inventory, Scheduling, and Disposition of Federal Records[4]

National Institute of Standards and Technology Special Publication 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," September 2020, as amended

[4] Available at https://www.archives.gov/records-mgmt/scheduling/values?_ga=2.147446260.231599913.1643731363-1717185861.1605815776

National Institute of Standards and Technology Special Publication 800-145, "The NIST Definition of Cloud Computing," September 2011

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

Office of Management and Budget Circular A-130, "Managing Information as a Strategic Resource," July 28, 2016

Office of Management and Budget and National Archives and Records Administration Memorandum M-19-21, "Transition to Electronic Records," June 28, 2019

Office of Management and Budget and National Archives and Records Administration Memorandum M-23-07. "Update to Transition to Electronic Records," December 23, 2022

Office of Personnel Management Operating Manual, "The Guide to Personnel Recordkeeping," June 1, 2011, as amended

Office of the Secretary of Defense, "Records and Information Management Program Primer," current edition[5]

Office of the Secretary of Defense Records Disposition Schedule, current edition

Public Law 104-191, "Health Insurance Portability and Accountability Act of 1996," August 21, 1996

Public Law 105-261, "Strom Thurmond National Defense Authorization Act for Fiscal Year 1999," October 17, 1998

Public Law 113-187, "Presidential and Federal Records Act Amendments of 2014," November 26, 2014

Senate Committee on Homeland Security and Governmental Affairs and House Committee on Government Reform, "United States Government Policy and Supporting Positions (Plum Book)," current edition

United States Code, Title 5

United States Code, Title 10

United States Code, Title 18

United States Code, Title 31, Chapter 63

United States Code, Title 40, Subtitle III (also known as the "Clinger-Cohen Act of 1996")

United States Code, Title 41, Section 8701

United States Code, Title 42

United States Code, Title 44

United States Security Authority for North Atlantic Treaty Organization Affairs Instruction 1-07, "Implementation of the North Atlantic Treaty Organization Security Requirements," April 5, 2007

United States Supreme Court, "Federal Rules of Civil Procedure," current edition

[5] Available on the RDD Website.