Office of the Deputy Chief Management Officer

# ADMINISTRATIVE INSTRUCTION

**NUMBER** 15
May 3, 2013
Incorporating Change 1, April 19, 2017

DCMO

SUBJECT: OSD Records and Information Management Program

References: See Enclosure 1

1. PURPOSE. This administrative instruction (AI):

a. Updates and renames AI 15, Volume I (Reference (a)), in accordance with the authorities in DoD Directive (DoDD) 5110.04 (Reference (b)), DoD Instruction 5015.02 (Reference (c)), chapters 29, 31, and 33 of Title 44, United States Code (U.S.C.) (Reference (d)), and chapter XII, subchapter B of Title 36, Code of Federal Regulations (CFR) (Reference (e)) to implement DoD policy, assign responsibilities, and provide procedures for the OSD Records Management and Information Management Program.

b. Establishes responsibilities and administrative procedures for the lifecycle management of records and information, as required by References (c) through (e).

c. Cancels AI 15, Volume II (Reference (f)) and authorizes the OSD Records Disposition Schedule (Reference (g)) to be published online at http://www.dtic.mil/whs/esd/rdd/recordsmgt.html. The schedule will be updated as National Archives and Records Administration (NARA) approves changes to the disposition schedules of the Washington Headquarters Services (WHS)-Serviced Components or revises the General Records Schedules (GRS) citations.

2. APPLICABILITY. This AI:

a. Applies to OSD, WHS, and other DoD Components and entities to whom WHS provides records management support (referred to collectively in this AI as the "WHS-serviced Components").

b. Applies to all advisory committees established or supported by the DoD , including those advisory committees exempted from Title 5, U.S.C. Appendix 2 (also known and referred to in this AI as "The Federal Advisory Committee Act of 1972 (FACA)") (Reference (h)) by an act of Congress.

3. POLICY. It is DoD policy, in accordance with Reference (c), to:

a. Limit the creation of records to those essential for the efficient conduct of official business and to preserve those of continuing value while systematically eliminating all others.

b. Ensure the management of records is in compliance with parts 1220-1239 of Reference (d), Reference (e), and chapters 102-193 of Title 41 CFR (Reference (i)).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. Enclosures 3 through 11 address the specific functions and requirements of the OSD Records and Information Management Program.

6. INFORMATION COLLECTIONS. The SD Form 828, "OSD Electronic Information System Appraisal," referred to in paragraph 12.b of Enclosure 6 of this AI, has been assigned report control symbol DD-DA&M(AR) 2517 in accordance with the procedures in DoD Manual 8910.01 (Reference (j)).

7. RELEASABILITY. **Cleared for public release**. This AI is available on the DoD Issuances Website at http://www.dtic.mil/whs/directives.

8. SUMMARY OF CHANGE 1. The changes to this issuance are administrative and update organizational titles and references for accuracy.

9. EFFECTIVE DATE. This AI is effective May 13, 2013.

Michael L. Rhodes
Director of Administration and Management

Enclosures:

1. References
2. Responsibilities
3. Management of Records and Information
4. Disposition Procedures
5. Disposition of Personal Files and Non-record Materials
6. Electronic Records
7. Preparing Records for Transfer to the FRC
8. Packing and Shipping Procedures for Transfer of Records
9. Recall of Records from the FRC

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES ..... 7

ENCLOSURE 2: RESPONSIBILITIES ..... 9

DIRECTOR FOR ADMINISTRATION, OFFICE OF THE DEPUTY CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE ..... 9
DIRECTOR, WHS ..... 9
OSD RECORDS ADMINISTRATOR ..... 9
ACMO ..... 11
WHS-SERVICED COMPONENT HEADS ..... 11
WHS-SERVICED COMPONENT CIOS ..... 13
WHS-SERVICED COMPONENT CRMOS AND RLS ..... 14
DOD EMPLOYEES OF WHS-SERVICED COMPONENTS ..... 15

ENCLOSURE 3: MANAGEMENT OF RECORDS AND INFORMATION ..... 16

OSD FUNCTIONAL FILE SYSTEM ..... 16
RECORDS ARRANGEMENTS ..... 16
FILE PLAN DESIGNATION ..... 16
RECORDS CATEGORIES ..... 18
BASIC FILE GROUPING ..... 19
FILING ARRANGEMENTS ..... 21
FUNCTIONAL FILE SYSTEM CONCEPT ..... 21
ORGANIZATION OF THE OSD FILE SYSTEM ..... 22
APPLICABILITY ..... 23
FUNCTIONAL AREA NUMBERING SYSTEM ..... 23
FILES CONTROL ..... 24
FILES CUTOFF PROCEDURES ..... 25
PREPARING AND USING GUIDE CARDS, FILE FOLDERS, AND LABELS ..... 26
CROSS REFERENCE ..... 30
LABELING FILE DRAWERS ..... 30
CLASSIFIED INFORMATION ..... 31
MANAGEMENT OF DOCUMENTS AND INFORMATION ..... 31

ENCLOSURE 4: DISPOSITION PROCEDURES ..... 33

GENERAL ..... 33
DISPOSITION STANDARDS ..... 33
SOURCE OF RETENTION PERIODS ..... 33
CHANGES TO RETENTION PERIODS ..... 33
RECORD FREEZES, PRESERVATION ORDERS, OR MORATORIUMS ..... 34
UNSCHEDULED (UNIDENTIFIED) RECORDS ..... 34
DISPOSITION INSTRUCTION ..... 34
DISPOSITION PROCEDURES ..... 36
TRANSFER OF FILES ..... 36

TRANSFER TO OTHER GOVERNMENT AGENCIES....36
NATO DOCUMENTS....37
DISPOSITION OF FILES AND CHANGES OF STATUS....37
RECORD SEARCHES AND PRESERVATION ORDERS....38
REQUESTING MODIFICATIONS TO THE OSD RECORDS DISPOSITION SCHEDULE....39

ENCLOSURE 5: DISPOSITION OF PERSONAL FILES AND NON-RECORD MATERIALS....42
RECORD AND NON-RECORD MATERIALS OF GOVERNMENT OFFICIALS....42
DISTINGUISHING PERSONAL FILES AND NON-RECORD MATERIAL....42
PERSONAL FILES....42
NON-RECORD MATERIALS....43
INSTRUCTIONS FOR REMOVAL OF PERSONAL FILES....45
ACCESS TO DONATED PERSONAL FILES, NON-RECORD MATERIALS, AND FEDERAL RECORDS....46
REMOVAL SUBJECT TO A NONDISCLOSURE AGREEMENT....47

ENCLOSURE 6: ELECTRONIC RECORDS....48

GENERAL....48
CATEGORIES OF ELECTRONIC RECORDS....48
ELECTRONIC RECORDS MANAGEMENT....50
ELECTRONIC MAIL (E-MAIL) AND INSTANT MESSAGING (IM)....57
RECORDS MANAGEMENT REQUIREMENTS FOR E-MAIL AND IM SYSTEMS....59
DISPOSITION OF E-MAIL AND IM....59
WEB 2.0 (SNS)....60
CLOUD COMPUTING SYSTEMS....61
RMA OR SYSTEMS....61
CAPITAL PLANNING AND MANAGING INFORMATION SYSTEMS....61
JUDICIAL USE....63
SCHEDULING....63
TRANFERRING PERMANENT ELECTRONIC RECORDS TO NARA....65
ADDITIONAL GUIDANCE....67

ENCLOSURE 7: PREPARING RECORDS FOR TRANSFER TO THE FRC....69

BACKGROUND....69
FILE TRANSFER SELECTION....69
SCREENING....69
FILING RECOMMENDATIONS....70

ENCLOSURE 8: PACKING AND SHIPPING PROCEDURES FOR TRANSFER OF RECORDS....71

PACKAGING RECORDS FOR TRANSFER TO FRC....71
SHIPPING CONTAINERS AND RELATED SUPPLIES....71

REQUISITIONING ..... 71
SHIPPING CONTAINERS FOR ODD-SIZED DOCUMENTS ..... 71
LISTING RECORDS FOR TRANSFER OR RETIREMENT ..... 71
TRANSFER OF RECORDS TO OTHER EXTERNAL ORGANIZATIONS ..... 72
RECORD PREPARATION FOR RETIREMENT AND SHIPMENT TO THE FRC ..... 72
RETIREMENT OF CLASSIFIED SECURITY INFORMATION ..... 76
MATERIAL THAT SHOULD BE DESTROYED ..... 77
USE OF RESTRICTED COLUMN ..... 77
ARRANGEMENT OF FILES IN FIBERBOARD BOXES ..... 78
PACKING AND SHIPPING CLASSIFIED FILES ..... 80

ENCLOSURE 9: RECALL OF RECORDS FROM THE FRC ..... 81

OFFICIALS AUTHORIZED TO MAKE RECALLS ..... 81
NORMAL RECALL PROCEDURES ..... 81
URGENT REQUESTS ..... 81
RETURNING RECORDS ..... 81
ACCESS TO FEDERAL RECORDS BY OTHER INDIVIDUALS ..... 82

GLOSSARY ..... 83

PART I. ACRONYMS AND ABBREVIATIONS ..... 83
PART II. DEFINITIONS ..... 84

TABLES

1. Functional Area Numbering System ..... 22
2. Example of Major Categories ..... 23
3. Examples of File Numbers ..... 23
4. Examples of Tiers Within a Series ..... 24
5. Abbreviations for Records Labels ..... 30

FIGURES:

1. Sample Format for a File Plan ..... 18
2. Records Categories ..... 19
3. Examples of Guide Cards and File Drawer Entries ..... 26
4. Samples of Folder Label Entries ..... 27
5. Samples of Label Entries for Binders Containing Reference Publications ..... 28
6. Sample of Label Entries for Electronic Media ..... 29
7. Disposition Instructions ..... 35
8. Flat File Structure. ..... 53
9. Subject Matter File Structure ..... 54
10. Consolidated File Structure ..... 55
11. Hierarchal File Structure ..... 56
12. Example of Standard Form 135 (SF135), “Records Transmittal and Receipt” ..... 74
13. Labeling of Retirement Boxes ..... 76
14. Example and Instructions for a Properly Stacked Pallet ..... 79

ENCLOSURE 1

REFERENCES

(a) Administrative Instruction 15, Volume I, "Office of the Secretary of Defense (OSD) Records Management Program - Administrative Procedures," November 14, 2006, as amended (hereby cancelled)
(b) DoD Directive 5110.04, "Washington Headquarters Services (WHS)," March 27, 2013
(c) DoD Instruction 5015.02, "DoD Records Management Program," February 24, 2015
(d) Title 44, United States Code
(e) Chapter XII, subchapter B of Title 36, Code of Federal Regulations
(f) Administrative Instruction 15, Volume II, "Office of the Secretary of Defense (OSD) Records Management Program-Records Disposition Schedules," April 18, 2008 (hereby cancelled)
(g) Office of the Secretary of Defense (OSD) Records Disposition Schedule
(h) Title 5, United States Code (section 552 is also known as "The Freedom of Information Act," section 552a is also known as "The Privacy Act of 1974," and Appendix 2 is also known as "The Federal Advisory Committee Act of 1972")
(i) Title 41, Code of Federal Regulations
(j) DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014, as amended
(k) DoD Manual 5230.30, "DoD Mandatory Declassification Review (MDR) Program," December 22, 2011
(l) Executive Order 13526, "Classified National Security Information," December 29, 2009
(m) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
(n) DoD Instruction 8910.01, "Information Collection and Reporting," May 19, 2014
(o) DoD Directive 3020.26, "Department of Defense Continuity Programs," January 9, 2009
(p) Administrative Instruction 27, "Control of North Atlantic Treaty Organization (NATO) Classified Documents," March 10, 2011
(q) DoD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard," April 25, 2007
(r) Title 18, United States Code
(s) Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition
(t) Executive Order 12829, "National Industrial Security Program," January 6, 1993
(u) Administrative Instruction 50, "Historical Research in the Files of the Office of the Secretary of Defense," May 20, 2015
(v) Office of Management and Budget Circular A-130, "Management of Federal Information Resources," current edition
(w) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
(x) Executive Order 12906, "Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure," April 13, 1994
(y) National Archives Records Disposition Authority, "DoD Visual Information," DAA-0330-2013-0014

(z) National Institute of Standards and Technology (NIST), "The NIST Definition of Cloud Computing," NIST Definition Version, September 28, 2011

# ENCLOSURE 2

## RESPONSIBILITIES

1. DIRECTOR FOR ADMINISTRATION, OFFICE OF THE DEPUTY CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE (DA ODCMO). The DA ODCMO will serve 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 consistent with DoD Manual 5230.30 (Reference (k)).

2. DIRECTOR, WHS. Under the authority, direction, and control of the DA ODCMO, the Director, WHS:

a. Directs and administers the records and information management program for the WHS-serviced Components.

b. Provides guidance to the WHS-serviced Components on the creation, organization, maintenance, use, and disposition of records and information they produce and receive.

c. Cooperates with NARA in developing and applying standards, procedures, and techniques designed to improve the management of records and information; ensures the maintenance and security of records of continuing value; and facilitates the identification, segregation, and disposal of all records of temporary value as well as non-record information.

d. Ensures compliance with References (c) through (e), (i), (j), and (k) through (x).

e. Coordinates with the DoD Chief Information Officer (DoD CIO) on records and information management policy pertaining to information technology (IT) and electronic records.

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

3. OSD RECORDS ADMINISTRATOR. The OSD Records Administrator (Chief, Records, Privacy and Declassification Division (RPDD), Executive Services Directorate (ESD), WHS):

a. Serves as the office of record and the Federal Agency Records Officer for records and information management activities for WHS-serviced Components in accordance with Reference (e).

b. Establishes a comprehensive OSD records and information management program to support the requirements of References (c) through (e), (g) through (i), and (l) through (x).

c. Ensures positive control over the organization, maintenance, use, designation, and disposition of WHS-serviced Components' records and information, regardless of media (paper, electronic, audiovisual, etc.).

d. Maintains and updates the OSD Records Disposition Schedule online at http://www.dtic.mil/whs/esd/rdd/recordsmgt.html as NARA approves changes to the disposition schedules of the WHS-serviced Components or revises the GRS citations.

e. Develops and applies standards, procedures, and techniques for improving records management; ensuring the maintenance and timely retirement of records of continuing value; and facilitating the segregation and disposal of all records of temporary value.

f. Oversees the implementation of this AI as the Federal Agency Records Officer.

g. Acts as the liaison official with NARA, other government agencies, private industry, and private citizens on records and information management matters of WHS-serviced Components.

h. Institutes and oversees a records management evaluation program in accordance with References (e), (i), and Executive Order 13526 (Reference (l)) to ensure compliance of the WHS-serviced Components and to provide for improvements and changes to existing procedures and records schedules to reflect current mission and organizational requirements.

i. Provides DoD employees and contractors of WHS-serviced Components with basic records and information management training in accordance with Reference (c).

j. Monitors the acquisition of IT systems within OSD and WHS enterprise architecture to ensure compliance with records management laws and regulations.

k. Provides the WHS-serviced Components with advice and management assistance when creating new and updating existing records, EISs, including implementing electronic records management, to ensure the systems are adequately documented, secure, and accessible and that disposition instructions are established and implemented.

l. Provides advice and assistance to the WHS-serviced Components on the identification, segregation, retention, and disposition of personal papers in accordance with References (e), (h), and (l).

m. Coordinates, controls, and supervises access to OSD records essential for historical research, ensuring that appropriate safeguards for information security and personal privacy, as outlined by Reference (i) and DoDD 5400.11 (Reference (m)) are followed.

n. Ensures DoD employees, contractors, or officials of WHS-serviced Components do not remove federal records and government-owned non-record information (paper or electronic) from government custody that was not cleared for public use in accordance with References (d), (e), (l), and (m).

o. Manages the transfer of WHS-serviced Component records to and retrieval from the Federal Records Centers (FRCs).

p. Maintains a record on all current suspension actions to normal disposition instructions, such as records holds, freezes, moratoriums, or preservation orders.

q. In consultation with the Advisory Committee Management Officer (ACMO), determines which advisory committee records are subject to processing through the OSD Records Administrator to NARA.

4. ACMO. Under the authority, direction, and control of the DA&M, and the statutory authorities outlined in section 8(b) of Reference (h), the ACMO will ensure all records of advisory committees established or supported by the WHS-serviced Components, including those advisory committees exempted from FACA by an act of Congress, are managed in accordance with this AI.

5. WHS-SERVICED COMPONENT HEADS. The WHS-serviced Component heads will:

a. Establish and sufficiently resource a records and information management program within their organization to support the requirements outlined in References (c) through (e), (g) through (i), (l) through (x) and with the regulations issued there under.

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 records no longer needed for current use (i.e., inactive records) receive appropriate disposition in accordance with the OSD Records Disposition Schedule.

d. Appoint an individual to be the Component Records Management Officer (CRMO) to perform the records management functions, serve as the accountable records custodian in their organization, and liaison with RPDD. The CRMOs must have knowledge of applicable laws and regulations governing records management. This appointment will be made in writing and furnished to the OSD Records Administrator. All appointments will state the organizations supported by the CRMO. Appointment memos will be updated upon the departure or change of the individual(s).

e. Ensure Records Liaisons (RLs) are appointed within each reporting office to perform the records management functions within their organizations and liaison with the CRMO. These appointments will be made in writing and furnished to the CRMO. Appointment memos will be updated upon the departure or change of the individual(s).

f. Ensure all DoD employees and contractors within their organization receive basic records management training at least annually to maintain compliance with Reference (c) and this AI.

g. Ensure all offices within their organization have approved file plans that are accessible to employees and contractors.

h. Evaluate current and potential EISs and databases, ensuring that the record information contained within the systems is retained as required by the OSD Records Disposition Schedule and systems are managed according to the policies in References (c) through (e) and procedures specified in this AI. Record information created or received during the conduct of business and maintained in these systems that is not identified in the OSD Records Disposition Schedule will be brought to the attention of RPDD.

i. Plan and budget for the migration of records and their associated metadata maintained in an EIS or database to new storage media or formats to avoid loss of record data due to media decay or technology obsolescence.

j. Ensure the policies and provisions of Reference (j) and DoD Instruction 8910.01 (Reference (n)) are followed in the creation of OSD records and information.

k. Ensure essential documents and record information needed for continuity of operations are identified and preserved in compliance with DoDD 3020.26 (Reference (o)).

l. Ensure North Atlantic Treaty Organization (NATO) documents are handled in accordance with AI 27 (Reference (p)).

m. Ensure the requirements of Reference (m) are satisfied if creating records or systems of records that are subject to section 552a of Reference (h) (also known and referred to in this AI as "The Privacy Act of 1974 (PA)").

n. Annually remind and caution all employees not to transfer or destroy records in their custody, to include e-mail, except as allowed under Reference (d) and the OSD Records Disposition Schedule.

o. Report to the OSD Records Administrator any actual, impending, or threatened unlawful removal, alteration, or destruction of federal records.

p. Ensure DoD employees and officials manage their personal papers in accordance with References (e) and (h) and Enclosure 5 of this AI.

q. Ensure that records and information posted to commercial and government-owned social media sites (Web 2.0) are maintained in accordance with Reference (e) and the OSD Records Disposition Schedule.

r. Direct contractors performing DoD program functions on behalf of the organization to create and maintain records to document these functions. In accordance with Reference (e)

contracts must specify the delivery to the government of all the information required for the adequate documentation of the contractor-operated program. The contractor will apply the appropriate file identification from the OSD Records Disposition Schedule.

s. Direct in a contract vehicle support contractor personnel within their organizations to:

(1) Maintain government records and information created and received in the course of their day-to-day responsibilities. Ensure that each record set is complete and that enclosures or related papers are retained or accounted for in both paper and electronic filing systems in accordance with the OSD Records Disposition Schedule.

(2) Maintain electronic mail and attachments that document work related activities in accordance with the OSD Records Disposition Schedule.

(3) Ensure that personal files, non-record material, and work-related records and information are maintained separately.

(4) Follow the procedures in Enclosure 5 of this AI when removing personal files.

t. Ensure that records and information maintained on network shared drives (also known as shared drives), websites, or Defense portals are maintained in accordance with the OSD Records Disposition Schedule and Enclosure 6 of this AI.

6. WHS-SERVICED COMPONENT CIOS. WHS-serviced Component CIOs:

a. Provide technical advice and assistance to the WHS-serviced Component heads in order to support the inclusion of electronic records management functions into the design, development, enhancement, and implementation of EISs in accordance with Reference (e) and the OSD Records Disposition Schedule.

b. As part of the capital planning and systems development lifecycle process ensure that:

(1) Records management controls are planned and implemented in the system in accordance with References (c) through (e).

(2) All records in the system will be retrievable and usable for as long as needed to conduct DoD business in accordance with the OSD Records Disposition Schedule, 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 EIS, the WHS-serviced Component heads and CIOs must plan and budget for the migration of records and their associated metadata to new storage media or formats to avoid loss due to media decay or technology obsolescence.

c. Assist in the transfer of permanent electronic records to NARA in accordance with Reference (e) and the OSD Records Disposition Schedule.

d. Use a standard interchange format (e.g., ASCII or XML) when needed to permit the exchange of electronic documents between offices using different software or operating systems.

e. Provide guidance and assistance to the WHS-serviced Component heads with the implementation of the requirements in Enclosures 5 through 7 of this AI and References (c), (e), (j), and (l) through (w).

7. WHS-SERVICED COMPONENT CRMOS AND RLS. WHS-serviced Component CRMOs and RLs:

a. Complete the OSD Records Administrator sponsored training within 3 months of their appointment. CRMOs and RLs should also consider attending NARA's Records Management Training.

b. Ensure every office within their organization has an office file plan. RLs are to prepare and submit file plans to the CRMO for approval. See Enclosure 3 of this AI for filing instructions.

c. Annually review and approve the file plan for each office within their organization to ensure that records are accurately identified.

d. Conduct records searches, implement preservation orders, and ensure organization offices are aware of the responsibilities to safeguard records and information identified in existing preservation orders.

e. Assist their organizations with the application of disposition procedures, to include the destruction and retirement of their records.

f. Notify the OSD Records Administrator of the unauthorized destruction, damage, alienation, or removal of official records.

g. Notify the OSD Records Administrator when officials intend to remove non-record information for personal use.

h. Ensure the proper maintenance of records and non-record information generated by their program offices.

i. Ensure all employees and contractors receive annual basic records management training to maintain compliance with Reference (c) and this AI.

j. Evaluate their records management program every 2 years to ensure compliance with the guidance in this AI.

8. DoD EMPLOYEES OF WHS-SERVICED COMPONENTS. DoD employees of WHS-serviced Components:

a. Maintain records and information created and received in the course of their day-to-day responsibilities. Ensure that each record set is complete and that enclosures or related papers are retained or accounted for in both paper and electronic filing systems in accordance with the OSD Records Disposition Schedule.

b. Maintain e-mail and attachments documenting work related activities in accordance with the OSD Records Disposition Schedule.

c. Ensure personal files, non-record material, and work-related records and information are maintained separately.

d. Follow the procedures in Enclosure 5 of this AI for the removal of non-record material.

# ENCLOSURE 3

## MANAGEMENT OF RECORDS AND INFORMATION

1. OSD FUNCTIONAL FILES SYSTEM. The OSD records disposition schedules reside on the WHS, ESD website at http://www.dtic.mil/whs/esd/rdd/recordsmgt.html. The OSD Records Disposition Schedule is arranged in a hybrid functional and organizational file system; however, the implementation of the schedule is based on function. This is the only filing system authorized for the WHS-serviced Components; modification of the numbering system is not permitted. This enclosure details how to create and maintain filing systems.

2. RECORDS ARRANGEMENT. To effectively manage records, locate and arrange them to facilitate their use and disposition. Primary considerations include making the files accessible, minimizing duplication, preserving permanent records, and systematically disposing of all others. The factors that must be considered in the storage and maintenance of hardcopy records are:

a. Access. Records will be kept sufficiently accessible to the using activities to make maintenance of duplicate files unnecessary.

b. Security. Classified material maintained in security containers or secured areas must be established in accordance with Reference (j) and personal information maintained with access restricted on a need-to-know basis in accordance with References (h), (k), and (n).

c. Space. Reserve adequate space for present and anticipated needs, factoring in the safety and health of office personnel. Systems selected to manage electronic records must comply with DoD 5015.02-STD (Reference (q)). Consider the retention period of the record when selecting the storage media for electronic records; for permanent records, offices must comply with the requirements in Reference (e). Offices storing large quantities of records must be given fire protection.

d. Arrangement. Position files equipment and supplies to provide control and convenience to the maximum number of users. Locate classified files and containers away from windows and doors to prevent illicit acquisition of or unauthorized access in accordance with sections 641 and 2071 of Title 18, U.S.C. (Reference (r)). Handle files containing privacy information in accordance with Reference (m).

3. FILE PLAN DESIGNATION. Every office within the WHS-serviced Components must have a file plan. Records accumulated and used in performing a function will be located in the organizational element performing the function.

a. The file plan will provide a comprehensive system of identification, maintenance, and disposition of all record information. At a minimum, each file plan must identify the file

number, title and brief file description, disposition instructions, media (paper or electronic), PA System of Records Notice (SORN) number, if applicable, and location(s) of the records (see Figure 1). Additional information, including record examples, classification, or records custodian, may be added as it suits the business needs of the applicable office.

b. File plans will be updated annually or more frequently if necessary. Review and update office file plans as file numbers are added, changed, or deleted or office functions change. If records are moved or locations otherwise change, update the new location information, as well.

c. RLs are to forward one copy of the file plan to the CRMO for review and approval. The CRMO and RLs will maintain a record for all approved file plans. Offices will make copies of the file plan accessible to all employees and contractor personnel.

d. Offices are to review the OSD Records Disposition Schedule periodically but particularly upon major reorganizations or functional changes to ensure that all records are properly identified and the schedule is accurate and complete.

e. WHS-serviced Components may centrally locate specialized files of organization-wide interest and use. The organizations may also establish decentralized records systems in their offices if they are more effective and convenient. See Enclosure 6 of this AI for the management of shared drives.

f. The WHS-serviced Components must establish written procedures explaining where record copies are filed. All locations for a series whether centralized, decentralized, electronic, safes, etc., must be included on the office file plan.

g. Each office is responsible for the custody, maintenance, retirement, and disposition of current records and information systems of the office it serves.

h. Each office will conduct a records evaluation using the SD Form 823, "Division/Branch/Office Standardized Recordkeeping Checklist." Each office will be evaluated at a minimum of every 2 years or when there is reorganization. The SD Form 823 will be maintained with the record copy of the office file plan.

Figure 1. Sample Format for a File Plan

ABC Directorate: Administration Office
Records Liaison or Custodian: Mr. John Doe
Component Records Management Officer: Ms. Jane Jones (signed)

Date Prepared: September 5, 2006
Date Approved: September 22, 2006

| FN | Title/Brief Description | PA Sys No. | Disposition | Media | Location |
|---|---|---|---|---|---|
| 101-01 | Office General Management: Internal office procedures, hours of duty, and individual duties | NA | DEST when 1 yr old | P | File Cabinet A2 |
| 101-02 | Office Inspection and Surveys: Extracts of inspection reports, security inspection reports, safety inspection reports that pertain only to office operations. | NA | DEST after next survey | P | File Cabinet A2 |
| 101-08 | Office Space Assignment: Administrative spaces assigned to an office. | NA | DEST when SS | P | File Cabinet A2 |
| 101-09 | Office Reading and Informational Files: Outgoing Communications and records received for general information purposes requiring no action. | NA | DEST when 3 months old | P | File Cabinet B2 |
| 201-11 | Orientation and Briefing Files: Orientations and briefings given to visitors and newly assigned individuals. | NA | DEST when SS | E | R:\Admin\201-11 |
| 202-03 | Management Survey Files: Individual studies and surveys concerning comprehensive review of organization or particular phase of management. | NA | DEL when 20 years old COFF on Proj completion | E | R:\Admin\202-03 |
| 202-04 | Management Improvement Files: Studies, charts, coordination papers, recommendations, statistical data, etc. | NA | DEL when 4 years old COFF on Proj completion | E | R:\Admin\202-04 |

Sample Format

4. RECORDS CATEGORIES. There are three categories of federal records: Temporary (TEMP), Permanent (PERM), and Unscheduled (see Glossary and Figure 2). The value of records is not necessarily determined by how long they are kept or if the document is an original or a copy. Many temporary documents (personnel and health records for instance) are important although they have no historical value (see Glossary). The evaluation process (also called scheduling) is participative and includes the document creator and recipient, RPDD, and NARA appraisers, as required (see Figure 2).

Figure 2. Record Categories

**Temporary Records**

Records and information that have a set lifecycle based on agency creation, maintenance, and use, as determined and approved by NARA. These records are destroyed at the end of the set lifecycle.

**Permanent Records**

Records and information determined to be sufficiently valuable for historical or other purposes to warrant continued preservation by the Federal Government and approved by NARA. These records are eventually transferred to the custody of the U.S. National Archives.

**PAPER MUST NOT BE DESTROYED WITHOUT NARA APPROVAL OF SCANNED IMAGE**

**Unscheduled Records**

Records and information whose lifecycle has not been determined or authorized by NARA. Unscheduled records, by law, shall be treated as permanent records until NARA approves the schedule for the records in question.

5. BASIC FILE GROUPING. Arrange or group files so that they can effectively document the action, event, decision, or process of the record. Effective documentation ensures a complete account of actions taken, commitments made, and results achieved in the creation of records. Documentation applies to records in all media (paper, electronic, microform, audiovisual, etc.). File arrangement is the relative positioning of information in a file. Effective file arrangement allows for easy retrieval and disposal of records.

a. Subject Files. These are files arranged according to their general content or information on the same topic in one place to make finding them easier. Subject files consist mainly of general correspondence but may also include forms, reports, and other material that relate to programs and functions but not to specific cases (see case or project files). The subject file provides complete documentation in the appropriate subject area. An example of subject files is office administration files that are broken down into policy, instruction, agreement, committee, staff visit, and reference subject categories.

b. Case or Project Files. A case or project file contains material on a specific action, transaction, event, person, project, or other subject. Case files may cover one or several subjects that relate to a particular case. A contract file maintained by an agency contracting office, for example, might contain proposals, bids, addenda, inspection reports, payment authorizations, correspondence, and legal papers. An agency contract monitor, on the other hand, would keep a case file containing copies of interim and final technical reports, memorandums, correspondence, and other documents on a contractor's performance and production of a specified deliverable.

Another example of a case file is the official personnel file. Case filing is the most efficient method for the maintenance of large quantities of records.

(1) The information may cover one or more subjects on a case or project but must always be filed by a specific title or number.

(2) A distinguishing feature of a case or project file is the similarity of the information within the case folders.

(3) Information is arranged within each case file in chronological order with the most recent documentation in front, or by subject, such as statement of work, deliverables, invoices, and modifications.

(4) Case or project files are closed upon occurrence of an event or action and placed in an inactive file. Events or actions that would move a file to an inactive status include the separation of personnel, a final contract payment, or project completion.

(5) Case files may be maintained alphabetically by name, title, country, organization or numerically to permit ease of filing and finding without resorting to special finding aids such as indexes and guide cards maintained separately.

c. Chronological Arrangement. These files are arranged by date when the date is the primary means of reference. This system is useful for keeping records in small, manageable groups; usually by year, month, and day. Reading and suspense files are examples of this type of arrangement. The use of chronological filing arrangements does not necessarily correlate to the disposition for chronological files in the OSD Records Disposition Schedule (File number 102-16). Incorrect use of this arrangement can lead to mixed series filing.

d. Reference Files. Called convenience or working files, reference files may include extra copies of documents that are officially stored elsewhere, such as books, pamphlets, and catalogs. Review these files periodically to retain only those that are current and of significant reference value in accordance with the OSD Records Disposition Schedule.

e. Working Files. In accordance with Reference (e), maintain working files and similar materials as records for purposes of adequate and proper documentation, if:

(1) They were circulated or made available to employees other than the creator for official purposes such as approval, comment, action, recommendation, follow-up, or to communicate with agency staff about agency business.

(2) They contain unique information, such as substantive annotations or comments that add to a proper understanding of the agency's formulation and execution of basic policies, decisions, actions, or responsibilities.

f. Record Status of Copies. The determination of a document as a record does not depend upon whether it contains unique information or an original signature. Copies of the same

document and documents containing duplicative information may each have a record status depending on how they are used by the agency to conduct business.

6. FILING ARRANGEMENTS. The first step in arranging a group of files is to determine the major functional categories that apply. These are listed in the OSD Records Disposition Schedule. RPDD can also assist in making this determination. After selecting the major functions file grouping, select a method of arranging each group (see paragraphs 5a through 5d of this enclosure) based on the primary function by which the file will be requested. Files can be further arranged in one or a combination of the filing arrangements listed in paragraphs 6a through 6e of this enclosure, depending upon the business or reference needs of the office. Records not covered by a PA SORN in accordance with Reference (m) **cannot** be retrieved by a personal identifier (i.e., name, date of birth, or social security number).

a. Numerical Arrangement. Files identified and retrieved by a number, such as a social security number, purchase order, or requisition.

b. Chronological Arrangement. Files identified and retrieved by date.

c. Alphabetical Arrangement. Files identified and retrieved by subject and name.

(1) Name. Files arranged by names of persons, companies, organizations, or agencies.

(2) Geographical. Files arranged by a geographical location such as region, country, state, or county.

(3) Subject. Subject titles are arranged alphabetically.

d. Alpha Numeric Arrangement. Alphanumeric files are identified and retrieved by an alphabetical numeric arrangement, such as contract files.

e. Functional Arrangement. Files identified and retrieved by the function to which the information relates and not necessarily the subject.

7. FUNCTIONAL FILE SYSTEM CONCEPT

a. The functional file system is based on the concept that an office maintains records documenting the performance of each of its functions.

b. The OSD functional file system identifies and arranges records following the principle that identification or coding of records, papers, correspondence, and communications is intertwined with the function they document. The coding and arrangement of files under this system lend themselves to a more flexible arrangement.

c. In selecting a file number, first determine the functional series that represents the subject matter and the specific subdivision. Exercise care in determining their administrative, legal, and research value to DoD; their relationship to the organization; usefulness as archival documents; and the costs of keeping them. See the OSD Records Disposition Schedule and the office file plan for proper file number.

d. Select the proper file designation (see Table 1) by referring to the series and title descriptions listed in the OSD Records Disposition Schedule.

Table 1. Functional Area Numbering System

| File Series | Title |
|---|---|
| 100 | Office Administrative Files |
| 200 | General Administration |
| 300 | OSD Comptroller |
| 400 | OSD General Counsel |
| 500 | OSD Intelligence |
| 600 | ASD Reserve Affairs |
| 700 | OSD Public Affairs |
| 800 | ASD International Security Affairs |
| 900 | ASD Health Affairs |
| 1000 | ASD Legislative Affairs |
| 1100 | DoD Chief Information Officer |
| 1200 | OSD Acquisition, Technology, and Logistics |
| 1300 | ASD Defense, Research, and Engineering |
| 1400 | OSD Cost Assessment and Program Evaluation |
| 1500 | ASD Nuclear, Chemical, and Biological Defense |
| 1600 | Electronic Records and Chief Information Officer |
| 1700 | U.S. Court of Appeals for the Armed Forces |
| 1800 | OSD Personnel and Readiness |
| 1900 | DoD Education Activity |
| 2000 | Director, Operational Test & Evaluation |
| 2100 | ASD Special Operations & Low Intensity Conflict |
| 2200 | ASD Drug Enforcement Policy and Support. |

8. ORGANIZATION OF THE OSD FILE SYSTEM. The organization of the OSD functional file system provides for the division and identification of record information into several distinct subject series to facilitate referencing and disposition.

a. Series 100 Pertains to General Office Administration Files. Information in this series relates primarily to the performance of routine administrative and housekeeping operations of any office.

b. Series 200 and Higher Pertain to the Functional Files. The first subdivision of each of these functional series is devoted to administrative files of the particular functions rather than the general office files in the 100 series. These series relate to specific major functional or functional subgroup areas of OSD. Series file number descriptions and instructions for retention and disposition for all the functional file series are contained in the OSD Records Disposition Schedule.

9. APPLICABILITY. The OSD records disposition schedule system will apply to all records and information, regardless of media. Excluded are copies of publications, blank forms, non-record materials, personal papers, books in formally organized and officially designated libraries, and reproduction material, such as stencils and offset masters; this is considered non-record material (see Enclosure 5 of this AI).

10. FUNCTIONAL AREA NUMBERING SYSTEM. The OSD Records Disposition Schedule is set up functionally and does not necessarily follow an organizational relationship. The major file series with their numerical designations are listed in Table 1.

a. These major series are further divided into categories, as shown in Table 2.

Table 2. Example of Major Categories

| Number | Category |
|---|---|
| 202 | Office Personnel Files |
| 203 | Records Management |
| 204 | Space Management |

b. A dash is employed before designating the file number; a two-digit number, such as 01, is always used to designate a file as shown in Table 3.

Table 3. Examples of File Numbers

| Number | File Title |
|---|---|
| 202-04 | Strength Reports |
| 303-06 | Investment Files |

c. By combining all elements of this numbering system, Table 4 demonstrates their composition:

Table 4. Examples of Tiers Within a Series

| Number | File Breakdown |
|---|---|
| 300 | Comptroller |
| 303 | Principal Deputy Comptroller |
| 303-01 | Comptroller Issues and Action Files |

d. Series and categories are functional breakdowns and not files. Files contain a description of the applicable records and a disposition. Some files identify a specific function, others identify all records relating to a work process, group of related work processes, or a broad program area to which the same length of retention should be applied; the latter are called "buckets."

(1) File numbers in the 100 series are common to all offices in the OSD and are described in detail in the OSD Records Disposition Schedule. Each office designates their specific functional files within this series.

(2) Each office must maintain a file plan of all files kept in an office and make it available to each employee.

(3) Each office will determine the functions they are primarily responsible for and identify the records that correspond to their function from the OSD Records Disposition Schedule. Records within a file number may be further arranged by date (Pay files), number arrangement (Project number), or alphabetical (subject, name, or organization). Records should be arranged to best meet the business needs of the office.

(4) Records arranged by a personal identifier (name of an individual, social security number, birth date) are subject to the PA System of Records in accordance with Reference (m) and must identify the notice number on the label and file plan.

## 11. FILES CONTROL

a. The management of information depends upon establishing continuous and systematic control over the creation, maintenance and use, and disposition of agency records and information in accordance with statutory and regulatory requirements.

b. The establishment and maintenance of proper filing and use of guide cards and filing materials assist in keeping the files orderly and effectively manages 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.

c. File folders must be established and labeled with all the information required to identify the information or papers in the folders, but they do not necessarily have to be in the exact

format shown in Figures 3 through 7 (see Enclosure 6 of this AI for electronic setup). Variations are permitted as temporary measures only, the standards prescribed herein should be adopted as soon as practical. The best time to do that is when new files are created or old ones are remade. Modification of file numbers is not authorized.

d. Effective documentation ensures a complete account of actions taken, commitments made, and results achieved in the creation of records. Documentation applies to records in all media (paper, electronic, microform, audiovisual, etc.) File arrangement is the relative positioning of information in a file. Effective file arrangement allows for easy retrieval and disposition of records.

## 12. FILES CUTOFF PROCEDURES

a. "Files cutoff" is the point when active files no longer needed for current business operations are moved to an inactive status. Generally, this is expressed on the file label as "COFF Dec 31, 2001," followed by transfer or destruction information. Until the file is transferred to an FRC or destroyed, it is held for reference only; no new documents will be added after the cutoff date. Inactive files must be kept separate from active ones to guard against misfiles. Put a new folder into the active files to replace the old one.

b. On an annual or fiscal year basis, whichever is appropriate, all offices will cut off files and separate active from inactive; retire, transfer, or destroy eligible material according to disposition procedures contained in the OSD Records Disposition Schedule, and review and destroy all duplicate or extraneous materials. Cut off:

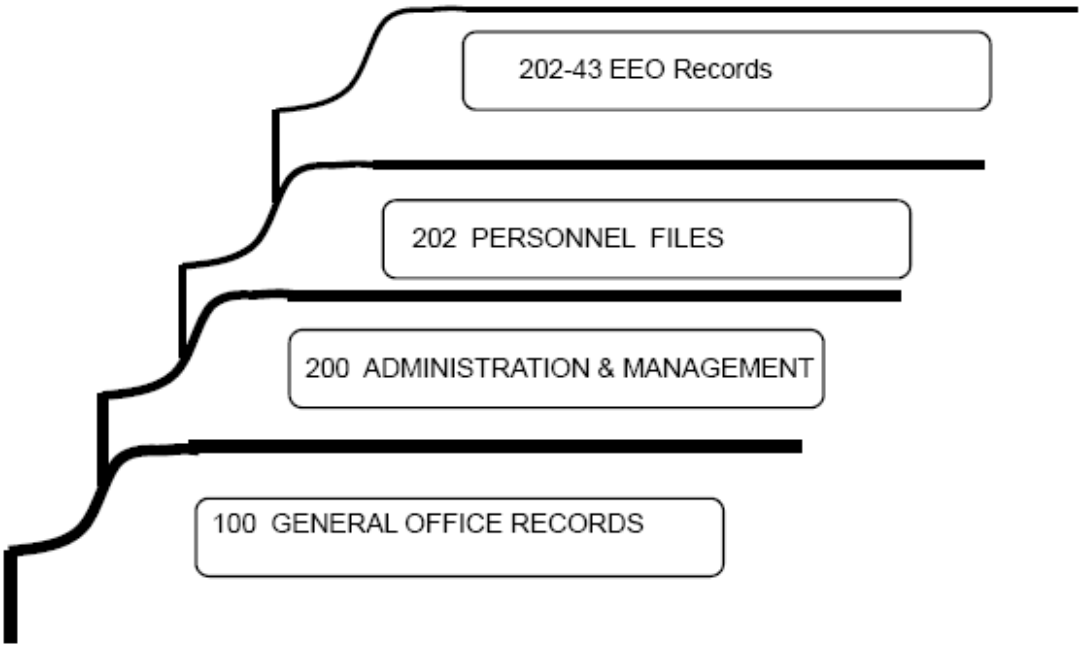
(1) Calendar year files on December 31.

(2) Fiscal year files on September 30.

(3) Files with a retention period of less than 1 year on a monthly or quarterly basis.

(4) Files maintained as case or project files upon the occurrence of a certain event, such as separation of personnel, final contract payment, or project completion. Upon cutoff, move files to an inactive file until they are eligible for destruction or transfer to an FRC, in accordance with disposition procedures in the OSD Records Disposition Schedule.

Figure 3. Examples of Guide Cards and File Drawer Entries




**GUIDE CARD LABELS** – Breakdown of guide cards is authorized if files within one subfunctional category are voluminous, e.g., the 200 category (Administration and Management) is further divided with guide cards for 202, 202-43 etc...

101-01 thru101-20 (05)

Sample label entry for drawer that contains two or more records series. No disposition is shown on the label because it varies among the several record series in the drawer.

(05)
101-09 READING FILES
COFF 31 DEC 05
DEST JAN 09

Sample label entry for drawer that contains one (and only one) record type. Note that drawer label is identical to folder label in this case.

13. PREPARING AND USING GUIDE CARDS, FILE FOLDERS, AND LABELS

a. Guide Cards. Prepare and use guide cards to identify each major file series or to identify and support portions of the series: type standard labels and attach them to the guide card tab; do not retire or discard file guides when files are disposed of; they should be reused (Figure 3).

b. File Folders. Type identifying data on standard labels, positioning them on the folders as outlined in Figure 4. When the material in any one folder reaches normal capacity of

approximately three-fourths of an inch in thickness, prepare another one. Begin the second folder at a logical point, such as the beginning of a month or a calendar quarter. Place folders behind related guides. When there are several folders under one number, a dummy file folder with a label that shows all the required disposition information but is not used to file documents may be used as the first folder in the file series. This saves repeating all the same information on the succeeding folders in that series, which require only the basic series number followed by the file name (see Figure 4).

Figure 4. Samples of Folder Label Entries

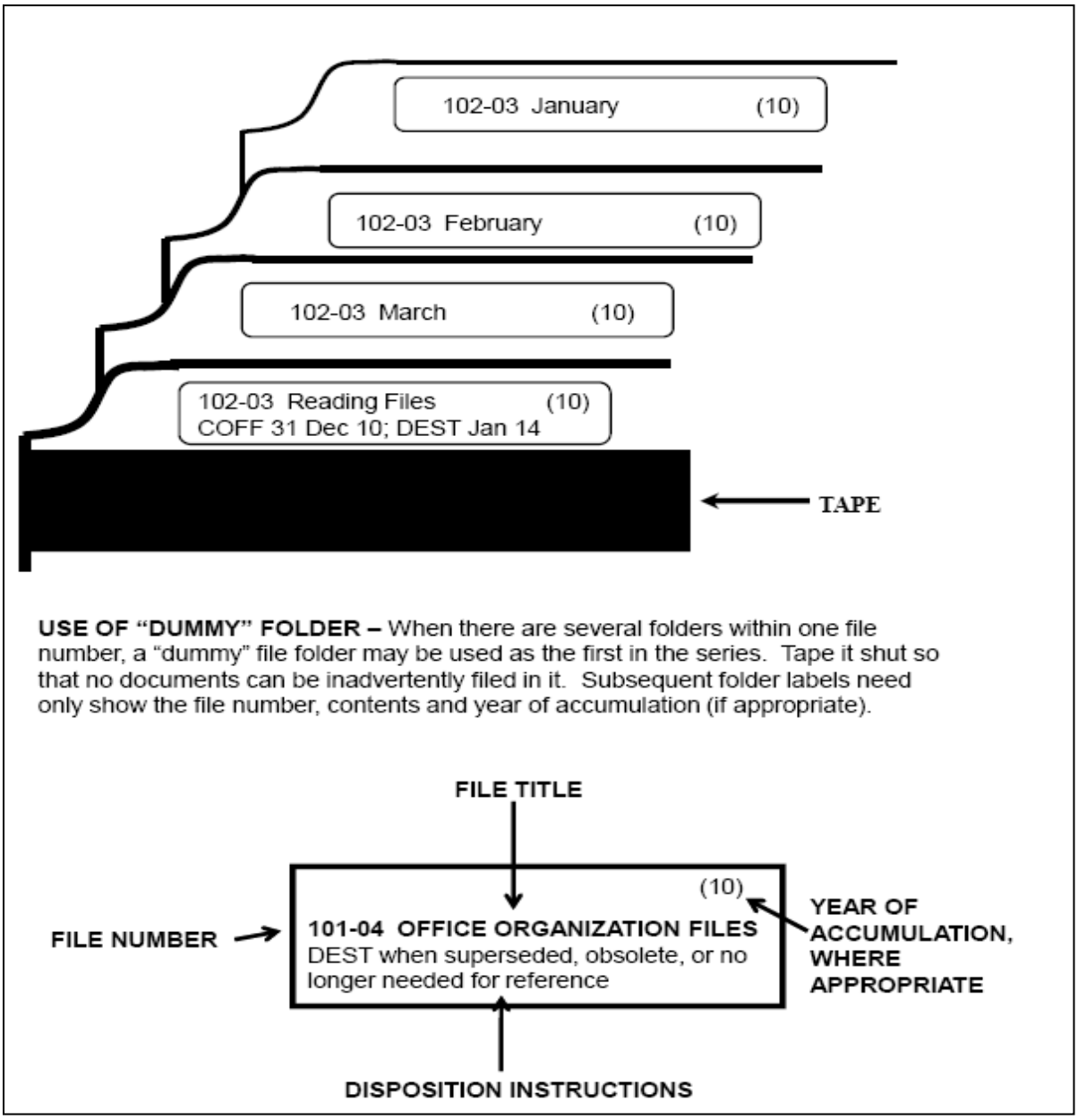
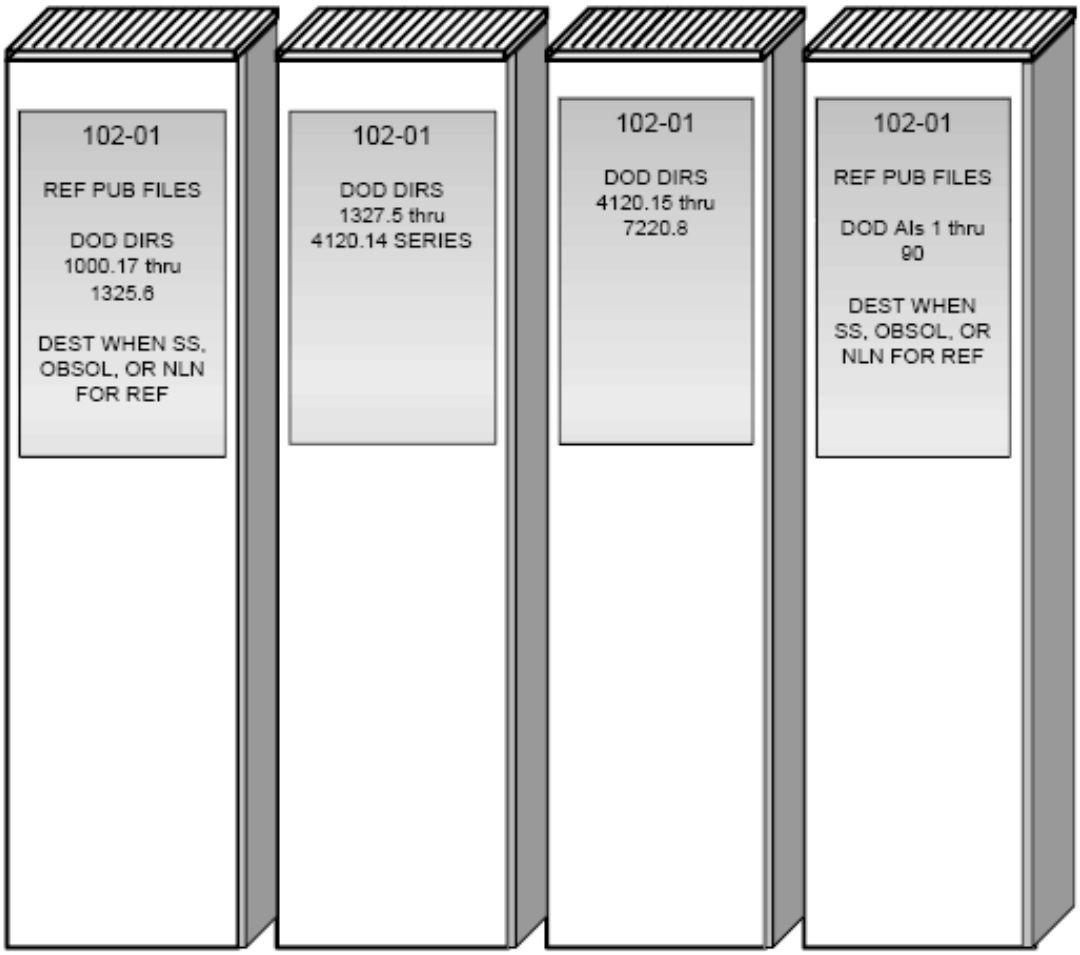


Figure 5. Samples of Label Entries for Binders Containing Reference Publications




c. Labels

(1) Preparation of Labels. Label all file folders, binders, or electronic media with the file number, title, year file created, cutoff date, disposition instructions, and PA SORN number, if applicable (see Figures 4 through 6). A dummy file may be used as stated in paragraph 12b of this enclosure. Subtitles and commonly accepted abbreviations may be used (see paragraph 12d of this enclosure and the DoD Dictionary of Military and Associated Terms (Reference (s))).

(2) Labels for Electronic Media. Type identifying data on standard labels, positioning them on the media (e.g., diskettes, compact disks (CDs), digital video disks (DVDs), external hard drives) as shown in Figure 6. Labels should contain file number, title, date, author or creator, office name, type of record or name of office (if applicable), PA SORN or security classification (if applicable), software version, and file extension. All files should have a standardized naming convention (example: X:\Research Services\Meetings\2005_01_01_04Agenda.doc) and date format (i.e., YYYYDDMM). In addition the following files must be included in ASCII text format in the media.

(a) A readme.txt file which contains the author's name, agency, and specific information on the diskettes, CDs, or DVDs. Example: Information was prepared by John Doe, Agency XYZ. Information herein contains the Audit Reports for the first quarter of 2002.

(b) A directory for CDs, DVDs, and external hard drives only if they contain various types of information. The directory should contain the number of diskettes, CDs, or DVDs (if more than one is required) and type of information contained, for example: Audit reports, background information, and DoD Inspector General or Government Accountability Office responses.

Figure 6. Sample of Label Entries for Electronic Media

d. Label Abbreviations. In addition to commonly used abbreviations, use the abbreviations in Table 5 in preparing labels:

Table 5. Abbreviations for Records Labels

| **Abbreviation** | **Explanation** |
|---|---|
| CFA | Current Files Area |
| COFF | Cut off |
| DEST | Destroy |
| NLN | No longer needed |
| NPRC (CIV) | National Personnel Records Center Annex, (Civilian Personnel Records), 1411 Boulder Boulevard, Valmeyer, IL 62295 |
| NPRC (MIL) | National Personnel Records (Military Personnel Records) 1 Archives Drive, St. Louis, Missouri 63138 |
| OBSOL | Obsolete |
| PERM | Permanent |
| PIF | Place in Inactive File |
| REFP | Reference paper |
| RET | Retire |
| SS | Superseded |
| TRF | Transfer |
| WNRC | Washington National Records Center, Suitland, MD 20746 |

14. CROSS-REFERENCE

a. Cross-references are made to locate documents promptly when needed. A cross-reference is a paper filed under one file series to show the location of material filed elsewhere.

b. Frequently an extra copy can be annotated to show where the original is located and then filed under the cross reference number. When this is not feasible, use a blank sheet, annotated to show the record copy location.

15. LABELING FILE DRAWERS. Label file drawers to facilitate retrieval, and use discretion to prevent revealing the classifications of material stored therein. Only the major file series and inclusive dates of the material will be indicated (see Figure 3).

16. CLASSIFIED INFORMATION

a. Classified files must be safeguarded in accordance with Reference (i) in approved classified containers, systems, or secure areas appropriate with the classification of the material to be protected.

b. The interfiling of unclassified and classified information is restricted to information that directly supports, explains, or documents the record of the action or transaction.

17. MANAGEMENT OF DOCUMENTS AND INFORMATION. Personnel will:

a. Prepare information for filing when all actions are completed, when record information is self-identifying, required by a business process, federal law or regulation, or DoD issuance or an official has requested that documentation be maintained.

b. Ensure that each record set is complete and that enclosures or related papers, to include e-mail, are retained or accounted for in both paper and electronic filing systems.

c. Remove or destroy identical or duplicate copies of information before filing. Ensure that duplicate copies of such records retained for convenience are identified as such and any duplicates or versions of records retained in computers that are no longer needed for reference are deleted in accordance with the OSD Records Disposition Schedule.

d. Remove all mail control forms, transitory e-mail, classified cover sheets, envelopes, and routing slips, except those containing remarks or information of significant record value.

e. Mend or reinforce torn or frayed temporary papers with transparent tape. Do not tape nor attempt to mend permanent documents. (Upon retirement, torn or frayed permanent documents should be supported as best as possible in new file folders. NARA personnel will mend such documents using methods and materials designed to ensure their preservation.)

f. Assemble related documents for filing. See Enclosure 6 for electronic media.

(1) The latest action on top by date or subject.

(2) The completed package or final document.

(3) Enclosures in numerical order.

(4) Supporting papers to include e-mail (return/read receipts), background documents, and substantive drafts.

g. Bring forward documents needed to conduct current business or still pending action; combine documents of a later date that relate or refer to documents of an earlier date only when

reference to them is necessary. A reference to an earlier document does not necessarily require that documents be combined. Do not combine:

(1) Recurring reports with the policy documents requiring such reports.

(2) Applications with the instructions governing their submission.

(3) Documents on the same subject on different transactions, such as reports of inspection of two different organizations.

h. Use a cross-reference sheet for documents brought forward to maintain continuity.

i. File papers loosely in the proper folder according to a filing arrangement that meets the office business needs. Use pronged fasteners when the files are frequently used, when sequence of arrangement is of special importance, and when all documents pertain to the same transaction case or project.

j. Keep folder labels visible by neatly arranging papers in the folders and do not allow the contents of the folder to obscure folder labels. When contents of the folder reach three-fourths of an inch, make a new folder bearing the same file designation and place it in front of the full folder, showing inclusive dates on the folders.

k. Prevent overcrowding files by allowing at least 4 inches of space in each active file drawer to permit sufficient working space.

l. Avoid cluttering the files. File bulky material separately in storage equipment suited to its size. Maintain this material in file classification, date, or serial number order. Make a cross-reference to the bulky material and annotate in a conspicuous location or with the filed papers. Mark the bulky material with storage location and file number to associate it with related information kept in the primary location.

m. Ensure that all action in a file is completed before cutting off the record and applying the disposition instructions.

n. Ensure that all paper and electronic record files are complete, identified, and maintained in accordance with this AI and DoD requirements. Do not separate case files or project files and ensure the origins of the records are preserved. See Enclosure 6 of this AI for more information about managing electronic records.

# ENCLOSURE 4

## DISPOSITION PROCEDURES

1. GENERAL. The OSD Records Management Program is designed to preserve records of continuing value; systematically eliminate all other records; and remove less active records to lower cost storage space. This ensures preservation of permanent records and reduces the cost and effort of recordkeeping. To achieve these objectives, standard procedures have been established for the disposition of all WHS-serviced Component records.

2. DISPOSITION STANDARDS. The OSD Records Administrator will review recommendations for new or revised files disposition procedures or standards and make recommendations for final approval to the NARA. Disposition changes to the OSD Records Disposition Schedule will be submitted by the WHS-serviced Components in accordance with section 14 of this enclosure.

3. SOURCE OF RETENTION PERIODS. Retention periods for categories of OSD files are published in the OSD Records Disposition Schedule. Retention periods cited therein have been established in accordance with records management regulations approved by the Archivist of the United States either upon specific application or through the GRS. Submit recommendations for changes to retention periods and disposition procedures to the OSD Records Administrator for approval. Records that do not have a NARA approved disposition are considered unscheduled records and cannot, by law, be destroyed or deleted in accordance with Reference (e).

4. CHANGES TO RETENTION PERIODS. Retention periods are changed as a result of the continuing evaluation of files and changes in statutory, legal, financial, and administrative requirements. Changes to the retention periods are submitted to the Archivist of the United States for approval using Standard Form (SF) 115, "Request for Records Disposition Authority (available at http://www.gsa.gov/portal/forms/type/SF). The following general rules apply when changing the retention of a record once it has been approved by the Archivist:

a. Increased Retention Period. If the change increases the retention period, the new retention period will be applied to all categories of files concerned, regardless of where they are maintained or when they were created. Those inactive and cut off files affected by the change will be brought under the new retention period.

b. Reduced Retention Period. If the change reduces the retention period, such period will be applied retroactively, unless it is impractical or uneconomical. For example, if the new retention period can be applied to inactive files only by screening files and marking folders on an individual basis, it would normally be more economical to retain the files for the longer period than to attempt to apply the change.

c. Conversion of Paper Records to Electronic or Other Media. Record information previously created and maintained in paper and converted to or created in information systems will have to be re-evaluated to ensure that new records have not resulted due to the nature of the software or media. For example, a system has the capability to create an index or document information not previously captured or created in the paper-based system. Permanent paper records or unscheduled records scanned or microfilmed cannot be destroyed without NARA's approval, in accordance with Reference (e).

5. RECORD FREEZES, PRESERVATION ORDERS, OR MORATORIUMS. The destruction of the affected record information is suspended until the record freeze, preservation order, or moratorium is lifted.

a. The requirement to suspend the retention period is court- or agency-imposed, and all affected record information is retained until all litigation or disputes are resolved.

b. Notification of record freezes, preservation orders, or moratoriums are provided to the OSD Records Administrator from the Department of Justice or the General Counsel of the Department of Defense (GC DoD).

c. These records freezes or moratoriums are usually accompanied by a records search for all applicable information. Records searches must be coordinated with the OSD Records Administrator who will notify the WHS-serviced CRMOs and NARA of the requested search and records freeze, as applicable.

d. Each organization is responsible for notifying its subordinate activities that a freeze exists or has been lifted.

6. UNSCHEDULED (UNIDENTIFIED) RECORDS. Any records which are not identified in the GRS or cannot be filed under any file number in the disposition schedule will be brought to the attention of the OSD Records Administrator for scheduling (SF 115 process). Unscheduled records will be maintained in the current files area (CFA) and treated like permanent records until disposition instructions have been approved by NARA.

7. DISPOSITION INSTRUCTION. The OSD Records Disposition Schedule provides the overall retention period for the files involved (for example, destroy after 2 years, destroy after 10 years, or retire 3 years after cut off). The disposal period begins at the date the file is cut off or closed, unless otherwise indicated. Examples of specific instructions containing exceptions to the general time periods and events are: "destroy when registrant becomes 36 years of age," "withdraw and destroy on departure of the individual," "destroy when superseded," "destroy after next survey." Figure 7 provides examples of how disposition instructions are to read on file labels maintained on a calendar basis. Normal periods of retention are:

a. Files with 1-Month Retention. Files having a retention period of 1 month or 30 days will be cut off at the end of the month, held 1 month in the CFA, and then destroyed.

b. Files with 3-Month Retention. Files having a retention period of 3 months or 90 days will be cut off at the end of each quarter, held 3 months in the CFA, and then destroyed.

c. Files with 1-Year Retention. Files having a retention period of 1 year will be cut off at the end of the calendar or fiscal year, held in the CFA, and then destroyed.

d. Files with 2- to 10-Year Retention. Files having a retention period of 2 to 10 years will be cut off at the end of the calendar or fiscal year, held 1 year after cut off in the CFA, and destroyed or retired as provided by the schedules in the OSD Records Disposition Schedule.

e. Files with a Flexible Retention. Files having a flexible retention period such as delete, destroy, or transfer when 5 to 7 years old, will be cut off at the end of the calendar or fiscal year; retained for at least 5 years but no longer than 7 years; and destroyed or transferred as provided by the OSD Records Disposition Schedule. The amount of time the record is retained is determined by the business needs of the office. Document business needs in a regulation, issuance, or standard operating procedure to ensure consistency in the retention of the record.

f. Files with Event Retention. Files having an event disposition such as cut off when superseded, obsolete, or property is turned in, will be maintained in the active files until the event occurs; transferred to inactive files and cut off at the end of the calendar or fiscal year; held for a time period specified after the event; and destroyed or retired as provided by the OSD Records Disposition Schedule.

g. Unscheduled Files. Files having no approved NARA retention period will be cut off at the end of the calendar or fiscal year and maintained in the CFA until disposition instructions are published in the OSD Records Disposition Schedule.

Figure 7. Disposition Instructions

Files with 1-Month Retention
COFF April 30, 2002, DEST June 2002.

Files with 3-Month Retention
COFF June 30, 2002, DEST Oct 2002.

Files with 1-Year Retention

| | |
|---|---|
| Calendar year file: | COFF Dec 31, 2002, DEST Jan 2004 |
| Fiscal year file: | COFF Sept 30, 2002, DEST Oct 2003 |

Files of 2- to 10-Year Retention.

| | |
|---|---|
| Calendar year file: | COFF Dec 31, 2002, RET to MPRC Jan 2004, DEST Jan 2010 |
| Fiscal year file: | COFF Sept 30, 2002, RET to WNRC Oct 2003, DEST Oct 2009 |

Files with Event Retention

| | |
|---|---|
| Disposition: | Destroy/Delete 15 years after next GAO Audit |
| Active file: | COFF upon next GAO Audit |
| Inactive file: | COFF 31 Dec 05, DEST Jan 2016 |

Files that Are Unscheduled.

COFF June 30, 2002, retain in CFA until disposition instructions are approved.

8. DISPOSITION PROCEDURES. WHS-serviced Components will:

a. Retire records designated for annual retirement on a calendar or fiscal year basis to the appropriate FRC.

b. Withdraw from the active file and destroy or delete documents that are disposable upon an event or action.

c. Terminate files that are disposable after a specific retention period following an event or an action, such as audit, final payment, or completion of a project, on the occurrence of the event or accomplishment of the action. Terminate such files by withdrawing them from the active file and placing them in an inactive file, or in the case of large volumes, simply by discontinuing further filing within the files. Cut off inactive or terminated files and effect disposition in the same manner as for other files with the same retention period.

d. Unless otherwise specified in the disposition instructions, cut off permanent files at the end of the calendar or fiscal year. Start new folders for the new year and place the old folder in the inactive files.

e. Include the CRMO or RPDD in the development of potential information systems or enhancement of current systems to evaluate the system for its record creating potential and determine records management requirements.

9. TRANSFER OF FILES. The transfer of the files from one organization to another is permitted only when a transfer of functions from one WHS-serviced Component to another requires it. The order directing the transfer of functions must provide for the transfer of files. The transferring organization will use the records transmittal procedures outlined in Enclosure 7 of this AI to properly document the files transfer.

10. TRANSFER TO OTHER GOVERNMENT AGENCIES

a. Transfer to NARA FRCs. WHS-serviced Components will transfer all permanent files to the FRC at periodic intervals so that they may be incorporated into the permanent archives of the U.S. Government. RPDD arranges for the transfer of the files and the establishment of procedures for their use. This is accomplished using SF 258, "Agreement to Transfer Records to the National Archives," available at: http://www.gsa.gov/portal/forms/type/SF. Offices will provide the unsigned form with a completed box list to RPDD for submission to NARA's Electronic Records Archive.

b. Transfer to Other Agencies. NARA regulations prohibit the transfer of files from one government agency to another without prior approval of the Archivist of the United States, except when:

(1) Records are transferred to a NARA FRC.

(2) The transfer of records or functions or both is required by statute, Executive order, Presidential reorganization plan, specific instructions in the OSD Records Disposition Schedule, or by a specific ruling or agreement.

(3) Authority to transfer OSD records to another government agency has been obtained from the OSD Records Administrator. Recommendations for transfer submitted to the OSD Records Administrator will include a concise description of the files to be transferred, an estimate of the volume in linear feet, name and location of the agency to which the files are to be transferred, and the reasons for the transfer.

## 11. NATO DOCUMENTS

a. Control Instructions. Reference (p) contains control instructions for NATO documents and refers to applicable disposal authorities. NATO documents classified Secret and below may be maintained with other OSD records when they form an integral part of a file of classified records of permanent value.

b. Control and Disposal Procedures

(1) Classified document receipts, destruction certificates, and registers relating to NATO, Top Secret, and Secret documents that reflect the final disposition of documents in a sub-registry will be disposed of in accordance with Reference (p).

(2) Document receipts, destruction certificates, and other control files relating to NATO or documents having a lower security classification than Secret will be disposed of in accordance with the OSD Records Disposition Schedule.

## 12. DISPOSITION OF FILES AND CHANGES OF STATUS

a. Transfer of Functions. When a function is transferred from one DoD Component (as defined in the Glossary) or OSD organization to another, the records in the CFA relating to the transferred function will be transferred to the gaining organization where they are maintained as a separate entity to preserve their administrative origin. The transfer of records can be completed by use of the SF 135, "Records and Transmittal Receipt," available at: http://www.gsa.gov/portal/forms/type/SF. Eligible inactive files can be retired to the FRC. A list of the files transferred to the gaining organization and a copy of the SF 135 listing inactive files retired to the FRC will be given to the CRMO of the gaining organization and a copy must be provided to the OSD Records Administrator.

b. Re-designation or Reorganization. On re-designation without transfer of function, files will be maintained in accordance with the appropriate disposition schedules as though no change had occurred.

c. Discontinuance of a WHS-serviced Component or an Organization. On discontinuance without transfer of functions, files not authorized for immediate disposal will be retired to the designated FRC via RPDD. These procedures are applicable to any specially organized element such as a board, committee, council, or commission.

d. Damage, Alienation, and Unauthorized Destruction of Records. Each WHS-serviced Component is responsible for preventing the loss of federal records.

(1) Records destroyed or damaged due to accidental loss or destruction, such as fire or water, are to be reconstructed by the office of record. Records can be reconstructed from information retained in other file series, non-record materials, or computers. Include documentation concerning the reconstruction and cross-referencing materials to aid in the identification of the record. Annotate an SF 135 with any information that cannot be reconstructed, to include with the rest of the files series, upon retirement. Notify RPDD of any accidental loss or destruction of records.

(2) Federal records may not be removed from the legal or physical custody of OSD or destroyed without regard to the provisions listed in this AI.

(3) The willful and unlawful destruction, damage, or alienation of federal records can result in a monetary fine, imprisonment, or both, pursuant to References (e) and (r).

## 13. RECORD SEARCHES AND PRESERVATION ORDERS

a. Record searches and orders to preserve records must be coordinated with the OSD Records Administrator (see section 5 of this enclosure), except for searches in response to requests under the PA and section 552 of Reference (h) (also known and referred to in this AI as "The Freedom of Information Act (FOIA)").

(1) Coordination of search and preservation taskings is essential before issuing document search, retrieval, or collection instructions. Vague directions and lack of coordination can lead to loss of data or documents subject to a preservation order.

(2) Preservation orders are not limited to information that constitutes the legal definition of a record, but may include drafts, working papers, and non-record materials, regardless of media, as well as electronic data in the organization's possession or control.

(3) Each WHS-serviced Component is responsible for conducting the search and implementing the preservation order as directed. Offices are responsible for preventing the loss of responsive information required for litigation, investigation, audit, or subpoena.

b. Any decision to direct a search and preservation of paper or electronic documents and data is a team effort involving the GC, DoD, records management officials, supporting information systems professionals and, in some cases, record custodians.

(1) Some searches will require extensive coordination and planning; others can be tasked out with a less formal coordination process. Potentially, end-user representatives or other individuals with knowledge of the relevant computer systems, such as information security personnel, may need to plan the response.

(2) The tasking authority should identify a lead office or individual to act as the organization's spokesperson or witness on issues relating to the scope of electronic and paper document production. Documents and data collected in response to a search must be reviewed for matters of privilege, classified information security, or other control requirements before release.

c. The preservation planning team responding to notices of records holds or searches for litigation should:

(1) Identify the WHS-serviced Components, agencies, offices, and officials whose files (paper or electronic) are most likely to contain relevant documents and information.

(2) Identify a lead office to consolidate the listing documents and data (and assemble the initial collection if required).

(3) Identify contacts in the GC, DoD and OSD Records Administrator who can address questions regarding preservation duties.

(4) Identify an appropriate IT liaison who works with records officials and legal counsel to identify any systems, files, or data that may be subject to the preservation obligation.

(5) Propose specific key words and metadata descriptors needed for a minimally sufficient search.

(6) Issue an internal records search and preservation memorandum to responsible officials (both organization heads and accountable records custodians) and task them to suspend routine disposition on relevant records, retain information (including electronic communications, data and non-record materials) that may be relevant to the litigation or query and, if required, collect and review records responsive to the request. The memorandum must describe the type of information to be preserved so the custodians can segregate and preserve identified files and data. It should also provide clear direction to the custodians about what to do with any records collected, i.e., if they should be delivered.

(7) Determine a suspense based on any external deadline, complexity of the search, and the amount of time required to complete the search and review.

14. <u>REQUESTING MODIFICATIONS TO THE OSD RECORDS DISPOSITION SCHEDULE</u>. To ensure the OSD Records Disposition Schedule meets the business needs of the WHS-serviced Component, the CRMOs will:

a. Recommend the modification of disposition procedures or schedules to the OSD Records Administrator, explaining in detail why they should be changed.

b. Follow the format and writing style used in the descriptions and disposition instructions of the OSD Records Disposition Schedule in presenting recommendations relating to unidentified files. Since the proposed standards may have WHS-serviced Components-wide or DoD-wide application, retention period for other offices that may be creating similar records will be considered.

c. Recommend to the RPDD the establishment of disposition standards for files for which no instructions are provided. Include the following information:

(1) Recommended series and file title.

(2) A complete description of the file, including types of record information included therein.

(3) Explain what the series documents: who, where, when, why, and how the record describes OSD operations or what OSD does or produces.

(4) Explain who creates the information used in the series, who receives the information, and who uses it.

(5) Explain what information is recorded in the series.

(6) Explain if the series is subject to legal, fiscal, or other requirements.

(7) Identify the retention period required to satisfy current business needs, such as:

(a) Retain in the office for 1, 2, or 3 years and destroy.

(b) Retain as above and retire to an FRC for 1, 2, 3, 5, or 7 years.

(c) Retain for the years specified above and then transfer to NARA for permanent retention.

(8) Explain the following:

(a) Physical form: paper, microform, electronic format (database, pdf, etc.).

(b) Arrangement: numerical, chronological, geographical, organizational, alphabetical, subject, functional.

(c) Volume to date in cubic feet, number of CD-ROMs, as applicable.

(d) Dates the files cover.

(e) Annual expected accumulation, in cubic feet or bytes.

(f) Location of the records.

d. Evaluate potential and existing information systems and websites to determine if record information is being created and notify the OSD Records Administrator to validate retention periods identified in the OSD Records Disposition Schedule. New, revised, or obsolete record information may require revision of the disposition schedule. This process will require the interaction of records management, information technology, and legal staffs.

e. Notify the OSD Records Administrator of any unauthorized destruction or damage of official records.

# ENCLOSURE 5

## DISPOSITION OF PERSONAL FILES AND NON-RECORD MATERIALS

1. RECORD AND NON-RECORD MATERIALS OF GOVERNMENT OFFICIALS. During their tenure in office, many government officials, employees, and Presidentially appointed, Senate confirmed (PAS) officials accumulate substantial collections of personal files and copies of official documents (includes electronic files and e-mail) created solely for convenience of reference (non-record material).

a. These non-record materials originated, reviewed, signed, or received during the PAS official's tenure can provide a historically valuable supplement to the official files.

b. When an official or employee departs, non-record materials are to be reviewed by the employee, the CRMO and, for a PAS official, the OSD Records Administrator, prior to their removal from DoD custody.

c. To prevent violations of References (d) and (e), officials, DoD employees (civilian and military), and contractors in the WHS-serviced Components must be able to distinguish between federal records, non-records, and personal files.

2. DISTINGUISHING PERSONAL FILES AND NON-RECORD MATERIAL. There is a difference between personal files and non-record materials. The distinction is sometimes unclear, especially when non-record materials become part of a collection referred to as an official's "personal files." Regardless of the status of non-record material, employees or officials are not entitled to remove as personal files collections of DoD e-mail or unclassified information in their possession while they were employed that is not cleared for public release.

3. PERSONAL FILES. Personal files are not subject to Reference (d) and the OSD Records Disposition Schedule, which pertain to the maintenance and disposal of federal records.

a. Personal files can be any information or documentary materials that are unrelated to the conduct of agency business and concern only to an individual's personal affairs (e.g., files relating to political activities, personal and family matters, or social or civic activities) or indirectly related to agency business but outside the scope of the definition of federal records (i.e., not used to conduct government business.) Personal files are excluded from the definition of federal records and are not owned by the government.

b. Examples of personal files are:

(1) Business or professional files accumulated by an official before joining government service that are not used subsequently in the transaction of any government business.

(2) Materials relating solely to an individual's private affairs, such as outside business pursuits, professional affiliations, personal social events, volunteer or community service records, or private political associations that do not relate to agency business.

(3) Diaries, journals, personal correspondence, personal calendars and appointment schedules, or other personal notes that are not prepared or used for or circulated or communicated in the course of transacting government business. This is the most difficult to distinguish from federal records because of its work-related content.

c. Paragraphs 3c(1) through 3c(4) of this enclosure pertain to the maintenance, marking, and handling of personal files:

(1) Personal files will be established by the employee at the start of their tenure, clearly designated as such and must, at all times, be maintained separately from the office's official records.

(2) If information about private matters and agency business appears in the same document, it will be copied or extracted at the time of receipt, with the personal information deleted, and incorporated into the office's official records.

(3) Materials labeled "personal," "confidential," or "private," or similarly designated, and used in the transaction of public business are federal records subject to the provisions of pertinent laws and regulations. The use of such a label is not sufficient to determine the status of documentary materials in a federal office. DoD email accounts are not considered personal files.

(4) Files that are strictly personal may be removed at the discretion of their creators, unless they contain classified information.

4. NON-RECORD MATERIALS. Non-record materials are government-owned documentary materials that do not meet the conditions of records status or are specifically excluded from the statutory definition of a federal record.

a. Non-record materials are extra copies of federal records accumulated for the **sole purpose** of ease of reference. Copies of official documents, to include e-mail, will not be made **solely** for the purpose of removal or donation (at the end of an official's or the employee's tenure); doing so may be a violation of References (d) and (e). Memorandums that contain an original ink signature or documentation that contain substantive annotations (see paragraph 4c(4) of this enclosure) are federal records. Record sets of publications, posters, and maps that serve as evidence of agency activities and have value for the information they contain are also preserved as federal records.

b. Non-record material existing in offices must be managed.

(1) Non-record materials will be:

(a) Physically segregated from records. Electronic non-record materials must be readily identifiable as such.

(b) Purged or destroyed in accordance with the OSD Records Disposition Schedule, if identified, or when no longer needed for reference.

(2) If a clear determination cannot be made on the status of the document or information, the materials should be treated as federal records. WHS-serviced Components should consult with RPDD for guidance.

c. Non-record materials may be removed from government control, in limited circumstances, provided the following conditions are met:

(1) Unclassified. Departing officials and employees only may remove extra copies of record materials as defined in paragraph 4a of this enclosure, if the conditions of paragraph 4d and section 5 of this enclosure are met.

(a) Removal of non-record materials must be coordinated with the WHS Serviced Component's CRMO and Security Manager.

(b) Removal of non-record materials by PAS officials will be coordinated with GC, DoD and approved by the OSD Records Administrator.

(c) Only Cabinet level officials may donate unclassified non-record material to a Presidential Library of the NARA, Library of Congress, or to some private institution (college, library, historical society, etc.).

(2) Classified. Information classified under the provisions of Reference (l) is not personal property and will not be removed from the government's control (see Glossary), except for the removal of custody taken in accordance with the requirements of the National Industrial Security Program established under Executive Order 12829 (Reference (t)) or a successor order. PAS officials may include declassified non-record materials for the purposes of historical retention to a government repository such as a Presidential Library. Declassified non-record materials may be removed after coordination and approval as described in paragraph 4c(1) and section 5 of this enclosure.

(3) PA, FOIA, and Other Statutes and DoD Regulations. Information restricted from release under the PA, FOIA, other statutes, or DoD issuances or policy will not be removed from government custody, except as permitted under those statutes and issuances.

(4) Working Files. Preliminary drafts and rough notes and other similar working files are classified as federal records when they are circulated for official purposes such as approval, comment, action, recommendation and when they contain unique information, such as substantive annotations or comments that add to a proper understanding of the agency's decision-making process or how its mission is accomplished; they may not be removed from government custody.

(5) E-mail. The removal of the non-record copy of e-mail will not affect the government's ability to invoke certain legal privileges under FOIA and PA. E-mail is provided to conduct government business and the first priority is to ensure that official record e-mail is accessible to the organization upon departure of the PAS official or employee.

d. Unclassified does **not** equal public use. Unclassified non-record materials requested for removal by a departing official or employee for the purpose of personal use must be cleared for public release prior to removal. Clearance for public use is recommended for non-record materials selected for donation, but instructions can be written in the deed of gift. Classified non-record materials cannot be removed or donated pursuant to References (e) and (l).

e. Any transfer of non-record copies of official documents to any government or private institution must be effected 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: potential violations of personal privacy; protection of national security information; statements made by or to the donor in confidence; materials or information that might prove prejudicial to the conduct of the foreign relations of the United States; and 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.

f. It is the responsibility of the donor and his or her immediate staff to ensure donated materials are screened to contain no official agency record copies or other material that cannot be removed from the government's control. The donor is responsible for compliance with all security regulations governing classified information and ensuring that such information is removed and maintained by the office of record, until it is eligible for destruction in accordance with the OSD Records Disposition Schedule

g. Non-record copies provided to departing employees to utilize in another DoD Component or government agency is to be considered a personal use release and therefore a public release unless the recipient DoD Component or agency accepts them as its record or non-record information under its control. See paragraph 12a of Enclosure 4 of this AI for interagency transfer guidance. Employees may not remove official files when they are reassigned or moved to another DoD Component.

## 5. INSTRUCTIONS FOR REMOVAL OF PERSONAL FILES

a. The WHS-serviced Components should ensure departing employees:

(1) Pack personal files in boxes or containers clearly marked as personal.

(2) Delete all personal files on the personal computer (PC) used (e-mail, spreadsheets, documents, etc.). E-mail and other electronic information that are of record status as stated in the OSD Records Disposition Schedule are to be captured as described in paragraph 5a(3) of this enclosure.

(3) Account for all program records created, received, and maintained during their employment, to include e-mail, record information on collaborative websites or social media networks, and all record information from their office PC or laptop by printing and filing, sending to a records management application (RMA), or moving to a designated area on the network. If the employee occasionally worked from home, the residential PC should also be considered for review.

(4) Provide access to program records by providing password and location of the records on the network.

(5) Provide a list of any convenience copies of records they wish to remove to the immediate supervisor, the CRMO, and the Security Manager for their review and approval. Removal of complete collections of DoD e-mail is not authorized. This list must be attached to the applicable forms in paragraph 5b of this enclosure.

b. Completion of the SD Form 821, "Component Records Management Checklist for Processing the Departure of Presidential Appointees or Senior Officials," or SD Form 822, "Departing Employee Checklist," is required to document the removal of non-record materials. CRMOs and RLs will retain the forms for the same amount of time as the applicable record information in the OSD Records Disposition Schedule or when the collection is transferred from the donor to the recipient institution. Approval for removal of non-record material may be considered if:

(1) It does not diminish the records of the DoD.

(2) It does not violate confidentiality required by national security, privacy, or other restrictions on disclosure.

(3) It does not exceed normal administrative resources of the DoD.

(4) It does not affect the DoD's ability to invoke legal privileges.

c. The OSD Records Administrator or the GC, DoD may provide additional guidance to the WHS-serviced Components, as needed.

6. <u>ACCESS TO DONATED PERSONAL FILES, NON-RECORD MATERIALS, AND FEDERAL RECORDS</u>. 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. The instrument of gift will be developed in accordance with References (h), (l), (m), and AI 50 (Reference (u)). Access to federal records by former officials which they originated, reviewed, signed, or received while serving as Presidential appointees can be granted in accordance with Reference (u).

7. REMOVAL SUBJECT TO A NON-DISCLOSURE AGREEMENT. Only Cabinet level officials may remove copies of unclassified information or materials not previously released to the public or with clearly identified restrictions.

a. The departing official must sign a non-disclosure agreement.

b. The former official must agree not to release or publish the information orally or in writing (paper or electronically) without the written approval of the DoD.

c. Upon request by the Cabinet-level official, the DoD will perform a public release review of the information. The review may result in possible denial or redaction of the information.

d. The DA&M serves as the appellate authority to any denials or redactions that may be contested.

# ENCLOSURE 6

# ELECTRONIC RECORDS

## 1. GENERAL

a. It is the responsibility of each WHS-serviced Component head and all of the organization's military, civilian, and contractor personnel to preserve electronic records. Personnel must ensure electronic records are maintained, protected, and stored in accordance with this AI and the OSD Records Disposition Schedule.

b. Electronic information meets the definition of a federal record when it is information made or received in connection with the transaction of public business and preserved or appropriate for preservation by an agency as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of data in them.

c. Electronic records are governed by the same records disposition principles as all federal records and should be identified as early as possible in their life cycles to ensure preservation.

(1) Electronic records may be created via e-mail, software programs (such as Excel or Adobe), websites and social networks or they may be converted from hard copy (via scanning) into electronic format.

(2) These records may also reside in databases or electronic information systems (EIS).

(3) In the case of EISs, the program office responsible for the system or database must incorporate records management requirements as defined in Reference (e) into the system design regardless of the classification of the data in accordance with Office of Management and Budget Circular A-130 (Reference (v)).

## 2. CATEGORIES OF ELECTRONIC RECORDS

a. Databases. Databases contain structured data which is centrally managed within the application. OSD Components must pay particular attention to databases that contain significant statistical data or information related to policy-making functions, as these may have long-term or permanent value. Databases must be evaluated for their administrative, legal, fiscal, and historical value. Information that may have to be scheduled includes: input/source records, system documentation (codebooks, record layouts, etc.), system outputs, and masterfile.

b. Information Systems. Records generated and created or used by data input personnel, computer operators, programmers, analysts, and systems administrators. They may include files required to manage system housekeeping, performance tuning, system usage, login and password control, system and audit trail files.

c. EIS. Records generated in systems created to perform mission related functions (payroll, finance, personnel, acquisition, etc.) and used by office or organizational personnel, computer operators, programmers, and systems administrators.

(1) These systems are usually identified by a specific name or acronym and contain structured data.

(2) Information produced by these systems will have to be evaluated for its legal, administrative, and fiscal values.

(3) The same information that may be scheduled for databases applies to EISs. In addition, inputs received from other systems or information transmitted to other systems must be identified and considered as part of the scheduling appraisal process.

d. Electronic Office Records. Records can be created electronically (electronic files) or they may be converted to electronic files (scanned records).

(1) Electronic files are created using office software, such as word processing, desktop publishing, spreadsheet and database files; e-mail; electronic calendars; appointment, telephone, trip and visit logs; finding or tracking aids, and other electronic helpers employed to enhance the effectiveness of the system. Some electronic files contain unstructured data and usually require a document management system or RMA to manage them effectively throughout their life cycle.

(2) Electronic files used strictly as backup for paper record copies or containing only transitory information as defined in Reference (e) that do not document the activities of an organization, are considered transitory records. Use the applicable file number in the 100 series in the OSD Records Disposition Schedule for the disposition of transitory electronic records. The electronic file may be erased when the hardcopy has been generated or when the data is no longer needed. However, users may elect not to erase certain electronic files, particularly if they are reusable for later revision of manuals, directives, recurring memorandums, and spreadsheet models as reference or working copies.

(3) Scanned or digital records are images, printed text, handwriting, or an object converted to a digital image by a scanning device. When converting official paper records to scanned images, offices must consider the disposition of the record in the OSD Records Disposition Schedule. Hard copy records with a disposition of permanent or that are unscheduled will not be destroyed once converted to a digital image without the approval of NARA. Scanned images of permanent records must meet the requirements in Reference (e). Prior to converting official hard copy documents (temporary or permanent), the program office will alert the CRMO and RPDD of the proposed conversion.

e. Websites. Websites containing record information must be maintained in accordance with the OSD Records Disposition Schedule. If websites are not identified in the schedule, then they must be scheduled; see paragraph 12a of this enclosure.

f. Web 2.0 (Commonly Referred to as Social Networking Sites (SNSs)). Web 2.0 technologies are commonly associated with web applications that facilitate interactive information sharing, interoperability, user-centered design, and collaboration on the World Wide Web. Examples include wikis, blogs, and SNSs like Facebook, MySpace, Twitter, and LinkedIn. These sites should be appraised to determine what records exist and what series in the OSD Records Disposition Schedule apply.

g. Cloud Computing. Cloud computing solutions enable the on-demand use of shared resources, software, and information via computers and other devices. Records stored in the cloud still belong to WHS-serviced Component and must be managed in compliance with this AI and the OSD Records Disposition Schedule.

3. ELECTRONIC RECORDS MANAGEMENT

a. The management of electronic records is similar to the management of paper records: Official records maintained in electronic formats (digital photographs, scanned images, databases, EISs, websites, etc.) must be maintained per the applicable file number in the OSD Records Disposition Schedule.

(1) If a file description does not match the content of the records, these records are considered unscheduled and the organization must submit an SF-115 to RPDD (see section 14 of Enclosure 4 of this AI for guidance on modifying the OSD Records Disposition Schedule).

(2) Store files needed often for the conduct of business conveniently for organizational access.

(3) Delete files not requiring long-term retention or not needed to document the business of an organization, such as draft documents, from the storage media in accordance with the OSD Records Disposition Schedule.

(4) Maintain classified information in accordance with References (l) and (t) and the OSD Records Disposition Schedule.

(5) Protect personally identifiable information (PII) under Reference (h) in accordance with Reference (m).

b. An office that relies only on electronic versions of its files for any of its official records must have them reviewed by RPDD for potential reappraisal by NARA. Some WHS-serviced Components may have a hybrid system; e.g., both paper and electronic versions of their official records. Offices purchasing new systems or upgrading old ones must ensure that records disposition instructions for the data are incorporated into the system's design in accordance with References (e) and (o). Offices must have NARA approval before destroying existing permanent hard copy records in accordance with part 1225 of Reference (e).

c. Shared environments do not provide the functionality of a recordkeeping system. However, through a combination of manual and automated policies and procedures a shared drive can be a recordkeeping system.

(1) Managing records in shared drives requires intervention which can be successfully met when the basic guidelines in paragraphs 3c(1) through 3c(5) of this enclosure are followed.

(2) If your agency or organization implements any type of Enterprise Content Management system or RMA, the office staff must consider the record value of the information created and received, its classification, and actively manage the records.

(3) Organized information can be easily retrieved; record copies can be easily identified and managed by the organization. Each office should implement a structure based on the business process. Basic guidelines for the management of records stored on shared environments include:

(a) Establish points of contact responsible for shared drive management.

(b) Survey or inventory shared drives to determine the status of the shared environment (unclassified, classified, PII, and personal) and identify the records to be managed. Issues to address are: naming conventions, version control, unprotected folders containing PII, access control, and the interfiling of personal, non-record, and official records.

(c) Identify records to be managed by consulting the file plan, organizational and functional guides, and staff knowledgeable about the organization and business process.

(d) Determine a structure of the shared environment that will be flexible for all users and protect PII related records.

(e) Establish a standardized file structure that is aligned with the office's business processes. Structure folder and subfolders will be associated with the corresponding records schedules, including cutoff and disposal instructions.

1. Flat File Structure. Files maintained on shared drives in a manner that closely replicates the office file plan. This is an example of shared drive organization. In this arrangement, the first folder level is named after the office; the second folder level contains the file number, subject, and retention. The third level has the calendar year (CY) or fiscal year (FY) and destruction date. The latter two levels can be reversed or combined. See Figure 8.

2. Subject Matter File Structure. A file structure where the first folder level is named after the organization, but the second folder starts with its subject and contains the file series in parentheses. Subfolders are arranged by year and contain the disposition instructions. See Figure 9.

3. Consolidated File Structure. A structured format that displays all offices within the organization on the shared drive, utilizing either the flat file or subject matter file structure. See Figure 10.

4. The Hierarchical File Structure. A structured format that replicates the organizational or command structure. This is an example of shared drive organization. In this structure each office within the organization establishes file folders based on their hierarchy within the starting principal (front) office, then each subordinate office. Each subordinate office establishes a file structure based on the office file plan and year of creation (CY or FY). See Figure 11.

d. Establish a standardized naming convention based on how the information is filed and retrieved (i.e., subject and date), taking into consideration version control.

(1) Files retrieved by date: 20100102_Records Management

(2) Files retrieved by subject: Records Management_01012010

(3) Files retrieved by subject with version control: Records Management_DraftV1_01012010

(4) Files retrieved by date with version control: 20100102_Records Management_FINAL

e. Restrict access rights to files containing PII (social security number, home address, medical information, etc.) to personnel who have a need-to-know determined by an appropriate local authority.

f. Use the document properties option to add metadata tags, including at a minimum the office of origin, file code, key words for retrieval, author, date, and security classification (if applicable).

g. Work with the organization's IT professionals to develop and implement software migration plans to:

(1) Prevent the unauthorized access, modification, or deletion of declared records, and ensure that appropriate audit trails are in place to track use of the records.

(2) Ensure that all records in the system are retrievable and usable for as long as needed to conduct agency business.

(3) Develop procedures to migrate records and related metadata to stable storage media and sustainable formats.

h. Maintain permanent records in formats pursuant to NARA requirements in Reference (e) and identify clearly to prevent inadvertent deletions. Permanent electronic records must be identified to the CRMO and RPDD for pre-accessioning to NARA.

Figure 8. Flat File Structure

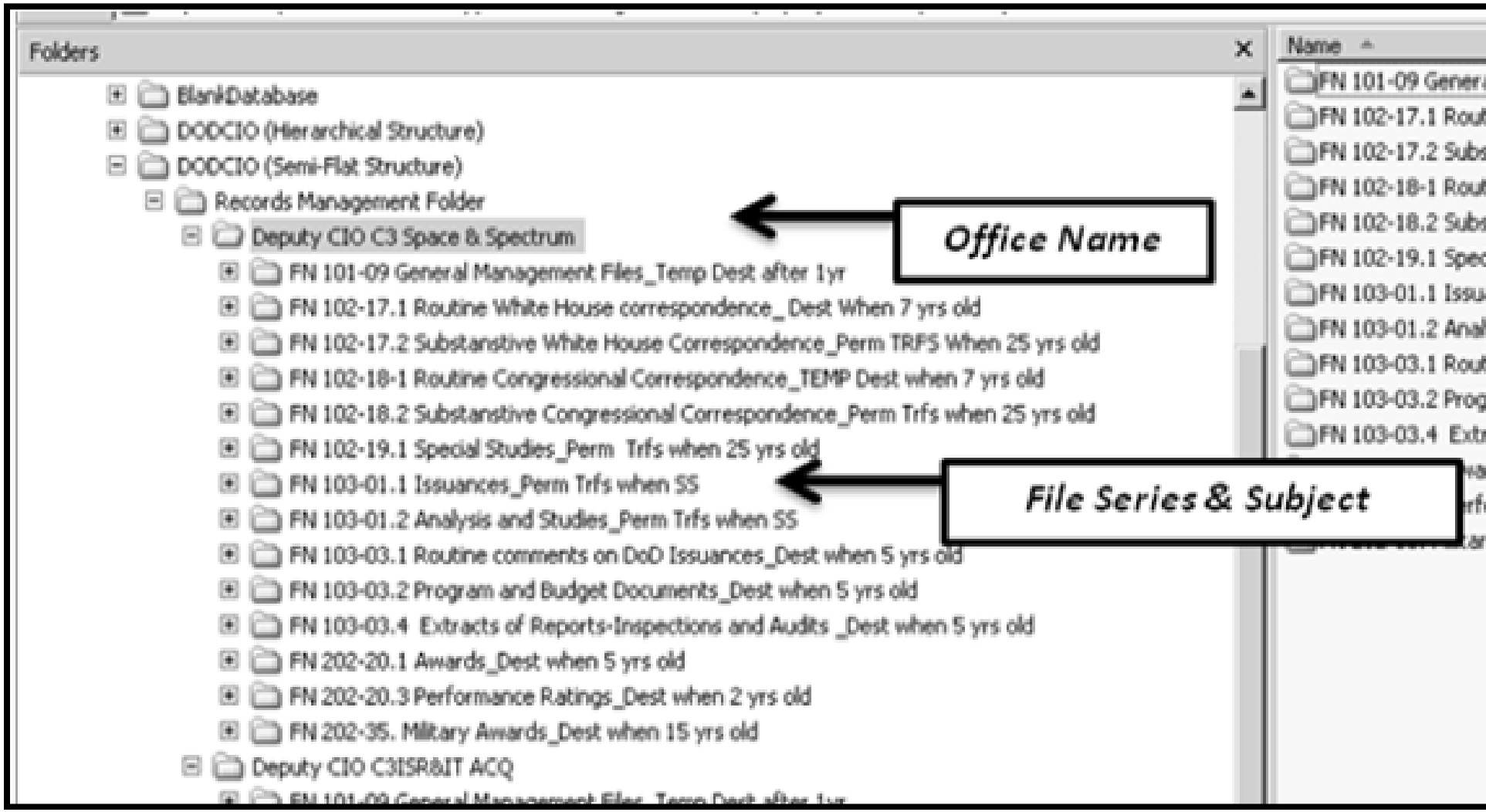


Figure 9. Subject Matter File Structure

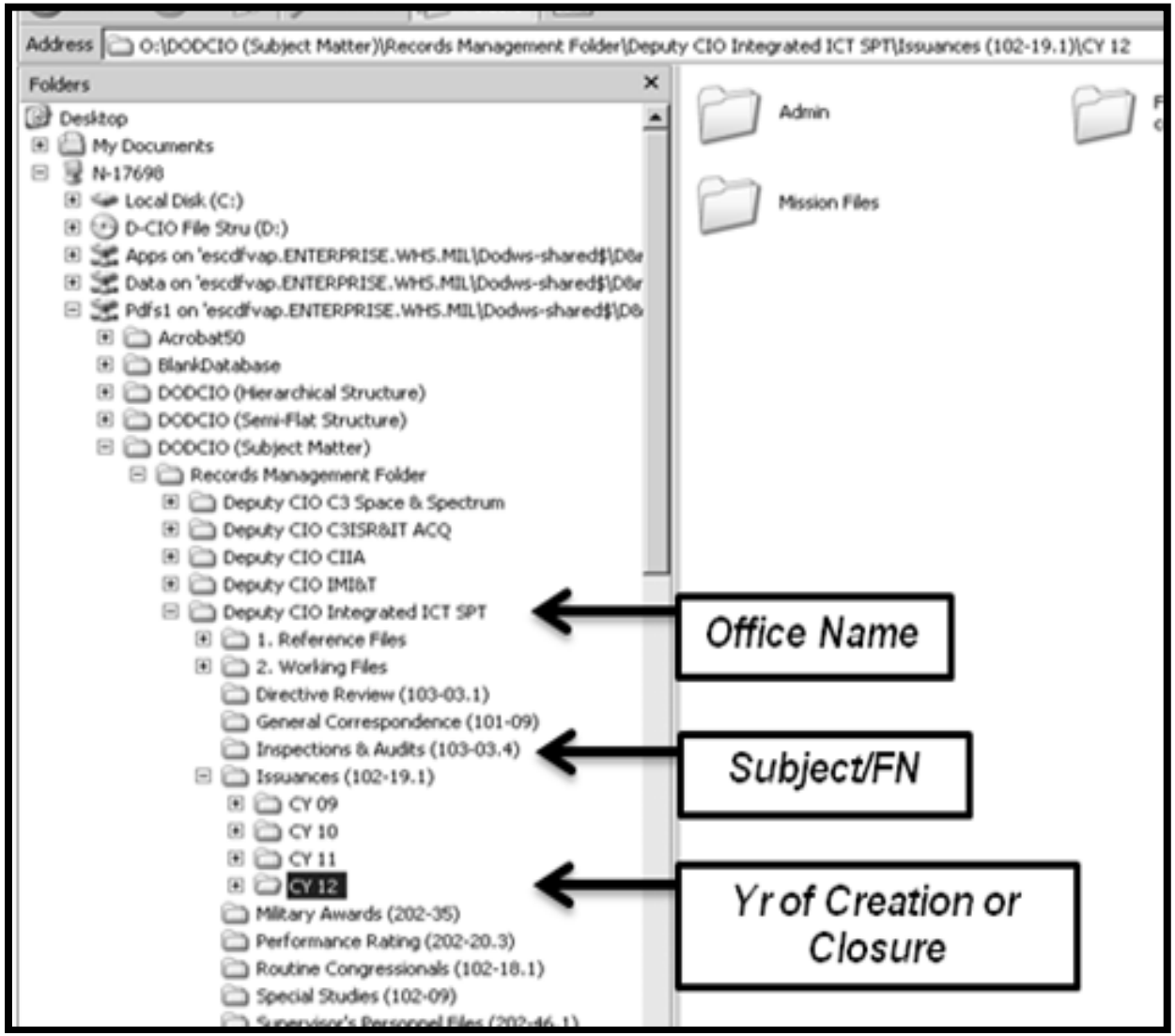


Figure 10. Consolidated File Structure

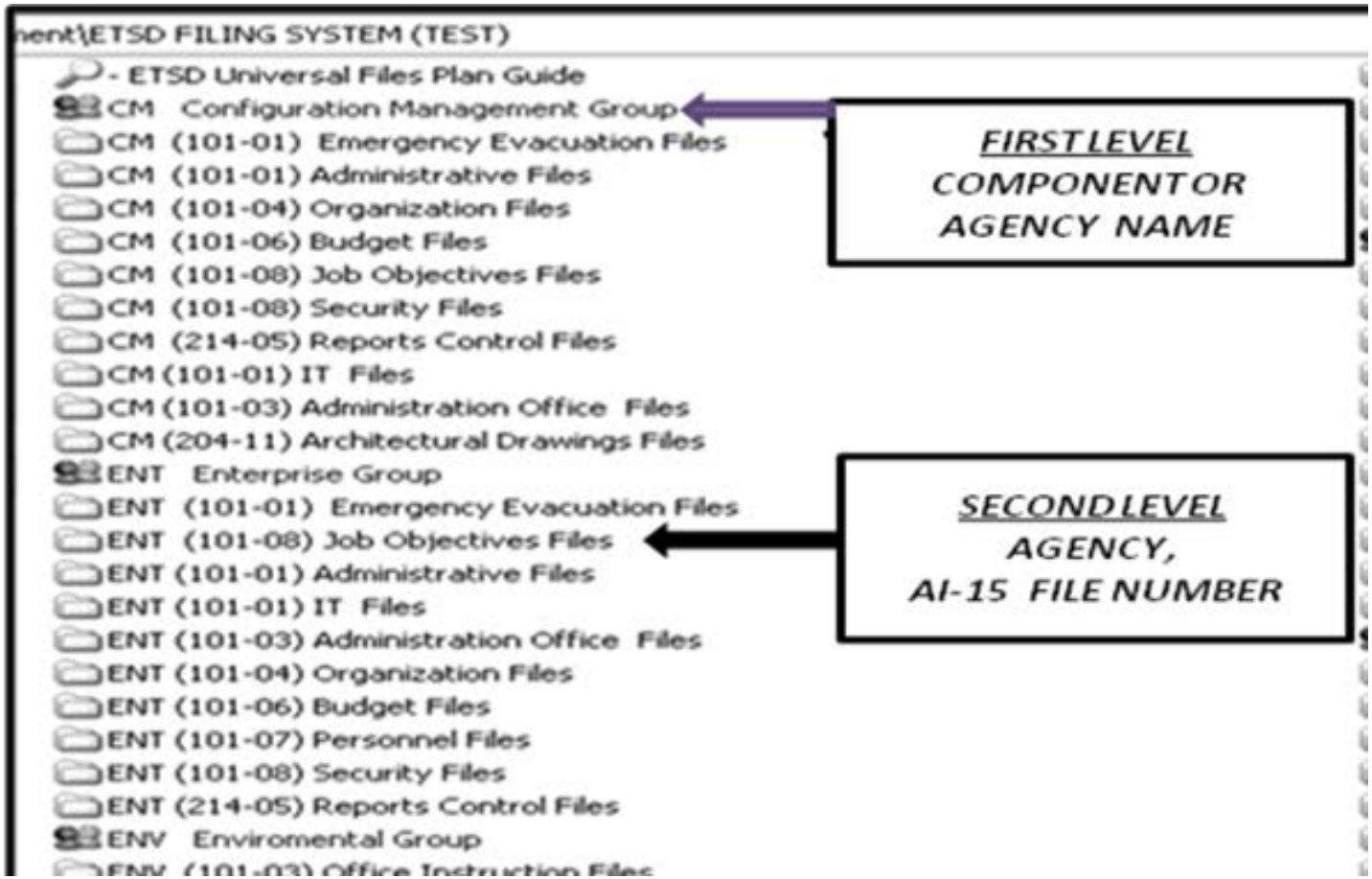
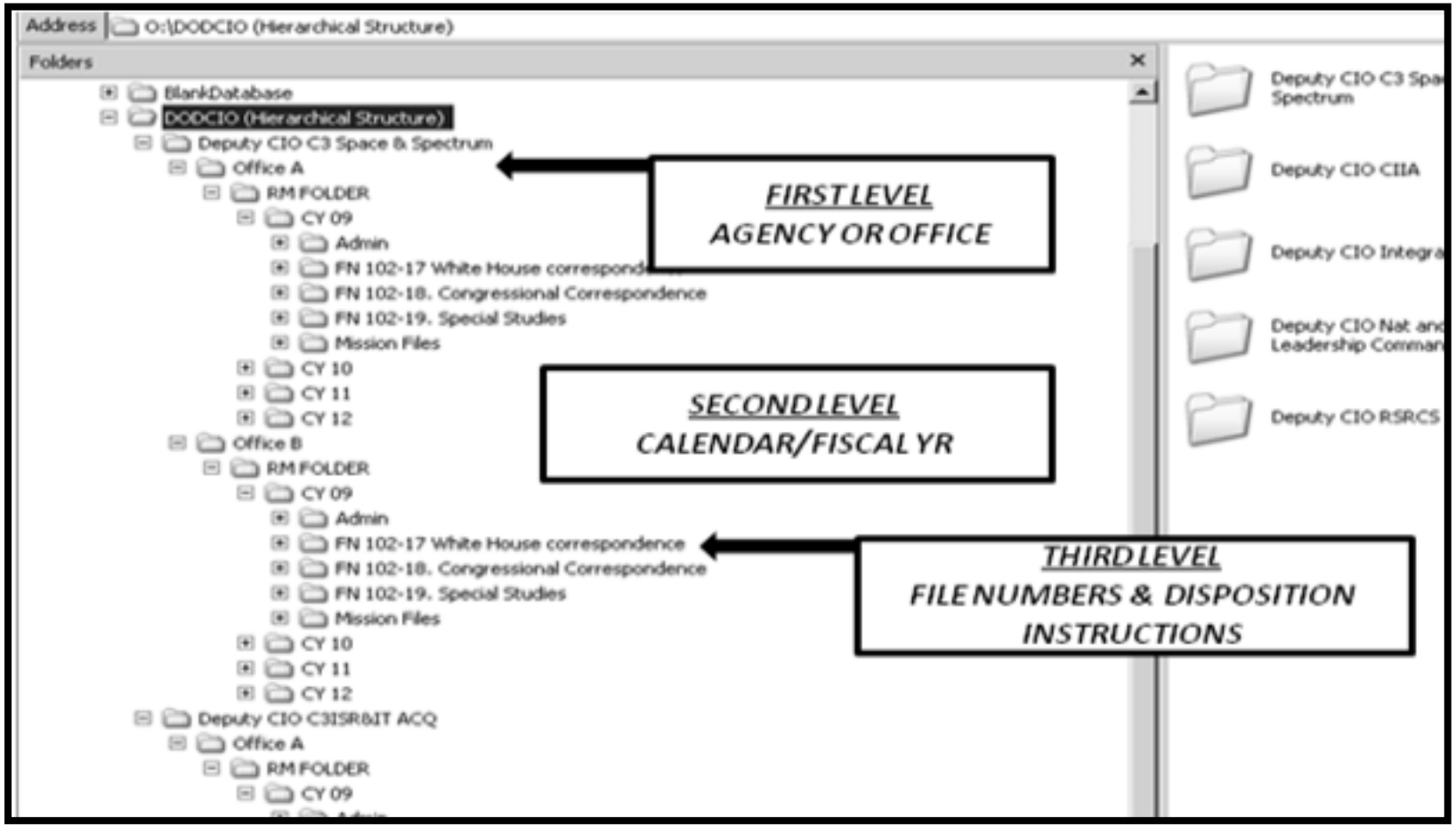


Figure 11. Hierarchical File Structure



i. Ensure records are maintained throughout their approved life cycle as stated in Reference (e) and the OSD Records Disposition Schedule.

j. Clearly identify and segregate from the official record all personal and non-record documents (e.g., personal correspondence, reference materials, periodicals) maintained on shared drives.

k. Institute business rules that ensure records can be identified, retrieved, and preserved and to prevent unintentional or illegal destruction.

l. Identify records and location on the office file plan.

m. Train staff in the use of the shared drive and in their records management responsibilities.

4. ELECTRONIC MAIL (E-MAIL) AND INSTANT MESSAGING (IM). Depending on their content, e-mail and IM may need to be managed as records. Only those e-mail and IMs that contain information documenting an organization's policies, programs, and activities as identified in the OSD Records Disposition Schedule will be managed as WHS-serviced Component records.

a. Functionally, e-mail and IM are similar; both allow sending and receiving of messages electronically. Employees use e-mail and IM to send messages, attach and exchange electronic files such as images, audio, video, and textual documents; respond to messages; and block other users with whom they do not want to exchange messages.

b. WHS-serviced Components are responsible for ensuring that records management policy, procedures, and dispositions are incorporated into their daily business practices for the management of e-mail and IMs. (See RM requirements in section 5 and email and IM disposition requirements in section 6 of this enclosure.)

c. Metadata tags on e-mail will include but are not limited to: office of origin; file code; key words for retrieval; author; date; and security classification (if applicable).

d. DoD e-mail and IM accounts are provided for business use and are not to be considered personal files, although they may contain personal information and non-record materials as part of its general use. Contents of e-mail accounts are subject to FOIA, PA, records management, and security procedures. Proper business protocols applying to any other type of communication should also be used for e-mail. E-mail and IM are records if they:

(1) Document agreements reached in meetings, telephone conversations, or other exchanges on substantive matters relating to business processes or work related activities.

(2) Provide concur or non-concur, comments on, or objections to the language on drafts of policy statements or action plans;

(3) Supplement information in official files or add to a complete understanding of the organization's operations and responsibilities;

(4) Are needed by the individual or their successor in carrying out organizational responsibilities;

(5) Make possible a proper scrutiny by Congress or other duly authorized agencies of the government;

(6) Protect the financial, legal, and other rights of the government and of persons directly affected by the government's actions; or

(7) Document the formulation and execution of basic policies and decisions and the taking of necessary actions, including all significant decisions and commitments reached orally (person-to-person, by telecommunications, or in conference).

e. E-mail calendars and task lists must be managed as records if:

(1) They contain substantive or non-substantive information relating to official activities of the employee. See the OSD Records Disposition Schedule, file number 103-18 for complete file description.

(2) They relate to the official activities of high government officials: calendars of the Secretary of Defense, Deputy Secretary of Defense, and the WHS-serviced Component heads that have **not** been incorporated into the office files will be considered a permanent record.

f. E-mail that should be deleted from the system immediately after being read or within 30 days are:

(1) Automatically generated news and marketing feeds.

(2) Auto-generated messages like out-of-office responses, published information.

(3) Solicitations (charitable or private industry).

(4) Official information captured elsewhere (paper or electronic) but preserved ONLY for convenience of reference.

(5) "Not read" or "Read" messages, not required as evidence of receipt.

(6) Personal messages that pertain **only** to an individual's private business and are considered non-record information.

g. E-mail archiving refers to applications that remove e-mail from the mail server and manage it in a central location known as an archive.

(1) These applications collect in a central repository the e-mail (which may include attachments, calendars, task lists, etc.) of some or all the organization's users.

(2) E-mail archiving applications typically require little to no action on the part of the user to store or manage the e-mail records. Once messages are stored, authorized users are able to search the repository.

(3) While these applications offer business benefits, e-mail archiving technologies do not necessarily meet all of the requirements of Reference (e).

(4) Organizations acquiring such systems should continue to apply e-mail guidance provided in sections 5 and 6 of this enclosure, unless records management policies and procedures, business rules, employee training, and other conditions necessary to ensure compliance with records management requirements are implemented with the system.

5. RECORDS MANAGEMENT REQUIREMENTS FOR E-MAIL AND IM SYSTEMS. WHS-serviced Components must:

a. Ensure e-mail and IM systems and file backup processes and media are not used as an electronic recordkeeping system, pursuant to Reference (e).

b. Ensure that transmission data (names of sender and addressees and date the message was sent) are preserved for each e-mail record. Any other transmission data needed for purposes of context should also be preserved such as "Not read" or "Read" messages, if needed as evidence of receipt.

c. Maintain distribution lists to ensure identification of the senders and addressees of messages that are records.

d. Require that electronic return receipts, if used to certify a message was delivered to the recipient, be filed with the original message so as to be retrievable throughout the disposition cycle of the original message.

e. Ensure that federal records sent or received on these systems are preserved in an approved recordkeeping system, along with transmission and receipt data.

6. DISPOSITION OF E-MAIL AND IM. Delete all non-record messages as soon as practicable. If records officers determine that an e-mail or IM is a record, it must be filed as follows:

a. E-mail or IM of Permanent Value or Long Term (1 Year or More) Temporary. If the e-mail or IM is identified as permanent record or long term temporary record as stated in the OSD Records Disposition Schedule, users must:

(1) Print the e-mail or IM and attachments and file in accordance with the OSD Records Disposition Schedule;

(2) Save to an approved RMA; or

(3) Save e-mail or IM and attachment and convert to .pdf, .tiff, or .jpeg formats and file in appropriate folder on a shared drive.

b. E-mail or IMs of Temporary Value (less than 5 years). If the e-mail is identified as a temporary record, users may manage in existing format.

c. E-mail or IMs of Transitory Value (180 days or less). If the e-mail is identified as a transitory record consistent with Reference (e) and the OSD Records Disposition Schedule it can reside in the user's inbox and then be deleted.

7. WEB 2.0 (SNS). Internet-based capabilities include collaborative tools such as social media, user-generated content, social software, e-mail, instant messaging, and discussion forums (e.g., YouTube, Facebook, MySpace, Twitter, Google Apps, LinkedIn, Wikis). SNSs can be publicly, privately, or government owned. Regardless of the status (public or private) all users of these Internet-based capabilities must be aware of the potential record value of their content to include content that may originate outside WHS-serviced Components in accordance with DoDI 8550.01(Reference (w)).

a. Public and Privately Owned SNSs

(1) Organizations maintaining profiles or channels on SNS must ensure that posts, photos, videos, and other nontraditional media types that document interactions with the public or post information not available elsewhere are captured and maintained as a part of the component's records in accordance with References (e) and (w).

(2) Organizations will identify all public or privately owned SNS on which it maintains a presence in the file plan. At the minimum, components will identify site name, uniform resource locator (URL), program manager, and disposition of data

(3) Ensure that all contracts between the SNS and the Department of Defense include language for records management compliance in accordance with Reference (e).

b. WHS-serviced Component-owned SNS:

(1) Applications such as wikis, blogs, instant messaging services, and collaborative tools solely built, used for and by DoD employees and authorized contractors must include the prerequisites in References (e) and (w).

(2) Organizations will maintain a record of the SNS and ensure sites are scheduled pursuant to Reference (e). At the minimum components must provide to RPDD site name, URL, disposition of the data and site, and program manager.

8. CLOUD COMPUTING SOLUTIONS. In addition to the prerequisites in paragraph 3a of this enclosure, WHS-serviced Components will ensure that cloud computing solutions can identify and manage both record and non-record information, and apply approved records dispositions. This includes but is not limited to wikis, blogs, IMs, and e-mail.

9. RMA OR SYSTEMS. An RMA collects, organizes, and categorizes electronic records in their native file form and in a NARA acceptable transfer format; it also manages the metadata regarding hard copy records.

a. Such a system automates the preservation, retrieval, use, and disposition of records.

b. Electronic recordkeeping systems that maintain the official file copy of text documents on electronic media must meet the requirements specified in Reference (q).

c. WHS-serviced Components will ensure that records maintained in such systems can be correlated with related records on paper, microform, or other media.

d. Most FRCs do not accept electronic records for retirement purposes, and NARA only accepts the early transfer of permanent records.

e. WHS-serviced Components should plan for the maintenance of temporary electronic records in a sustainable format that increases the likelihood of a record being accessible throughout its life cycle.

10. CAPITAL PLANNING AND MANAGING INFORMATION SYSTEMS

a. WHS-serviced Components will incorporate records management and archival functions into the design, development, and implementation of information systems. Reference (v) requires federal agencies to record, preserve, and make accessible sufficient information to ensure the management and accountability of agency programs, and to protect the legal and financial rights of the federal government. Each WHS-serviced Component will ensure that their EISs are in compliance with References (d) and (e). WHS-serviced Components are to notify RPDD to ensure their systems have a NARA approved disposition schedule.

b. The functional proponents developing or purchasing information systems, including commercial off-the-shelf (COTS) products, are responsible for ensuring that records management functionality, policy, procedures, and dispositions are incorporated into each system. All functional proponents will submit an electronic information system survey (SD828), available at http://www.dtic.mil/whs/directives/forms/eforms/sd0828.pdf, to RPDD.

c. WHS-serviced Components, CIOs, and system developers must incorporate records management controls into the EIS, or integrate them into a recordkeeping system that is external to the information system itself, in accordance with section 1236.20 of Reference (e) and Reference (q). The following types of records management controls are needed to ensure that federal records in EISs can provide adequate and proper documentation of DoD business for as long as the information is needed.

(1) Reliability: Controls to ensure a full and accurate representation of the transactions, activities, or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

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

(3) Integrity: Controls, such as audit trails, to ensure records are complete and unaltered.

(4) Usability: Mechanisms to ensure records can be located, retrieved, presented, and interpreted.

(5) Content: Mechanisms to preserve the information contained within the record itself that was produced by the creator of the record.

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

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

d. Functional proponents must integrate records management functionality and archival requirements into the design, development, and implementation of new EIS and ensure the requirements listed in paragraphs 10d(1) and 10d(2) of this enclosure are built into existing systems, when updated.

(1) All records are to be retrievable and usable for as long as needed to conduct government business. Records are to be protected against technological obsolescence by designing and implementing migration strategies to counteract hardware and software dependencies of information systems.

(2) Archiving and migration strategies will address non-active electronic records that are stored off-line. Where the records will need to be retained beyond the planned life of the system, functional proponents must plan and budget for the migration of records and their associated metadata to new storage media or formats to avoid loss due to media decay or technology obsolescence.

e. Systems must have the ability to transfer permanent records to NARA; see section 13 of this enclosure.

f. Systems and file backup processes and media are not to be used for recordkeeping, as they do not provide the appropriate recordkeeping functionalities, as required in Reference (e).

g. A WHS-serviced Component's unique records and information system not listed in OSD Records Disposition Schedule must have records schedules drafted and submitted to NARA in accordance with paragraph 12b of this enclosure.

h. Information systems that replace a manual (paper-based) system are to be appraised to identify any new records being created by the automation of the process.

i. Contracts that require the creation of data for the government's use will address records created, processed, or in possession of contractor-owned system or non-federal entity. Contracts must safeguard federal records; see part 1222 of Reference (e) for additional requirements.

11. JUDICIAL USE. Electronic records are admissible as evidence in federal court proceedings if the record is deemed trustworthy by ensuring its accuracy, integrity, and authenticity of the information. To ensure the trustworthiness of an electronic record:

a. Protect the information from unauthorized deletions, modifications, or additions. Validate the system to prevent unauthorized access.

b. Demonstrate that a standard method for storing and retrieving the information is utilized.

c. Identify the location of the record information and retain the record as prescribed in the disposition instructions.

d. Coordinate with records management, legal, and IT personnel to ensure compliance with current regulatory requirements.

12. SCHEDULING. The program office and CRMO will work with RPDD to describe and develop records schedules for websites, EISs, and databases.

a. Scheduling Websites. When developing disposition schedules for internet and intranet websites, be sure the schedule identifies the web content records of the site itself and the management and operations records, which provide the website's context and structure.

(1) Web content records include: The content pages that compose the site, inclusive of the HTML markup; records generated when a user interacts with a site; and if the WHS-serviced Component chooses to document its site this way, lists of the URLs referenced by the site's hyperlinks.

(2) Web management and operations records that provide context to the site include: Website design records, records that specify the WHS-serviced Component's web policies and procedures on addressing such matters as how records are selected for the site and when and how they may be removed, records documenting the use of copyrighted material on a site, records relating to the software applications used to operate the site, and records that document user access and when pages are placed on the site, updated, or removed.

(3) Web management and operations records that provide structure related to the site include: site maps that show the directory structure into which content pages are organized and COTS software configuration files used to operate the site and establish its look and feel, including server environment configuration specifications.

(4) To assist RPDD in determining retention periods for website-related records, the WHS-serviced Component needs to assess how long the information will be needed to satisfy its business needs and mitigate risk, taking into consideration accountability to the public and the protection of legal rights. The Component will designate if specific web content is available in places other than the web and determine whether the existence of the information in other records affects the retention needs for the web records. In the case of information unique to the website, the web version may be considered the only recordkeeping copy by NARA.

(5) Most web records do not warrant permanent retention and are to be scheduled for disposal in accordance with the guidance in Enclosure 4 of this AI. If NARA determines that a site or portions of a site have long-term historical value, RD&D will work with the creating organization's program office to develop procedures to preserve the records and provide for their transfer to NARA. While a snapshot of the website may provide some indication of the look and feel of a component's web presence on one particular day, the web snapshot does not systematically or completely document the organization's actions or functions in a meaningful way. Such records are to be found in other ongoing, systematic records series identified in OSD Records Disposition Schedule. Steps to implement in the management of websites include:

(a) Document the systems used to create and maintain the web records.

(b) Ensure that web records are created and maintained in a secure environment that protects the records from unauthorized alteration or destruction.

(c) Implement standard operating procedures for the creation, use, and management of web records and maintain adequate written documentation of those procedures.

(d) Create and maintain web records according to these documented standard operating procedures.

(e) Train staff in the standard operating procedures for creating and maintaining web records.

(f) Ensure there is an approved disposition schedule for web records. The WHS-serviced Component will need to cite the official disposition authorities found in the OSD

Records Disposition Schedule if it is faced with legal challenges to produce records that have been destroyed.

b. Scheduling EISs and Databases. To assist RPDD in scheduling EISs and databases, the program office for the EIS or database must first identify its systems to RPDD and complete an SD Form 828 available at http://www.dtic.mil/whs/directives/infomgt/forms/sd/sdforms.htm for each EIS or database. The SD 828 will describe the system and record data contained therein, and recommend retention periods for the EIS or database. The program office should also cite any applicable laws or regulations, PA SORN, or information collection requirements that apply to the system.

13. TRANSFERRING PERMANENT ELECTRONIC RECORDS TO NARA. Transfer of permanent electronic records to the legal custody of the National Archives must be on a medium acceptable to NARA at the time they are transferred. Each WHS-serviced Component is responsible for the integrity of the records it transfers to the National Archives. To ensure that permanently valuable electronic records are preserved, each WHS-serviced Component will transfer electronic records to NARA promptly in accordance with the OSD Records Disposition Schedule. All permanent electronic records must be transferred in discrete file sets that contain ONLY permanent records identified in a separate and distinct manner in accordance with NARA requirements.

a. Temporary Retention of Copy. Each WHS-serviced Component will retain a second copy of any permanently valuable electronic records that it transfers to NARA until it receives official notification from NARA or RPDD that the transfer was successful and NARA has assumed legal responsibility for continuing preservation of the records.

(1) WHS-serviced Components may transfer a copy of permanently valuable electronic records to the NARA while retaining legal custody and control over access to the records (pre-accessioning).

(2) NARA processes and preserves these records and maintains physical custody until the records are scheduled to transfer into NARA's legal custody.

(3) WHS-serviced Components will keep duplicate copies of the records and retain responsibility for responding to discovery efforts, FOIA requests, or reference inquiries until legal custody of the records is transferred to NARA.

b. Transfer Media. The WHS-serviced Components will use only media that are sound and free from defects for electronic records transfers; the organization will take reasonable steps to meet this requirement. See section 1235 of Reference (e) for the requirements governing the selection of electronic records storage media. The media types that are approved for transfer are open reel magnetic tape, magnetic tape cartridge, compact disk read only memory (CD-ROM), DVD, and removable hard drives. See part 1235 of Reference (e) for media specifications and transfer instructions.

c. Formats

(1) The WHS-serviced Components may not transfer to the National Archives electronic records that are in a format dependent on specific hardware or software.

(2) The records must not be compressed unless NARA approves the transfer in the compressed form in advance. In such cases, NARA may require the component to provide the software to decompress the records.

(3) Some of the formats currently acceptable to NARA are: data files and databases; e-mail; plain ASCII files, with or without standard generalized markup language (SGML) tags; .TIFF; portable document format (PDF); digital spatial data files; digital photos; and web records (HTML or extensible markup language (XML)).

(4) WHS-serviced Components should identify any other categories of electronic records that could cause a foreseeable problem in the transfer of potentially permanent electronic records in accordance with part 1234 of Reference (e) at the time the records are scheduled.

(5) Special transfer requirements agreed upon by NARA and the component will be included in the disposition instructions.

d. Documentation. Documentation adequate to identify, service, and interpret electronic records that have been designated for preservation by NARA will be transferred with the records. This documentation will include completed NARA Form 14097, "Technical Description for Transfer of Electronic Records," and a completed NARA Form 14028, "Information System Description Form," or their equivalents. Where possible, agencies should submit required documentation in an electronic form that conforms to the provisions of this section.

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

(2) Digital Spatial Data Files. Digital spatial data files will include the documentation specified in part 1235 of Reference (e). In addition, documentation for digital spatial data files may include metadata that conforms to the Federal Geographic Data Committee's Content Standards for Digital Geospatial Metadata, as specified in Executive Order 12906 (Reference (x)).

(3) Documents Containing SGML Tags. Documentation for electronic files containing textual documents with SGML tags will include a table for interpreting the SGML tags, when appropriate.

(4) Web Content Records. In addition to the transfer documentation requirements in part 1235 of Reference (e), for each transfer, if applicable, WHS-serviced Components must supply documentation that identifies:

(a) Web platform and server, including the specific software application(s) and, where available, intended browser application(s) and version(s).

(b) Name of the web site.

(c) URL of the web site, including the file name of the starting page of the transferred content.

(d) Organizational unit primarily responsible for managing web site content.

(e) Method and date of capture:

1. If harvested, also include the application used with either a URL to the application's web site or a description of the harvester's capabilities and the log file(s) generated by the harvester that document the harvesting process.

2. If .pdf, also include the software and version used to capture the .pdf.

3. If more than one method is used, clearly identify which content was captured by which method.

4. Include contact information for individual(s) responsible.

(f) The name and version of any content management system used to manage files on the web.

(g) All file names, inclusive of both the path (or directory) name and the file name.

(h) The business logic and web interfaces clearly identified with each corresponding database.

(i) If available, a site map of the web site from which the web content records originated.

14. ADDITIONAL GUIDANCE

a. NARA is continuously evaluating industry standards for various transfer formats. For the transfer of e-mail, IMs, scanned images of textual records, pdf records, digital photographic records, digital geospatial records, and web content records, go to NARA Electronic Records Guidance web page: http://www.archives.gov/records-mgmt/initiatives/erm-guidance.html.

b. For up to date guidance on acceptable transfer media and formats for electronic records visit the following web sites:

(1) Reference (e) Electronic Records: http://www.gpoaccess.gov/cfr/index.html.

(2) NARA Records Management site: Transfer of Permanent Electronic Records to NARA: http://www.archives.gov/records-mgmt/initiatives/transfer-to-nara.html.

c. For guidance on the management of audiovisual records, see National Archives Records Disposition Authority, "DoD Visual Information," DAA-0330-2013-0014 (Reference (y)).

d. For guidance on requirements for audiovisual, cartographic, and related records management from part 1237 of Reference (e), go to: https://www.ecfr.gov/cgi-bin/text-idx?SID=7c1463f70ae14cf931c68cef35a65792&mc=true&tpl=/ecfrbrowse/Title36/36cfr1237_main_02.tpl.

# ENCLOSURE 7

## PREPARING RECORDS FOR TRANSFER TO THE FRC

1. BACKGROUND. There are two types of records that may be transferred to the FRC: PERM and TEMP. PERM hardcopy records will be held at the FRC for a specified period of time, usually 25 to 30 years, and then offered to NARA for accession. TEMP records are held at the FRC until they are ready for destruction and then they are disposed of by FRC personnel, usually from 2 to 20 years after their transfer. Only TEMP records with a specified destruction date can be retired to an FRC. Preparing records for transfer is a two-step process: selecting and screening. Preparing the records for actual transfer, packing them, and preparing the paperwork is covered in Enclosure 9 of this AI. Enclosure 3 of this AI describes the steps to prepare and screen files.

2. FILE TRANSFER SELECTION. To be transferred to an FRC, records must:

a. Be scheduled for transfer to an FRC. To determine this, check the appropriate files series at the OSD Records Disposition Schedule.

b. Not be needed to carry out current organizational operations. Files must be closed.

c. Not be eligible for immediate destruction, unless pre-empted by a records freeze. Records under a records freeze due to litigation (see section 5 of Enclosure 4) can be retired to the FRC if no longer needed for current business. Records must have at least 1-year retention from the date of transfer and cannot contain disposition instructions that state, "Destroy when superseded, no longer needed, or obsolete."

3. SCREENING

a. Permanent records and records scheduled for retention for 30 years and more must be screened and extraneous materials removed. Remove extra (non-record) copies of documents, empty folders or folders containing temporary information, or other materials that are unnecessary or have no lasting value to the record series being transferred. This includes duplicate copies of documents with no additional record value (see section 17 of Enclosure 3 of this AI for specifics).

b. TEMP files do not have to be screened when retained in the office. Files transferred to an FRC must be screened. To be useful to anyone, files should always be ready for reference. In deciding whether to screen, consider:

(1) Can complete folders be removed? For example, are there folders that are empty or contain information that has met its disposition?

(2) Can disposable material be separated easily from individual folders?

(3) Can materials to be removed be easily identified?

(4) Can the records to be screened be easily accessed?

(5) Is physical processing such as the removal of fasteners necessary?

4. FILING RECOMMENDATIONS

a. Screening problems are reduced if records to be retained permanently or for long periods are not filed with papers of lesser value and file numbers are annotated on the file labels.

b. If papers have to be recalled from the FRC, the more clearly they are marked and organized, the easier they will be to find. If filing is done thoroughly, individual file folders can be recalled instead of whole boxes or accessions.

# ENCLOSURE 8

## PACKING AND SHIPPING PROCEDURES FOR TRANSFER OF RECORDS

1. PACKAGING RECORDS FOR TRANSFER TO FRC. Records are transferred in standard General Services Administration (GSA) cardboard cartons each holding 1 cubic foot. **No exceptions are permitted**. The cartons will accommodate either letter- or legal-sized material. Special containers may be obtained for oversized materials or magnetic tapes. Nonstandard boxes cannot be used.

2. SHIPPING CONTAINERS AND RELATED SUPPLIES. The standard record shipping container to be used for the transfer of files is a fiberboard (lock bottom with reinforced hand holes on each side); 275-pound test; size: 14-3/4 x 12 x 9-1/2 inches; FSN: 8115-00-117-8249.

3. REQUISITIONING. Standard-sized boxes are available in the self-service supply centers. Containers for odd-size boxes should be ordered directly from supply services using the stock numbers listed in section 4 of this enclosure.

4. SHIPPING CONTAINERS FOR ODD-SIZED DOCUMENTS. When records being shipped are too large or too small for the container described in section 2 of this enclosure, the documents will be securely packed and shipped in a manner that prevents damage in route. The following containers are recommended for the types of records indicated:

a. Half-size box, 14-3/4 X 9-1/2 X 4-7/8 inches, NSN: 8115-00-117-8338. For shipping 3 by 5-inch card files when strips of cardboard are placed between rows of cards and wadded paper is used to fill any open space in the box. In addition, this box is suitable for shipping punched cards.

b. Magnetic tape box, 14-3/4 x 11-3/4 x 11-3/4 inches for magnetic tape records, NSN: 8115-00-117-8347.

c. Microfiche box, 14-3/4 x 6-1/2 x 4-1/2, NSN: 8115-01-025-3254.

d. Tubes, not longer than 36 inches should be used for documents that are normally shipped rolled (maps, charts, plans). If tubes are not available, fold these records and ship in the standard container above. Use tubes for permanent records.

5. LISTING RECORDS FOR TRANSFER OR RETIREMENT. Files to be retired to the FRC will be identified on the SF 135 available in electronic form from the NARA website at http://www.archives.gov/records_center_program/forms/forms.html. When more than one page is required for the box list, continue the list in a separate electronic file (MS Word, Excel, or

PDF formats are acceptable). The SF 135 serves as a packing list for the transfer and retirement of files; as a medium for controlling the location and disposition of files in record holding areas and FRCs; and as a receipt for records retired to the FRCs.

6. TRANSFER OF RECORDS TO OTHER EXTERNAL ORGANIZATIONS

a. Unclassified files transferred to other external organizations as a result of a transfer of functions or for other reasons will be approved by the OSD Records Administrator and listed on the SF 135.

b. Distribution of the SF 135:

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

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

7. RECORD PREPARATION FOR RETIREMENT AND SHIPMENT TO THE FRC

a. The retirement and transfer of records require the preparation of an SF 135 (see Figure 12 for a sample). As Figure 12 illustrates, each different series of records is a block of records having the same disposal authority and the same disposal date. An attached box list must accompany each SF 135. Use the electronic version of the SF 135 for retirement of the records. Detailed instructions for completion of the SF 135 are on the NARA website www.archives.gov or can be requested from RPDD. In addition to these instructions, the WHS-serviced Components will:

(1) Describe the records adequately, including the inclusive dates in column (f) and the security classification in column (g). Transmittal documents for all records must list the beginning and ending file in each box. Provide a folder title list of the box contents or equivalent detailed records description for every box. Do not list classified titles or PII protected under the PA on the SF 135. The SF 135 and box list is considered a publicly accessible record.

(2) Obtain the OSD job number and POC for submitting the SF 135 from RPDD. For shipments, enter the total number of boxes in the volume column on the SF 135. Except when special containers are used to package oversized materials, punch cards, or magnetic tapes, volume will be expressed as number of boxes or containers; capacity of a standard GSA cardboard records retirement carton is 1 cubic foot.

(3) When completing column 6(h) on the SF 135, Disposal Authority, in addition to the OSD Records Disposition Schedule disposal citation (file series number), you must include either the GRS citation or the SF 115 Authority. The Authority Number (N1-330-XX-XX) is located before the disposition instructions. If you cannot find these citations or are not sure which ones apply to the records you are preparing for transfer, call RPDD for assistance. Sample entries include:

(a) AI 15, series 801-01., NC1-330-76-1.

(b) AI 15, series 301-09., GRS 6, Item 1a.

(4) Complete the SF 135 and box list.

(5) Limit the number of boxes on the SF 135 to 50 cubic feet per accession.

b. Submit the completed SF 135 and box list via e-mail to the RPDD POC through the CRMO. The RPDD POC will review for completeness, provide an OSD job number, sign block 2, and submit to the appropriate FRC for processing. The FRC will provide the accession number once the records have been approved for transfer. The RPDD POC will provide the requesting component office with a copy of the approved form containing the accession number. Retain one copy of the completed SF 135 and box list in your Office Record Locator files (101-05, the OSD Records Disposition Schedule).

c. RPDD will furnish the completed SF 135 via e-mail to the requesting office once the records have been transferred to the FRC. Since this is the only source of information describing the records being transferred to the FRC, this document is vital to the WHS-serviced Components when the need to retrieve specific papers from the FRC arises. When retrieval is necessary, identify the accession number of the box that contains the specific material, along with the box number and file title, if requesting individual folders.

d. The transfer of records constituting a PA SORN subject to the provisions of Reference (m) will be accompanied by the most recent PA SORN covering the records. Include the PA System Records number in column (i) of the SF 135; omit information subject to the PA.

Figure 12. Example of Standard Form 135 (SF 135), "Records Transmittal and Receipt"

**RECORDS TRANSMITTAL AND RECEIPT** Complete and send original and one copy of this form to the appropriate Federal Records Center for approval prior to shipment of records. See specific instructions on reverse. PAGE 1 OF 3 PAGES

1 TO (Complete the address for the records center serving your area as shown in 36 CFR 1228.150.)

**Federal Records Center**
Washington National Records Center
4205 Suitland Road
Suitland, MD 20746-8001

5 FROM (*Enter the name and complete mailing address of the office retiring the records. The signed receipt of this form will be sent to this address.*)

**CRN: OSD-YY-NNNN [Completed by RDD Staff]**

DOD/Washington Headquarters Services
Records and Declassification Division
1155 Defense Pentagon
Washington D.C. 20301-1155

| | | | |
|---|---|---|---|
| 2 | AGENCY TRANSFER AUTHOR-IZATION | TRANSFERRING AGENCY OFFICIAL (*signature and title*)<br>Ron McCully FOR<br>OSD Records Administrator | DATE<br>MM/DD/YYYY |
| 3 | AGENCY CONTACT | TRANSFERRING AGENCY LIAISON OFFICIAL:<br>Enter your name, office abbreviation, phone number and email address | |
| 4 | RECORDS CENTER RECEIPT | RECORDS RECEIVED BY (*Signature and Title*) | DATE |

6 **RECORDS DATA**

| ACCESSION NUMBER | | | | | | | | | COMPLETED BY RECORDS CENTER | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| RG (a) | FY (b) | NUMBER (c) | VOLUME (*cu. ft.*) (d) | AGENCY BOX NUMBERS (e) | SERIES DESCRIPTION (*with inclusive dates of records*) (f) | RESTRIC-TION (g) | DISPOSAL AUTHORITY (*schedule and item number*) (h) | DISPOSAL DATE (i) | LOCATION (j) | SHELF PLAN (k) | CONT. TYPE (l) | AUTO. DISP. (m) |
| PT-330 | 10 | | No. of Boxes (ex: 7) | Enter range of boxes (ex: 1-7) | Enter Full Name of Office<br>Enter a brief description of records<br>Enter date range of the records (EX: FY 1999, CY 2000, 2000 – 2006 or 4/1/1999 – 5/2/2001)<br><br>Enter "See Attached Box List" or otherwise refer to the box list.<br>**IF** records are under a Privacy Act Systems of Records Notice, enter: "Subject to the Privacy Act"<br>IF records are restricted, enter<br>• DO NOT include classification level of the records. Use block 6g.<br>• DO NOT include any classified or personal information; SFs 135 are public records. | | OSD AI 15<br>[enter FN]<br>[Enter Disposition Authority Number EX: GRS 3/1a or NC1-330-77-5] | Enter the Disposition information Ex:<br><br>PERM Transfer when 30 years old 1/1/2040<br><br>OR<br><br>DEST 3 years after cutoff 10/1/2013 | | | | |

DRAFT

e. For the efficient and proper preservation of the records and ease of future reference by DoD and NARA personnel, pack the cartons according to this guidance:

(1) Destroy any records eligible for destruction as authorized in the OSD Records Disposal Schedule.

(2) Pack records snugly in the box, but do not force. For ease of future reference, leave at least 2 inches of space for unclassified records. For classified boxes leave 4 inches of space in each box to allow for future declassification processing. Do not disturb existing filing arrangements to make future reference easier. Do not retire guide cards.

(3) Do **not** pack records with different retention periods and different accession numbers in the same box. Records must be of the same file series with the same classification. The OSD Records Disposition Schedule contains retention periods.

(4) Do not mix classified with unclassified records, nor different classification of classified records together. Accession will have the highest classification of documentation in the record set.

(5) Do not pack records on different media (CD-ROM, diskettes, and microfilm) with paper records; these records will be packed separately and the media will be identified on the SF 135, column (i).

(6) Maintain documentation in the original file folder. File labels and folders are to be in good condition. Replace folders that are excessively worn or labels that are falling off. Do not place rubber bands or clips on records nor place them loosely in a box.

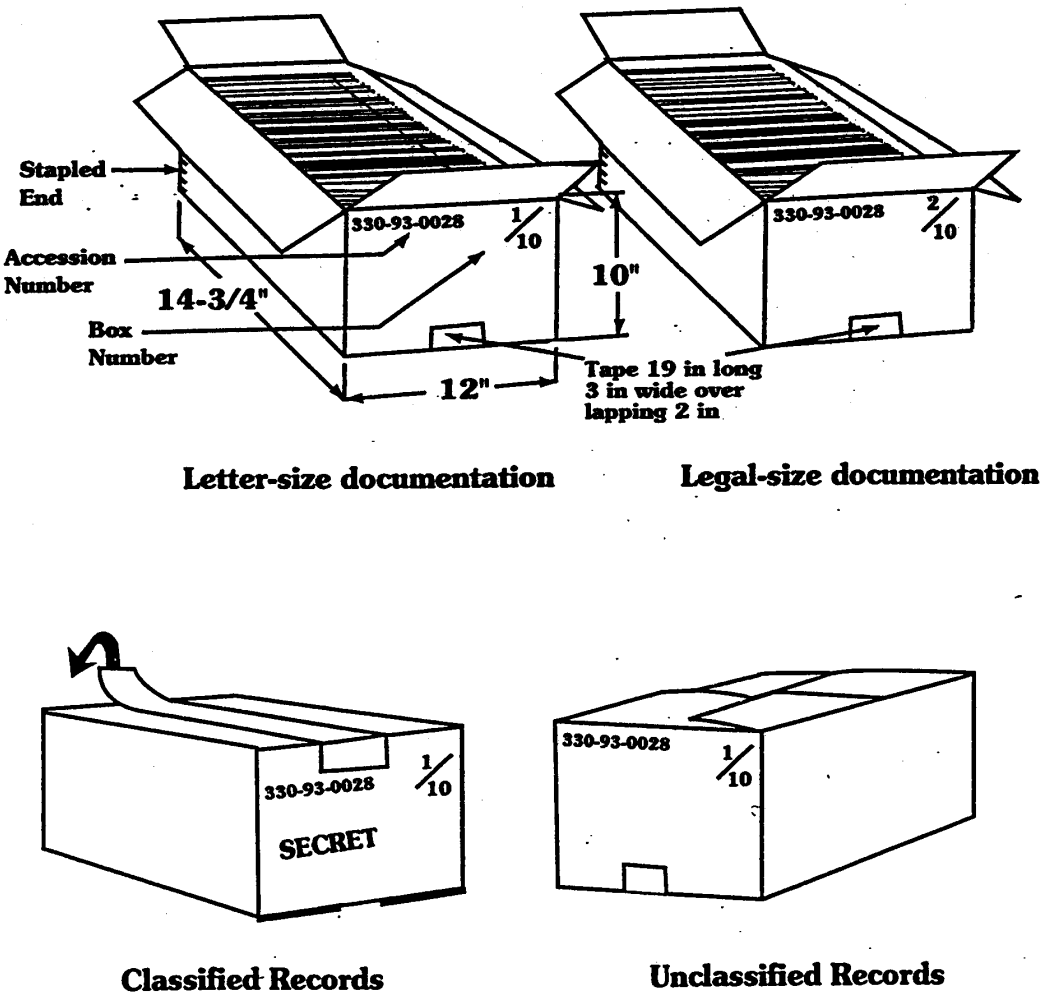
(7) Maintain the date range of the records to within the same year or within the time span of each other. For example all the records were created in 1999 only or from 1999 to 2001.

(8) Arrange folders in the order identified on the box list.

(9) Do not pack binders in boxes. Remove records from the binders and place in folders and label accordingly (see Figure 4).

f. Print the information on the end of the box legibly, in black magic marker, and include the accession number, carton number, and security classification if any. Number the boxes consecutively in the upper right hand corner of the front end of the box. Identify the box number and the total number of boxes in the accession. For example, if the shipment has three boxes, the numbers should read “1/3, 2/3, and 3/3.” Each series of records transferred will be assigned a separate accession number. See Figure 13 for placement of the accession number on the box.

Figure13. Labeling of Retirement Boxes




8. RETIREMENT OF CLASSIFIED SECURITY INFORMATION

a. When eligible for retirement, classified records will be transferred to the FRC. Complete column (g), "Restrictions," of the SF 135 to indicate the classification of the records being transferred. The SF 135 is a public record; for column (f), "Series Description," do not include any classified information.

b. Observe security requirements of Reference (l) when retiring Confidential and Secret files to the FRC. Before transferring classified material, ascertain whether the material can legitimately be downgraded in accordance with section 4, paragraph 3-402, chapter III of Reference (l) or destroyed in accordance with the OSD Records Disposition Schedule.

c. Follow Reference (l) rules for safeguarding classified material when material is packed in boxes. Comply with Reference (l), paragraphs 8-200b.4 and 8-201b before transfer or disposal of any classified material. Tape boxes containing classified data closed, taking care not to cover the informational matter on the outside of the box (see Figure 13). Mark each box conspicuously

with the highest classification of material contained in it. When the boxes are shipped to the FRC, the provisions of Chapter VIII of Reference (l) must be complied with.

d. Retire Top Secret documents eligible for retirement to the FRC as specified in Enclosure 5 of this AI. Complete the SF 135 in the usual manner except do not list classified titles on the SF 135 or the accompanying box list; all titles must be unclassified. Identify Top Secret documents under a separate accession number. The FRC provides separate storage compartments for Confidential, Secret, and Top Secret records. Ensure Top Secret documents are not included in accessions retired under a Secret or below accession number; this constitutes a security violation since special storage arrangements are made at the FRC for each level of classification.

e. Cross-reference regraded or declassified Top Secret documents that formed a part of the files that have already been retired and sent to the FRC. Make an entry on the SF 135 transmitting the documents to retirement. On the Records Transmittal and Receipt form show the designation of the organization and administrative subdivision, the file number and title of the file, and the accession shipment number assigned by the OSD Records Administrator.

f. Staffs of organizations slated for discontinuance must, prior to discontinuance, review all Top Secret documents for downgrading or declassification before shipping to the FRC.

g. Since some FRCs may not provide storage for classified Sensitive Information documents, verify with RPDD prior to retiring records whether the FRC is cleared.

h. See paragraph 10e of this enclosure for the transfer of Restricted Data or Critical Nuclear Weapon Design Information (CNWDI).

9. MATERIAL THAT SHOULD BE DESTROYED. All eligible records are identified and destroyed in accordance with the disposal standards authorization contained in the OSD Records Disposition Schedule. Destroy obsolete reference material, such as extra copies of speeches, staff papers, news releases, blank forms, reports, and publications. Eliminate extra carbon and photocopies. Do not retire housekeeping records to the FRC. See Enclosure 4 to this AI for detailed instructions on the selection of files.

10. USE OF RESTRICTED COLUMN

a. A single classification must be shown for each accession number.

b. Only the highest classification in the box is shown; the classification of each document in the box is not shown.

c. Do not file only a few classified documents in an accession number that is predominantly unclassified.

d. See Figure 12 for how to complete SF 135.

e. Boxes containing Restricted Data or CNWDI must use the "C-E" designation and clearly indicate on the SF 135 that access is restricted to only personnel of the office that retired the records who are cleared for Restricted Data or CNWDI.

## 11. ARRANGEMENT OF FILES IN FIBERBOARD BOXES

a. Regardless of the type of container used, fill containers with only one row of file folders, not stacked one on top of the other.

b. Pack letter and legal-sized files in fiberboard boxes. When filled to capacity, the box holds 15 inches of letter-sized or 12 inches of legal-sized files. Do **not** place additional material on the bottom, side, or top of the box.

(1) When the corrugated fiberboard boxes are filled to capacity with files, no packing material is required between the files and the inner walls of the box. When shipping partially filled boxes, fill the space between the files and the inner walls of the box with crumpled or wadded paper or other suitable packing material to prevent movement of the contents during shipment. Do not use excelsior, shredded paper, newspapers, or surplus file folders as packing material.

(2) Do not over pack the boxes. Fill to capacity when sufficient files are available; however, exercise care to ensure boxes are not packed so tightly that files cannot be serviced while in the container or that the box cannot be closed completely with the flaps flat. Leave enough room in the boxes for ease of reference and the declassification process. See paragraph 7f (2) of this enclosure.

c. Use the stacking instructions at Figure 14 for large shipments of records, whether shipping via a commercial carrier or requesting a pickup from the FRC.

d. Segregate permanent and temporary into the groups in paragraphs 11d(1) through (4) of this enclosure. For Official Use Only (FOUO) records are retired as unclassified material.

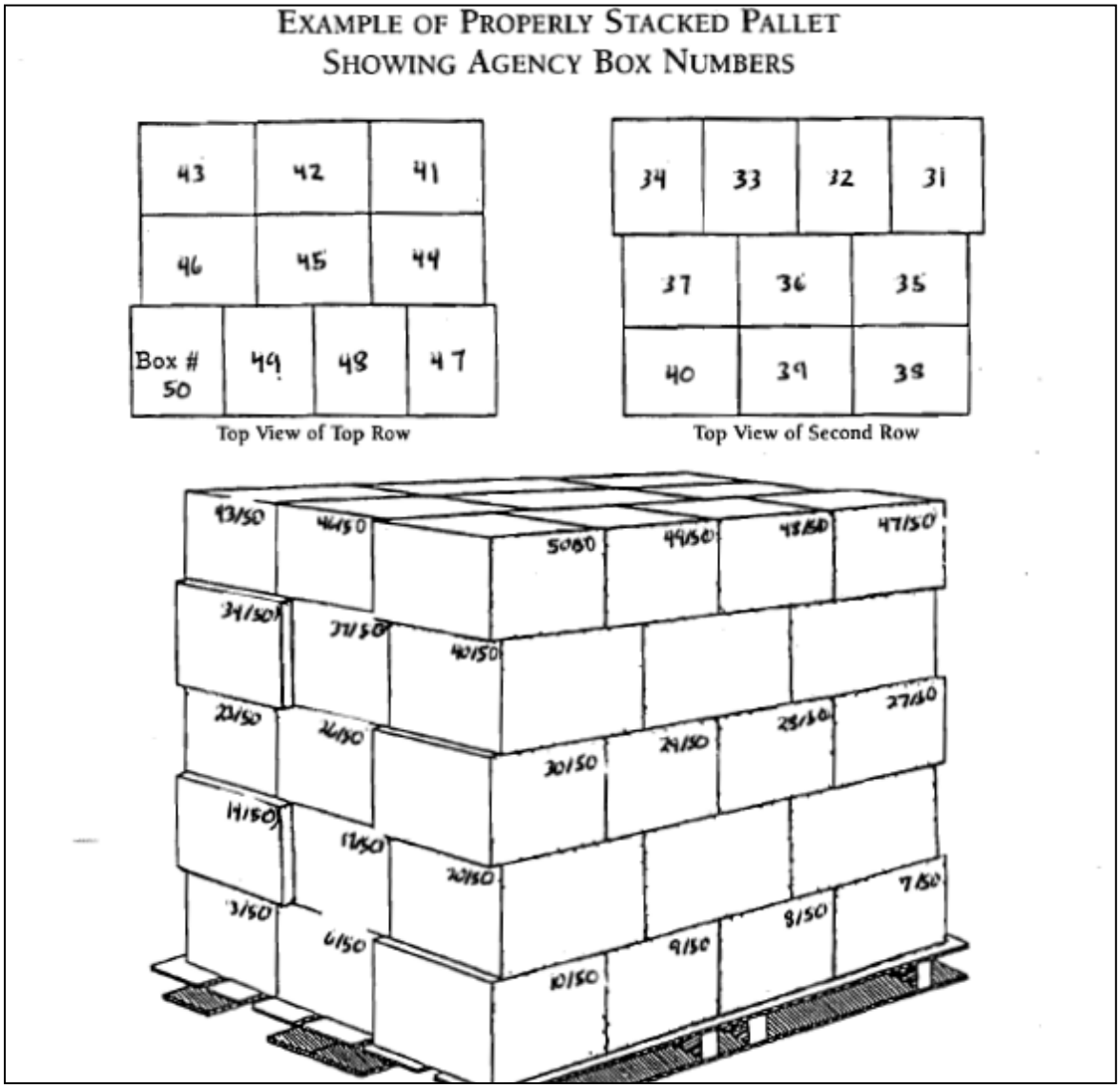
(1) Unclassified temporary records.

(2) Unclassified permanent records.

(3) Classified temporary records.

(4) Classified permanent records.

Figure 14. Example and Instructions for a Properly Stacked Pallet




Instructions:
1. Face the boxes as shown in diagram.
2. Stacking pattern for palletized records in 10 standard records center cartons per row, 5 rows per pallet. 50 cartons per pallet. Box 50 is in the top row, and box 1 is in the bottom row.
3. Four boxes on each row are placed perpendicular to the rest of the boxes in that row.
4. Numbered end not facing the front of the pallet should face right.
5. When records are boxed before pallets are available, keep the boxes in numerical order so they can be loaded on pallets properly.
6. Failure to load pallets properly will be cause for the FRC to refuse the records.
7. Pallets should be banded with steel, plastic, or cord strapping before shipping.

12. PACKING AND SHIPPING CLASSIFIED FILES. Do not ship large quantities of unclassified material in classified shipments.

a. Segregate shipments of 10 cubic feet or less and forward as two shipments, one classified, and one unclassified, when more than 50 percent of the material is unclassified.

b. Segregate unclassified material in shipments in excess of 10 cubic feet containing 25 percent or more unclassified material and forward as a separate unclassified shipment.

# ENCLOSURE 9

## RECALL OF RECORDS FROM THE FRC

1. OFFICIALS AUTHORIZED TO MAKE RECALLS. The OSD Records Administrator will maintain an up-to-date list of personnel authorized by each WHS-serviced Component organization to recall its records. This list will be provided to the servicing FRC and updated annually. Only personnel identified on the access list can request records to be recalled via RPDD. The RPDD recalls records from FRC for the WHS-serviced Components, except as noted in paragraph 2b of this enclosure. Each WHS-serviced Component designee is responsible for picking up (as applicable, records can also be mailed to the office) and returning recalled records. Responsibility for this extends to Top Secret transfers, which may necessitate an office courier or Defense Courier Service arrangements.

2. NORMAL RECALL PROCEDURES

a. To obtain reference service on records at the FRC, the CRMO or personnel authorized to request records will submit the request to RPDD. RPDD will recall the records via Archives and Records Centers Information System (ARCIS). Offices will submit requests via the CRMO by e-mail, listing accession number, box numbers, file title (if requesting folder), office address, pick-up date and time (if records are to be picked up by office staff). The request will state whether it is a temporary or permanent withdrawal, classified or unclassified request, and provide POC information (no location number needed for ARCIS) to RPDD. For records being picked up at the FRC by office staff, a minimum 3 days notice is required for non-emergency requests.

b. Customers having high-volume requirements may obtain an ARCIS account through RPDD and access the system directly. For more information about ARCIS, CRMOs should contact the RPDD POC.

3. URGENT REQUESTS. Urgent requests must be kept to a minimum. An urgent request recalls records needed to complete testimony before Congress, required as part of a legal proceeding, or specifically requested by the Secretary of Defense. RPDD will arrange all emergency recalls.

4. RETURNING RECORDS

a. To avoid the misplacing, inadvertent destruction of permanent records, or re-assimilation of recalled records into the current file system, return records to the FRC as soon as they are no longer needed. WHS-serviced Component offices will report the location of recalled records and the reason for their retention to the OSD Records Administrator when recalled records are retained for more than a year.

b. Return records in their original folder or box to allow accurate refiling. If the record box or folder is not reusable for shipment, copy the information on the previous container to its replacement. Write the word "REFILE" on the white copy of the ARCIS documentation form that accompanied the records. If these documents are no longer attached to the records, specify the refile action in a brief note or cover letter and attach it to the records being returned. The memo should include the same information used to request the records. The CRMO or records requestor will notify RPDD when records are returned to the FRCs.

5. ACCESS TO FEDERAL RECORDS BY OTHER INDIVIDUALS. Access to federal records by individuals not employed by a WHS-serviced Component or an assigned service member of the Military Services such as historical researchers, former Presidential appointees, and non-DoD employees will be processed in accordance with Reference (q). WHS-serviced Components are not authorized to recall, retrieve, or duplicate records for these individuals.

# GLOSSARY

## PART I. ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| AI | Administrative Instruction |
| ACMO | Advisory Committee Management Officer |
| ARCIS | Archives and Records Centers Information System |
| | |
| CD | compact disk |
| CD-ROM | compact disk-read only memory |
| CIO | chief information officer |
| CFA | current files area |
| CFR | Code of Federal Regulations |
| CNWDI | Critical Nuclear Weapon Design Information |
| COTS | commercial off the shelf |
| CRMO | Component Records Management Officer |
| CY | calendar year |
| | |
| DA&M | Director of Administration and Management |
| DoDD | Department of Defense Directive |
| DVD | digital video disk |
| | |
| EIS | electronic information system |
| ESD | Executive Services Division |
| | |
| FACA | Federal Advisory Committee Act of 1972 |
| FOIA | Freedom of Information Act |
| FRC | Federal Records Center |
| FY | fiscal year |
| | |
| GC, DoD | General Counsel, Department of Defense |
| GRS | General Records Schedule |
| GSA | General Services Administration |
| | |
| IM | instant message |
| IT | information technology |
| | |
| NARA | National Archives and Records Agency |
| NATO | North Atlantic Treaty Organization |
| NIST | National Institute of Standards and Technology |
| | |
| PA | Privacy Act |
| PAS | Presidentially Appointed, Senate confirmed |
| PC | personal computer |
| PERM | permanent |

| | |
|---|---|
| POC | point of contact |
| RPDD | Records, Privacy, and Declassification Division |
| RL | records liaison |
| RMA | records management application |
| SF | standard form |
| SNS | social networking sites (also known as social media) |
| SORN | System of Records Notice |
| TEMP | temporary |
| URL | uniform resource locator |
| U.S.C. | United States Code |
| WHS | Washington Headquarters Services |

## PART II. DEFINITIONS

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

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.

accession number. The NARA or ARCIS assigned tracking number for the transfer of agency records to the National Archives or FRC (see Retirement and Transfer Number).

active records. See current records.

archival value. The determination by appraisal that records are worthy of permanent preservation by the Archivist of the United States. See historical value.

audiovisual files. Files in pictorial or aural form, regardless of format. Included are still photos, graphic arts such as posters and original art, motion pictures, video recordings, audio or sound recordings, microform, and related records.

block. A chronological grouping of records consisting of one or more segments of records that belong to the same series and are dealt with as a unit for efficient transfer, especially the transfer of permanent records to the NARA. For example, a transfer of records in 5-year blocks.

bucket or aggregate schedule. A type of flexible schedule. Flexible scheduling using big buckets or large aggregations is an application of disposition instructions against a body of

records grouped at a level of aggregation greater than the traditional file series or electronic system that can be along a specific program area, functional line, or business process.

case file. Files, regardless of media, containing material on a specific action, event, person, place, project, or other subjects. Sometimes referred to as a "project file" or a "transaction file." Also a collection of such folders or other file units.

case working files. Support files, such as worksheets, questionnaires, rough notes, calculations, are generally kept for a shorter period of time than the papers that serve to document the project. See working files.

central files. The files of several offices or organizational units physically or functionally centralized and supervised in one location.

CFA. The area where current records are physically maintained, usually in a location that provides convenient access for reference and retrieval.

chronological reading file. See reading file.

classified information. Information that has been determined pursuant to Reference (e) or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

closed file. A file unit or series containing documents on which action has been completed and to which additional documents are not likely to be added. A file unit or series to which access is limited or denied. See cut off.

COFF. Termination of files at specific intervals to permit transfer, retirement, or disposal in periodic (quarterly, semiannual, or annual) blocks. Sometimes called "file break." See also block.

cloud computing. A technology that allows convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Depending upon user needs, and other considerations, cloud computing services are typically deployed using one of the following four models as defined in "The NIST Definition of Cloud Computing" (Reference (y)):

private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated

by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

convenience file. Non-record copies of correspondence, completed forms, publications, and other information maintained for ease of access and reference. Sometimes referred to as "working files."

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, comeback copy, file 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.

cross-reference. A procedure used to show the location of a document that may be filed, because of content, under more than one subject.

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."

custody. The guardianship of records that in a strict sense includes both physical possession (protective responsibility) and legal title (legal responsibility). For example, OSD records transferred to an FRC are in the **physical possession** of that facility but legal title to them remains with the OSD and access may be granted only with the approval of the originating agency; when accessioned by the National Archives, legal title, and physical possession then pass to the Archivist of the United States, who may grant access without reference to the originating agency.

discontinuance. The placing of an organization in an inactive or surplus status. It includes inactivation, disbandment, discontinuance, or reduction to zero in strength.

disposal. Physical destruction of temporary records. See also disposition.

disposal authority. The legal authorization for the disposition of records obtained from the Archivist of the United States empowering an agency to transfer permanent records to the NARA and to carry out the disposal of temporary records. Also called "disposition authority."

disposition. Those actions taken regarding federal records after they are no longer needed in office space to conduct current agency business. Records disposition is any activity that includes:

Disposal of temporary records by destruction or donation;

Transfer of records to federal agency storage facilities or FRCs;

Transfer to the Archives of the United States, records determined to have sufficient historical or other value to warrant continued preservation; or

Transfer of records from one federal agency to any other federal agency.

disposition instruction. An instruction for the cut off, transfer, retirement, or destruction of documents.

disposition program. Practices designed to achieve efficient and economical disposition of records. The program involves developing standards, procedures, and techniques for managing the longevity of records. Includes controls over office filing equipment, scheduling records for disposition and administering their storage, documenting agency benefits accruing from the program, and undertaking surveys and audits of disposal operations.

disposition schedule. A document governing the continuing mandatory disposition of a record series of an organization or agency. Also known as a "records schedule," "records control schedule," "retention schedule," or "records retention schedule." The OSD Records Disposition Schedule contains the only authorized disposition schedule for OSD. See also GRS.

disposition standard. The time period for the cut-off transfer to a records center, destruction, or transfer to the NARA of a file series.

DoD Component. An organizational entity of the Department of Defense such as the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, and DoD Field Activities.

EIS. A system that contains and provides access to computerized federal records and other information usually dedicated to a business process and/or specific function(s).

electronic records. Records stored in a form that only a computer can process and satisfies the definition of a federal record, also referred to as machine-readable records or automatic data processing records.

e-mail system. A computer application used to create, receive, and transmit messages, and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain transmission data), data systems used to collect and process data that have been organized into data files or databases on either personal computers or mainframe computers, and word processing documents not transmitted with the message.

evidential value. The usefulness of records in documenting the organization, functions, and activities of the agency creating or receiving them. See historical value.

federal records. See record.

file. An accumulation of records or non-record materials arranged according to an approved plan. Used primarily in reference to current records in an office. A unit, such as a folder, microform, or electronic medium, containing records, non-records, or personal files. In electronic records, an organized collection of related data, usually arranged into logical records stored together and treated as a unit. The unit is larger than a data record but smaller than a data system and is sometimes known as a "data set." Referred to collectively as "files."

file inventory. A survey of agency records used to develop a disposition schedule. Includes a descriptive listing of each record series of a system, together with an indication of where it is located and other pertinent data.

finding aids. Indexes or other lists designed to make it easier to locate relevant files.

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.

frozen records. Those temporary records that cannot be destroyed on schedule because special circumstances, such as a preservation or court order, require a temporary extension of the approved retention period.

government control. The ability of the originating government agency to regulate access to documentary materials, especially classified information.

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 thereby. Exceptions may be granted only by the Archivist of the United States. The GRS does **not** apply to an agency's program records.

historical value. The usefulness of records for historical research concerning the agency of origin.

holding area. Agency space assigned for the temporary storage of active or semi-active records and for records with relatively short retention periods. Also known as a "staging area."

housekeeping records. Records of an organization that relate to budget, fiscal, personnel, supply, and similar administrative or support operations normally common to most agencies, as distinguished from records that relate to an agency's primary functions. (See GRS.)

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. The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated (EIS) or manual.

legal value. The use of records containing evidence of legally enforceable rights or obligations of government or private persons.

life cycle of records. The concept that records pass through three stages: creation/receipt, maintenance and use, and disposition. Records should be managed properly during all three phases of the life cycle.

metadata. Data describing the structure, data elements, interrelationships, and other characteristics of an electronic record. Usually described as data about the data.

microform. Any form containing greatly reduced images, or micro-images, usually on microfilm. Roll microforms include microfilm on reels, cartridges, and cassettes. Flat microfilms include microfilm jackets, aperture cards, and micro-cards, or micro-opaques.

non-record material. 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 record). 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. Catalogs, trade journals, and other publications that are received from other government agencies, commercial firms, or private institutions and that require no action and are not part of a case on which action is taken. (Stocks do not include serial or record sets of agency publications and processed documents, including annual reports, brochures, pamphlets, books, handbooks, posters and maps.)

official records. See records.

OSD functional file system. A system of files based on the major functions by which the records will be retrieved. With program records or mission-related files, these functions mirror the office organization and reflect the nature of the work being done there. The OSD uses a functional file system

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.

personal files (also referred to as personal papers). Documentary materials belonging to an individual that are not used to conduct agency business. Personal files are excluded from the definition of federal records and are not owned by the government. Personal papers are required to be filed separately from official records of the office.

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."

reading file. A file containing copies of documents, usually outgoing correspondence only which is arranged in chronological order --sometimes referred to as a "chron file," or "chronological reading file."

record copy. The official file or coordination copy created by an action office, complete with coordinations, enclosures, or related background papers that form a complete file or history of that action. Multiple copies of the same document(s) containing duplicative information may be considered a record copy within the organization depending on how they are used to conduct government business.

record group. A body of organizationally related records established by NARA to keep track of agency records during and after the scheduling process, including those transferred to FRCs or the National Archives. The record group for OSD is 330; other elements of the Department of Defense are assigned their own record group numbers.

records. (Also referred to as federal records or official records). The term "records" includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them; and 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.

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

records center. See FRC.

records center container. A corrugated cardboard box designed to hold one cubic foot of records, either legal or letter size, and used chiefly in records centers. These are the only containers authorized for shipment of DoD records to an FRC.

records control schedule. A listing prepared by each OSD office identifying the records series, filing arrangement, and ultimate disposition of all files maintained.

Records Disposition Schedule. Sometimes called a Records Control Schedule, Records Retention Schedule or a Records Schedule. 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.

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

records manager. The person responsible for or engaged in a records management program. Sometimes called “records officer” or “records administrator.”

reference copies. A collection of extra copies of official records on a specific action used for ready reference.

retention period. The time period that a specific series of records is to be kept. Also called “retention standard.”

retirement. The movement of inactive files having a permanent or long-term value to an FRC for storage, servicing, and ultimate disposition. See transfer.

screening. The examination of records to apply access restrictions and to determine the presence of extraneous material (extra copies, classified cover sheets, mail control forms, envelopes, routing slips (except those with remarks of significant value), blank forms, etc.) before filing, transfer, or retirement.

series. File units or documents arranged in accordance with an approved filing system. Also called “record series.”

structured data. Any data that has an enforced composition to the atomic data types. The data is managed by technology, which allows for querying and reporting. A database is structured data.

sustainable format. Means the ability to access an electronic record throughout its life cycle, regardless of the technology used when it was created. A sustainable format increases the likelihood of a record being accessible in the future.

technical reference files. Extra copies of articles, periodicals, reports, studies, vendor catalogs, and similar materials that are needed for reference and information and are properly a part of the office's records.

temporary records. Records designated for retention for a specified period of time and then authorized to be destroyed in the CFA area. Temporary records are most commonly found among housekeeping records and administrative files.

transfer. The movement of records out of office space to a depository but not necessarily an FRC. (See retirement.)

transfer number. The control number given to any OSD functional element retiring records to an FRC. This number consists of the Record Group number, fiscal year in which the number was issued, and a four-digit sequential control number, also referred to as accession number. The transfer number is the basic reference for any records shipment and must be used when retrieving papers from any FRC. Transfer numbers are issued by ARCIS and controlled by RPDD.

transitory record. Records of short-term interest (180 days or less), including in electronic form (e.g., e-mail messages), which have minimal or no documentary or evidential value. The format or media of the record does not dictate its record value.

unscheduled records. Records whose final disposition has not been approved by the Archivist of the United States.

unstructured data. Any data stored in an unstructured format at the atomic level. Refers to computerized information which does not have a data structure that is easily readable by a machine and requires human intervention to make the data machine readable. Examples of unstructured data are e-mail, spreadsheets, or word processing documents.

vital records. Documents essential to the continued functioning or reconstitution of an organization during and after an emergency and also those documents essential to protecting the rights and interests of that organization and the individuals directly affected by its activities. Sometimes called "vital files" or "essential records." Includes both emergency-operating and right-and-interests records that are duplicates or extra copies of originals stored off-site.

Washington National Records Center. The official off-site repository for OSD records located at Suitland, Maryland.

web site. Web sites are a collection of interconnected web pages consisting of a homepage, images, videos, or other digital assets that are addressed relative to a common URL, often consisting of only the domain name, or the IP address, and the root path ('/') in an Internet

Protocol-based network. They are generally located on the same server, and prepared and maintained as a collection of information by a person, group, or organization.

working files. Documents such as rough notes, calculations, or drafts assembled or created and used in the preparation or analysis of other documents. In electronic records, temporary files in auxiliary storage. May also include non-record material and technical reference files.