# OFFICE OF THE SECRETARY OF DEFENSE

## RECORDS AND INFORMATION MANAGEMENT PROGRAM

# PRIMER

## Table of Contents

## SECTION 1:

## 1.0. AUTHORIZATION

a. The policies and procedures dictated in this Procedural Resource and Instructional Manual (PRIMER) are issued in accordance with:

(1) Title 44, United States Code (USC), Chapter 31 “Records Management by Federal Agencies”

(2) Title 44, United States Code (USC), Chapter 33 “Disposal of Records”

(3) 36 Code of Federal Regulations (CFR); Chapter XII “National Archives and Records Administration”; Subchapter B “Records Management”

b. Assignment of Records and Information Management (RIM) roles and responsibilities are issued per:

(1) Department of Defense (DoD) Issuance (DoDI) 5015.02, “DoD Records Management Program”

(2) DoDD Directive (DoDD) 5110.04, “Washington Headquarters Services”

(3) Administrative Instruction (AI) 15, “OSD Records and Information Management Program”

c. Issuance of this web publication establishes administrative procedures regarding implementation of a lifecycle management of records and information program within the Washington Headquarters Service (WHS)-serviced Components (see Section 2.0 Scope).

d. Revisions to this document will be issued periodically by the Office of the Secretary of Defense (OSD) RIM Program, as managed by the WHS/Records and Declassification Division (RDD), reflecting changes to policy, procedures, or responsibilities.

SMITH.JOHN.D.
1404592560

Digitally signed by
SMITH.JOHN.D.1404592560
Date: 2023.12.14 17:18:44
-05'00'

John D. Smith
Chief, Records and Declassification Division,
Executive Services Directorate,
OSD Records Administrator
Washington Headquarters Services (WHS)

Digitally signed by
IRVINE.DARREN.LYNN.
1049959130
Date: 2023.12.14
14:50:43 -05'00'

Darren Irvine
Director, Executive Services Directorate,
OSD Senior Agency Official for Records
Management (SAORM)
Washington Headquarters Services (WHS)

**SECTION 2:**

## 2.0. SCOPE

a. The OSD PRIMER provides in-depth guidance to the OSD Components serviced by the OSD RIM program, (cited as the “WHS-serviced Components”) on the implementation and compliance of Federal law, regulations, DoD RIM directives and issuances, specifically as they relate to:

(1) Management of records throughout their lifecycles, to include record creation, maintenance, use, and disposition.

(2) Implementation of Electronic Records Management (ERM) requirements into Federal Information Systems (FIS).

(3) Development of file plans.

(4) Implementation of paper and electronic folder structures.

(5) Completion of RIM web-based or classroom training.

(6) Transfer of permanent records to the National Archives and Records Administration (NARA) and temporary or permanent records to a Federal Records Center (FRC), such as the Washington National Records Center (WNRC).

(7) Conversion of paper records to digital images

(8) Administration of social media content, web 2.0 technologies, text messages, e-messaging accounts, messaging services provided on mobile devices, third-party applications, encrypted communications, messaging applications, and direct messages on social media platforms.

b. WHS-serviced Components. No one person or unit can be directly responsible for all the records created within a WHS-serviced Component. Therefore, every office, division, directorate, or department creating and receiving OSD records and information is responsible for:

(1) Implementing RIM practices consistent with this PRIMER and AI 15.

(2) Educating staff in RIM practices.

(3) Preserving records as required in accordance with their approved disposition authorities.

(4) Properly disposing of inactive records at the end of the applicable retention periods.

(5) Protecting records and information against misuse, misplacement, damage, loss, destruction, or theft.

(6) Monitoring compliance with AI 15.

c. List of WHS-serviced Components:

| **(1) OSD PRINCIPAL STAFF** |
|---|
| **Secretary of Defense/Deputy Secretary of Defense** |
| **Under Secretary of Defense for Research & Engineering (USD(R&E))** |
| **Under Secretary of Defense for Acquisition & Sustainment (USD(A&S))** |
| **Under Secretary of Defense for Policy (USD(P))** |
| **Under Secretary of Defense for Comptroller/Chief Financial Officer (USD(C)/CFO))** |
| **Under Secretary of Defense for Personnel and Readiness (USD(P&R))** |
| **Under Secretary of Defense for Intelligence and Security (USD(I&S))** |
| **Assistant Secretary of Defense for Legislative Affairs (ASD(LA))** |
| **Assistant to the Secretary of Defense for Public Affairs (ATSD(PA))** |
| **Assistant to the Secretary of Defense for Privacy, Civil Liberties and Transparency (ATSD(PCLT))** |
| **Director, Cost Assessment and Program Evaluation (DCAPE)** |
| **General Counsel, DoD (GC, DoD)** |
| **Director, Net Assessment (DNA)** |
| **Director, Administration and Management (DA&M)** |
| **Director, Operational Test and Evaluation (DOT&E)** |
| **Chief Data and Artificial Intelligence Officer (CDAO)** |
| **DoD Chief Information Officer (DoD CIO)** |
| **(2) DEFENSE AGENCIES** |
| **Defense Advanced Research Projects Agency (DARPA) via USD(R&E)** |
| **Defense Health Agency (DHA) via USD(P&R)/ASD(HA)** |
| **Defense Legal Services Agency (DLSA) via GC, DoD** |
| **Defense POW/MIA Accounting Agency (DPAA) via USD(P)** |
| **Defense Security Cooperation Agency (DSCA) via USD(P)** |
| **Pentagon Force Protection Agency (PFPA) via DA&M** |
| **(3) DEFENSE SCHOOLS** |
| **Defense Acquisition University (DAU) via USD(A&S)** |
| **Defense Information School (DINFOS) vs ASD(PA)/DMA** |
| **Department of Defense Education Activity (DoDEA) via USD(P&R)** |
| **Uniformed Services University of the Health Sciences (USUHS) via USD(P&R)** |
| **Defense Institute of Security Cooperation Studies (DISCS) via USD(P)** |
| **Defense Institute of International Legal Studies (DIILS) via USD(P)** |
| **(4) DoD FIELD ACTIVITIES** |
| **Defense Media Activity (DMA) via ATSD(PA)** |
| **Defense Office of Hearings and Appeals (DOHA) via GC, DoD** |
| **Defense Technology Security Administration (DTSA) via USD(P)** |

| |
|---|
| **Defense Human Resources Activity (DHRA) via USD(P&R)** |
| **Test Resource Management Center (TRMC) via USD(R&E)** |
| **Office of Local Defense Community Cooperation (OLDCC) via USD(A&S)** |
| **Washington Headquarters Services (WHS) via DA&M** |
| **Office of Military Commissions (OMC) via GC, DoD** |

## SECTION 3:
## 3.0. RESPONSIBILITIES

Sections 2 and 3 of AI 15 provides an overview of the duties and responsibilities for the:

a. Heads of WHS-serviced Components.

b. OSD Senior Agency Officials (SAOs).

c. CIO/IT Staff of WHS-serviced Components.

d. WHS-serviced Component acquisition and procurement officers.

e. OSD employees of WHS-serviced Components (including civilians, contractors, and military service members).

f. OSD Component Records Management Officers (CRMO), Defense Agency/DoD Field Activity (DAFA) Records Managers (RMs), and DoD Advisory Committee RMs.

SECTION 4:

## 4.0. IMPLEMENTATION OF OSD RIM PROGRAM

### 4.1. PURPOSE

a. The purpose of the OSD RIM Program is to ensure each WHS-serviced Component is retaining records and information needed to preserve aspects of its institutional memory, history or to meet current and future business and operational requirements by:

(1) Documenting past and present decisions and activities.

(2) Implementing systematic mechanisms to destroy records no longer necessary.

(3) Retaining records in context of missions, programs, and functions.

(4) Complying with legal or statuary requirements.

b. While wide swaths of information WHS-serviced Components create and receive are legally considered records, not everything has long-term institutional value. Therefore, the RIM Program assists in developing and educating WHS-serviced Components on the value of information created and received.

c. RIM fundamentals apply to both individual documents and multi-documents (case files) that make up program, mission, fiscal, legal, and administrative files. Records basically refer to document(s) created, sent, or received that are used for the execution of the day-to-day activities of OSD employees, contractors, or service members regardless of format. You may often refer to them as:

| | | |
|---|---|---|
| Contracts/agreements | Applications | Surveys |
| Reports | Issuances | Databases |
| Personnel files | Information collections | Correspondence |
| Forms | Invoices/receipts | Press releases and speeches |
| Training coursework | Meeting minutes | Maps and architectural drawings |

d. In addition to identifying records of institutional value, RIM provides WHS-serviced Components with a broader utility regarding implementing governance, managing risk, and ensuring compliance with other regulations such as the Privacy Act of 1974 (5 USC § 552), and the Paperwork Reduction Act (44 USC §§ 3501–3521). RIM is primarily concerned with managing the evidence of an organization's activities as well as the reduction or mitigation of risk associated with the management of OSD records and information.

e. To document the transactions of federal business and missions, federal regulations and DoD policies require that federal records are created, maintained, used, and preserved or disposed.

f. Records management is not just a federal requirement that ensures the mission and actions of federal offices are suitably documented. It is also a wise business investment to optimize productivity and support better decision-making.

g. The maintenance of OSD records and information depends on establishing continuous and systematic control over the creation, maintenance, use, and disposition (i.e., preservation or disposal) of agency records and information, in accordance with 44 USC Chapter 3101; 31, 44 USC Chapter 33; and 36 CFR § 1220-1249.

h. The establishment and maintenance of an organization's records begins with identifying what program and missions the offices within each Component or directorate support. Maintenance of records, including proper filing and setup of proper filing structures for electronic and paper records, all assist with keeping the files orderly and easily retrievable regardless of media, location, classification, or format. Finding aids assist in retrieving the files, charging them out, and performing disposition (transferring permanent or destroying temporary inactive files) in accordance with approved disposition schedules regardless of media, classification, and format.

## 4.2. IDENTIFYING AGENCY RECORDS

a. As previously stated, not everything an organization creates, sends, and receives meets the criteria for being considered a record. This section will assist WHS-serviced Components with distinguishing their organization's records from non-records and personal materials. Agency records can be broken down into four primary groups: (1) administrative, (2) program/mission/operational, (3) financial, and (4) legal.

(1) Administrative records consist of documents that facilitate the administrative (sometimes called housekeeping) operations and management of an agency, department, or office. These may include, but are not limited to:

| |
|---|
| Postal/mail (digital and hardcopies) |
| Hours of duty/schedules |
| Access and recall rosters |
| Security logs |
| Training Requests |
| Completed forms (those on placed on safes, cabinets, or vaults containing classified documents, equipment listings, travel claims, purchase requests, network access requests, etc.) |
| Purchase of supplies (paper, printer cartridges, folders, etc.) |
| Hand receipts, or comparable documents showing accountable property charged to the office |
| Orientations and briefings given to visitors and newly assigned personnel |
| Documents used in accounting for office personnel and management of employees |

(2) Program/mission/operational records consist of documents directly related to the mission of the group, office, division, etc., as defined by federal law (e.g., 10 USC §131 - Office of the Secretary of Defense), DoD issuance (e.g., DoD Directive (DoDD) 1145.02E - United States Military Entrance Processing Command (USMEPCOM), or regulations (e.g., National Defense Authorization Act (NDAA) 2019). These may include, but are not limited to:

| |
|---|
| Enabling legislation - including the development of formal regulations |
| The issuance of policy that prescribe procedures or effect organizational structures |
| Relations with the White House, Executive Office of the President, Congress, or the public including Congressional hearing statements, transcripts, and correspondence |
| Foreign affairs; including treaties, agreements, testimony, international disputes, military aid |
| Litigations and formal legal opinions |
| Documents directly related to the mission of special projects, commissions, councils, conferences, panels, task forces, or other similar groups special programs, initiatives, studies, etc. |
| Agreements (memoranda of agreement (MOA), memoranda of understanding (MOU), and similar documents) between the OSD Components and the Military Services, the Defense Agencies, Federal Agencies, or non-Federal organizations or agencies |
| Early warnings of incidents, potential threats, and situation estimates that are obtained from Federal, State, or local investigative or law enforcement agencies |
| Documents that develop, coordinate, and promulgate intelligence and intelligence-related planning and programming at the OSD-level |
| Documents directly related to the mission of military such as construction programs and operation and equipment maintenance programs |

(3) Financial records that have fiscal value relate to an agency's financial transactions. These may include but are not limited to:

| |
|---|
| Budgets, to include all preliminary budget estimates, justifications, cost statements, narrative statements, rough data formulation and execution documentation, and similar materials |
| Payroll, to include audit and inspection reports |
| Contracts, to include requisitions, purchase orders, and interagency agreements |
| Accounting records, to include appropriation, apportionment, and allotment files |
| Disbursement schedules and vouchers |
| Statements of transactions, such as cash register transaction records, credit card and charge cards receipts |
| Sale of excess and surplus personal property, such as fee or rate schedules and supporting documentation and out-leases of federal property |
| Fee and fine collection records, garnishment |

(4) Legal records consist of documents that chronicles or formally expresses a legally enforceable act, process, or contractual duty, obligation, or right, and therefore evidence that act, process, or agreement, i.e., with evidence of legally enforceable rights or obligations of the federal government. These may include, but are not limited to:

| |
|---|
| Records relating to property rights, including land, probate, contracts, agreements, leases, licenses |
| Records relating to citizenship rights, including vital statistics (birth, death, marriage), some legal proceedings, and criminal cases |
| Records relating to employment, such as veterans' records involving legal rights attached to employment, benefit rights, basic state personnel records, and, in some cases, payroll records |
| Records containing information required to protect the federal government against claims or to enforce statutes: executive orders, rules, regulations, and records to establish or support judicial opinions and interpretations |
| Records produced at the behest of a legal statute, such as Freedom of Information Act (FOIA), Privacy Act (PA), Federal Advisory Committee Act (FACA), statutes specifically mandating reports, etc. |
| Formal legal decisions and legal advice records |
| Records relating to criminal and civil investigations |

### 4.3. RECORD VALUE

a. There are three categories of record value: temporary, permanent, and unscheduled (see Section 12 for glossary). 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 administrative records for instance) are important, although they have no historical value, as they are needed for extended periods to meet operational, legal, or administrative needs.

(1) Temporary records are those NARA appraised and approved for destruction after a specified time or event.

(2) Permanent records are those NARA appraised to have sufficient historical value or other value to warrant continued preservation by the Federal Government beyond the time they are needed for administrative, legal, or fiscal purposes.

(a) Permanent records can be created at all levels within an organization, but usually document OSD/DoD-Wide Programs or initiatives.

(b) Permanent records will be transferred into the legal and physical custody of the National Archives of the United States after their retention period ends.

(3) Unscheduled records are those yet to be determined to be permanent or temporary. Until the final disposition of these records is approved by NARA, unscheduled records must be maintained as permanent records. If you receive or use information that cannot be characterized

by a records schedule, report it to your CRMO/DAFA RM so that they can propose a new schedule to the OSD RIM Program for NARA's approval.

b. The Federal Records Act requires each office within OSD to identify, manage, and disposition the records and information it creates and receives. A byproduct of this requirement may require the retention of copies (duplicates of the same record) at multiple levels within a WHS-serviced Component as a fundamental part of a RIM program.

(1) Although a copy of a record may be retained at multiple levels, it does not necessarily keep the same value. Understanding the role each individual office, program, or mission plays within the Component helps to define the value of the records it manages. This understanding assists action officers, program leads, records liaisons (RLs), and custodians in selecting the appropriate file number to apply to its records and information.

(2) An example is the annual FOIA report the DoD Components' Privacy Act Officers submit to ATSD(PCLT).

(a) Many lower echelon offices throughout DoD submit these reports to higher headquarters. The higher headquarters offices consolidate and submit to ATSD(PCLT), which then further consolidates for submission to the Department of Justice (DOJ).

(b) In this example, DOJ maintains a complete record of all Federal Agency inputs. The generated report and this complete record case file has a higher value than the feeder elements used to create the complete record set. Therefore, the feeder reports consolidated by each Component's Privacy Act Program Office for submittal to ATSD(PCLT) will not have the same informational value as the consolidated report created from the feeder reports.

## 4.4. BASIC RECORDKEEPING PRACTICES

a. Good recordkeeping is required to effectively manage, locate, and arrange records, and facilitates their creation, use, and disposition. Primary considerations include managing access, minimizing duplication, preserving permanent records, and systematically disposing of temporary records according to the disposition instructions listed under its applicable file number in the OSD Records Disposition Schedules (RDS). The factors that must be considered in the storage and maintenance of records are:

(1) Access. Records will be kept sufficiently accessible to make maintenance of duplicate files unnecessary and to facilitate operations.

(2) Security. Classified material maintained in security containers or secured areas must be managed to prevent or minimize incursions and/or interference, in accordance with DoD 5200.08-R, while access to Controlled Unclassified Information (CUI), including personally identifiable information (PII), is restricted on a need-to-know basis, in accordance with Volumes 1-3 of DoD Manual (DoDM) 5200.01, The Privacy Act of 1974, DoD 5400.11-R, and 32 CFR § 2002.

(3) Space. When maintaining paper or electronic records, adequate space must be reserved for present and anticipated needs, factoring in the safety and health of office personnel in accordance with DoDM 4140.70 for paper records. Additionally, offices storing large quantities of paper records must meet fire protection requirements, and transition to paperless environments in accordance with the requirements in Office of Management and Budget (OMB)/NARA Memorandum M-23-07.

(4) Media. Retention period of the records will be considered when selecting the storage media for paper or electronic records. Retention of permanent records in electronic formats must comply with the requirements in 36 CFR § 1236 and Section 6 of this PRIMER.

(5) Arrangement.

(a) Arranging records, regardless of media and format, aids in retrieving active and inactive files, sharing of information, and dispositioning of inactive files in accordance with approved file numbers from the RDS. When arranging records there are generally two types:

(1) A centralized filing system is one in which the records for several people or units are in one, central location and, under the control of records personnel or in the case of large, centralized filing systems, several people.

(2) A decentralized filing system is one in which the files are located throughout the office, generally at individual workstations, and usually controlled by the person who creates and/or receives them.

(b) Organizations and personnel must make every effort to ensure records are arranged in a logical context relating to the program, mission, or function in which they are created or received. This includes, but is not limited to, forms, surveys, spreadsheet, drafts, and working papers created, received, or collected to document OSD functions such as:

(1) The development, implementation, or oversight of legal and regulatory requirements.

(2) Creation or decommissioning of business functions, activities and transactions or work processes.

(3) Acquisition of FIS, applications, technologies, or business systems.

(4) Processes contracted to third party providers, vendors, service level agreements.

(c) To prevent illicit acquisition of or unauthorized access classified files and containers will be located away from windows and doors (for paper records) or maintained on approved secure networks (for electronic records), in accordance with 18 USC §§ 641 and 2071.

(d) Files containing classified North Atlantic Treaty Organization (NATO) material, Alternative Compensatory Control Measures (ACCM), or Special Access Program (SAP) must be maintained separately from other classified material in accordance with United States Security Authority for NATO (USSAN) Instruction 1-07 and DoDM 5200.01 Volumes 1-3. Components must handle files containing privacy information in accordance with DoD 5400.11-R.

## 4.5. OSD NUMERIC FILING SYSTEM

a. The OSD numeric filing system, reflected in the OSD RDS, ensures all records, regardless of media or format, are consistently housed, identified, and maintained so that they can be retrieved using standard equipment, practices, and procedures.

b. The OSD RDS resides on the WHS Executive Services Directorate (ESD) website at the OSD RDS is the only filing system authorized for the WHS-serviced Components. Modification of the numbering system is not permitted.

c. The OSD RDS documents the major records or subject matter related to the activities of each office. It identifies temporary and permanent records and provides mandatory instructions for the retention and disposition (retirement or destruction). All records disposition schedules are approved by the Archivist of the United States.

d. The OSD RDS is arranged in a hybrid functional and organizational file system. The implementation of the schedule, however, is based on function.

e. The OSD RDS applies to all records and information, regardless of media classification and format. Excluded are publication stock copies of publications, blank forms, personal papers, books in designated libraries, museum materials intended for exhibition purposes and reproduction material, such as stencils and offset masters; these are all considered non-record material.

## 4.6. UNDERSTANDING THE OSD RDS

a. The OSD RDS provides for the identification of records and information and defines how records should be managed until their eventual destruction or transfer. The OSD RDS is organized by series, starting with 100 and 200, which contain the most common administrative and human resources records created by all OSD Components, Defense Agencies and Field Activities. The 300 through 2200 series are assigned to specific OSD Components and their Defense Agencies/Field Activities. These series identify and identifies their mission, functional and program records.

b. The OSD RDS is set up functionally (i.e., by subject matter) and consists of 3 levels: Record Series (100, 200, 300, etc.), Records Category (101, 202, 305, etc.) and File Number (101-01.1, 202-70, etc.). Record series, categories, and file numbers are the itemization of subject matter records created or received by WHS-serviced Components.

(1) The Record Series level contains Series Title, Series Description, and inclusive Components/DAFAs. The Record Series is indicated by a numerical designation (e.g., 500)

while the Series Title and Series Description outlines the overall subject matter of the records therein.

(2) Following the description is a list of inclusive Components/DAFAs which are authorized to use the file numbers within the series.

c. Examples of the record series with their numerical designations are listed in Table 1 below.

| Example Record Series | Example Record Series Title |
|---|---|
| 100 Series | General Office Records |
| 200 Series | Management and Operations |
| 300 Series | USD(Comptroller) |
| 400 Series | DoD General Counsel |

Table 1. Example of Records Series

d. These record series are further divided into Records Categories, examples depicted in Table 2, that identify the subject matter or mission and program name of a set of records and information within the Category. Each Records Category lists the Category Title and Description about the types of records listed in the Category.

| Example Records Category | Example Function/Subject Matter |
|---|---|
| 202 | Office Personnel Files |
| 203 | Information Management Files |
| 204 | Space Management and Service Files |

Table 2. Example of Records Categories

e. Each files series is divided into applicable file numbers, examples of which are contained in Table 3. The file number is usually five digits, where the first three digits indicate the Records Category Number, followed by a dash and a sequential two-digit number, such as 01. In some cases, a sequential number is further divided by a decimal followed by a number, such as .1.

| Example File Number | Example File Title |
|---|---|
| 201-01.1 | Organization Planning Files |
| 303-06 | Research and Development Investment Files Prior to FY 2017 |
| 1203-03.2 | Construction Operations Files – Surveillance or Acquisition |

Table 3. Examples of File Numbers

(1) File numbers contain a file title, description, cutoff, retention and disposition instructions, legal authorities, and whether a Privacy Act (PA) system of records notice (SORN) is applicable.

(2) File numbers in the 100 and 200 series are common to most OSD Component and DAFA offices, but they also contain the mission records of several specific Components such as

the Immediate Offices of the Secretary of Defense, WHS, DA&M, and PFPA. Each office identifies their specific file numbers based on their overall duties and responsibilities.

(3) Per 36 CFR 1225.22, every five years, each organizational unit within the OSD Component and DAFA office will review the functions, subject matter, and programs it is primarily responsible for to identify the corresponding file numbers from the OSD RDS.

## 4.7. FILE PLANS

a. The file plan provides a comprehensive system of identification, maintenance, and disposition of all records and information created or received within an organizational unit. Every office within an OSD Component or DAFA, shall have a file plan documenting the records accumulated and used in performing its functions.

(1) File plans will be updated at least annually, to include approval by the CRMO/DAFA RM. File plans may need updating more frequently if the physical or digital location moves, other information requires updating, or in cases where the office restructures (gaining or losing a mission or program).

(2) During annual reviews of file plans RIM personnel will ensure:

(a) File plans reflect file numbers contained in the most current version of the OSD RDS available on the OSD RIM Program website.

(b) File numbers are added, changed, or deleted, as needed when office functions change.

(c) All applicable locations of paper or electronic records are updated and accurate.

b. At a minimum, each file plan must identify the information listed in Figure 1. Additional information may be added as it suits the business needs of the applicable office, such as examples, name of the office records liaison or custodian, volume, or date range of the records.

| File Number | Title and File Description | Cutoff, Retention, and Disposition Instructions | Disposition Authority Number | Records Classification | Essential (Vital) (y/n) | Media (Paper or Electronic) | Privacy Act, (SORN) Number, if applicable | Location(s) of the records (Paper or Electronic) |
|---|---|---|---|---|---|---|---|---|

Figure 1: Minimum File Plan Elements

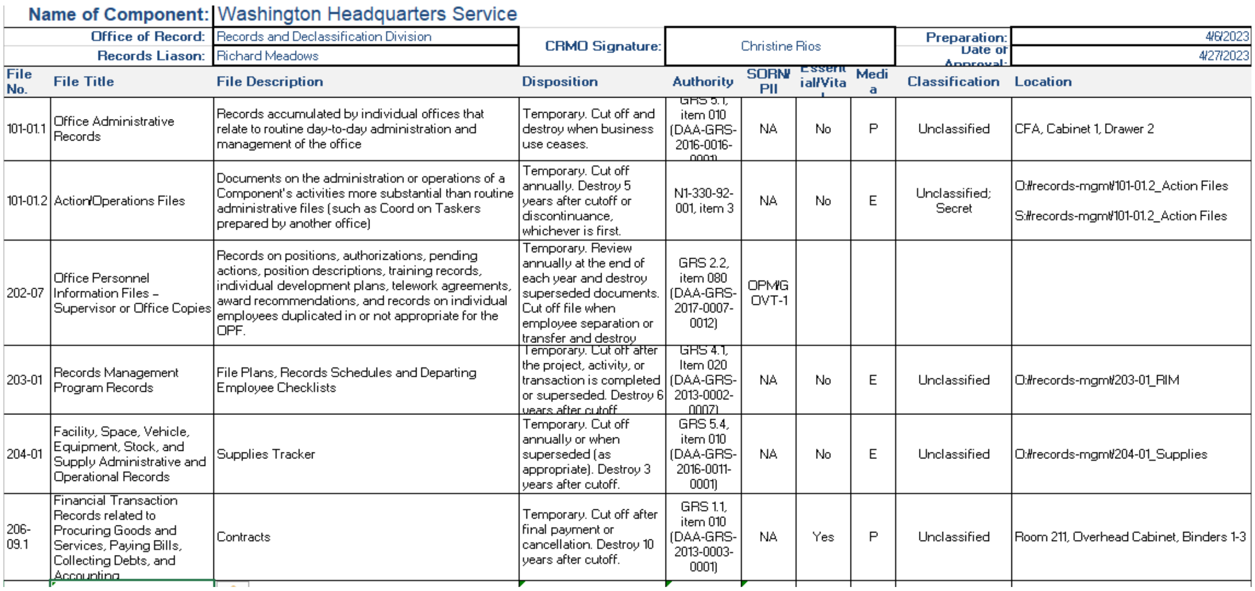
(1) In the file plan, the file number, file title, and disposition authority number must be cited exactly as written in the OSD RDS (no changes are permitted). The file description may be summarized and abbreviated, however, due to the length of the description and/or to provide efficiencies in the application of the file number to the files in their office. Cutoff, retention, and disposition instructions must match the OSD RDS, but can be abbreviated (e.g., “Temporary. COFF CY, DEST 5 yrs. after COFF” or “Permanent. COFF CY, TFR to NARA 25 yrs. after COFF”). Note: it is recommended all OSD Component/DAFA, use the Joint Publication 1-02, also known as DoD Dictionary of Military and Associated Terms, to standardize abbreviations.

(2) The notation in the Location column must be specific enough for users to locate the records and must include all locations where records associated with that file number are stored, regardless of media or file format (i.e., all networks, file cabinets, FIS, etc.).

(3) Records and information containing National Security Information (NSI) maintained on the Secret Internet Protocol Router Network (SIPRNet) or the Joint Worldwide Intelligence Communications System (JWICS) network can be documented within the Classification column by denoting the highest classification level, and by adding all network locations in the Location column with spaces between each. Alternatively, offices may choose to maintain a separate file plan for each network.

(4) File plans containing NSI according to security classification guides must be treated as classified documents, and handled in accordance with Executive Order 13526, DoDI 5200.01, DoDM 5200.01 Volumes 1-3, and DoDD 5205.07. This may include classified titles and/or SIPR/JWICS file paths when classified information is present in the file path.

c. RLs will forward a copy of the file plan to their CRMO or DAFA RM for review and approval. RIM personnel will retain a record of all approved file plans. Reporting offices will ensure copies of the file plan(s) are accessible to all employees, service members and contractor personnel. An example file plan is included in Figure 2.



| | | | | |
|---|---|---|---|---|
| Name of Component: | Washington Headquarters Service | | | |
| Office of Record: | Records and Declassification Division | CRMO Signature: | Christine Rios | Preparation: 4/6/2023 |
| Records Liason: | Richard Meadows | | | Date of Approval: 4/27/2023 |

| File No. | File Title | File Description | Disposition | Authority | SORN/PII | Essential/Vital | Media | Classification | Location |
|---|---|---|---|---|---|---|---|---|---|
| 101-01.1 | Office Administrative Records | Records accumulated by individual offices that relate to routine day-to-day administration and management of the office | Temporary. Cut off and destroy when business use ceases. | GRS 5.1, item 010 (DAA-GRS-2016-0016-0001) | NA | No | P | Unclassified | CFA, Cabinet 1, Drawer 2 |
| 101-01.2 | Action/Operations Files | Documents on the administration or operations of a Component's activities more substantial than routine administrative files (such as Coord on Taskers prepared by another office) | Temporary. Cut off annually. Destroy 5 years after cutoff or discontinuance, whichever is first. | N1-330-92-001, item 3 | NA | No | E | Unclassified; Secret | O:/records-mgmt/101-01.2_Action Files<br>S:/records-mgmt/101-01.2_Action Files |
| 202-07 | Office Personnel Information Files – Supervisor or Office Copies | Records on positions, authorizations, pending actions, position descriptions, training records, individual development plans, telework agreements, award recommendations, and records on individual employees duplicated in or not appropriate for the OPF. | Temporary. Review annually at the end of each year and destroy superseded documents. Cut off file when employee separation or transfer and destroy | GRS 2.2, item 080 (DAA-GRS-2017-0007-0012) | OPM/GOVT-1 | | | | |
| 203-01 | Records Management Program Records | File Plans, Records Schedules and Departing Employee Checklists | Temporary. Cut off after the project, activity, or transaction is completed or superseded. Destroy 6 years after cutoff | GRS 4.1, Item 020 (DAA-GRS-2013-0002-0007) | NA | No | E | Unclassified | O:/records-mgmt/203-01_RIM |
| 204-01 | Facility, Space, Vehicle, Equipment, Stock, and Supply Administrative and Operational Records | Supplies Tracker | Temporary. Cut off annually or when superseded (as appropriate). Destroy 3 years after cutoff. | GRS 5.4, item 010 (DAA-GRS-2016-0011-0001) | NA | No | E | Unclassified | O:/records-mgmt/204-01_Supplies |
| 206-09.1 | Financial Transaction Records related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting | Contracts | Temporary. Cut off after final payment or cancellation. Destroy 10 years after cutoff. | GRS 1.1, item 010 (DAA-GRS-2013-0003-0001) | NA | Yes | P | Unclassified | Room 211, Overhead Cabinet, Binders 1-3 |

Figure 2: Example File Plan

## 4.8. FILING ARRANGEMENTS

a. The arrangement of records is a multi-step process and must be based on your organization and its business or operational needs. The first step is deciding which filing system meets your components' requirements. Examples include but are not limited to:

(1) Centrally locating specialized files of Component-wide interest and use.

(2) Establishing centralized or decentralized filing systems.

(a) A centralized filing system is one in which the records for several people or units are in one, central location.

(b) A decentralized filing system is one in which the files are located throughout the office, generally at individual workstations, and usually controlled by the person who creates and/or receives them.

b. After deciding on an overall filing system, the next step in arranging a group of files is to determine the records series that applies (i.e., 100, 200, etc.). After selecting the record series, select the applicable file numbers relevant to the records created, sent, or received by the office. Once the applicable file number is selected, select a method of arranging the records within each file number based on the primary function by which the file will be recalled. Files can be further arranged in one or a combination of the filing arrangements listed in the following paragraphs, depending upon the business or reference needs of the office:

(1) 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 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 files that are broken down into policy, instruction, agreement, committee, staff visit, and reference subject categories.

(2) Case or Project Files. Case files may cover one or several subjects that relate to a particular case, program, or project but must always be filed by a specific title or number. 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. Other examples of case files include an official personnel file, or a case file associated with creating (or revising) policy. Case filing is the most efficient method for the maintenance of large quantities of records when:

(a) 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.

(b) Case or project files are closed upon the 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, approval/finalization of a policy, or project completion.

(c) 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 or recall. This system is useful for keeping records in small, manageable groups, usually by year, month, and day. Reading files and suspense files are examples of this type of filing arrangement. The use of chronological filing arrangements does not necessarily correlate to the disposition for chronological files in the OSD RDS (File number 102-16 – Office Chronological Reading Files). Incorrect use of this arrangement can lead to misfiling.

d. Other file arrangements include:

(1) Numerical Arrangement. Files identified and retrieved by a number, such as a contract number, purchase order, or requisition number.

(2) Alphabetical Arrangement. Files identified and retrieved by title, subject, task, or project.

(3) Name. Files arranged by companies, organizations, or agencies. Note: Arranging files using the personally identifiable information of an employee, contractor or service member is only authorized in compliance with the Privacy Act.

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

(5) Functional Arrangement. Files identified and retrieved by the function to which the information relates, and not necessarily the subject.

## 4.9. STATUS OF RECORDS

a. 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 have a record status depending on how they are used by the Component (or office) to conduct business. For example, a report commissioned by a contract with a USD(R&E) office may be stored in that office under two (or more) file numbers: for documentation of contractual requirements submitted by contractors under file number 206-09.1 (Financial Transaction Records related to Procuring Goods and Services, Paying Bills, Collecting Debts, and Accounting), and for plans for the allocation of development resources under file number 1308-01 (Air Warfare Files).

b. Working Papers or Files. Components must be mindful of drafts and working papers or files. Offices must ensure they maintain the documentation of proposals, evaluations, legal opinions, and other alternatives created to justify decisions even if these documents are drafts/working copies.

(1) In accordance with 36 CFR § 1222.12, offices must maintain working files and similar materials as records for purposes of adequate and proper documentation, if they:

(a) Are or 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.

(b) 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. These include, but are not limited to, reports, special studies, memoranda, issuance case files, and correspondence that support major program policy development that should be incorporated into program or mission files.

(2) Working papers or files can contain:

(a) Rough notes, calculations, or drafts assembled or created and used to prepare or analyze other documents or content.

(b) Mid- and high-level policies and decisions, policy formulation, execution and support documents used in preparing reports or studies, and preliminary drafts of policy or documents not circulated for comment.

c. Reference Files. Sometimes referred to as convenience copies or working papers, these are duplicate files of records preserved elsewhere or publications necessary for the execution of the roles and responsibilities of the office or position that are used purely for reference purposes. Review these files periodically to retain only those that are current and of significant reference value in accordance with the OSD RDS.

## 4.10. RECORDS OF CAPSTONE OFFICIALS.

a. Capstone is a simplified and automated approach to managing e-mail and text messages, as opposed to using either print and file systems or records management applications that require staff to file e-mail/text records individually. Using this approach, OSD can categorize, and schedule e-mail and text messages based on the work and/or position of the account owner.

b. Capstone officials' titles may vary by Component; they include, but are not limited to, the Secretary of Defense, Deputy Secretary of Defense, Under Secretaries of Defense, Assistant Secretaries of Defense, and the Directors or heads of OSD Components and DAFAs.

c. The records of Capstone officials generally fall into four major categories:

(1) Major Functions of OSD. This includes documentation of the development, supervision, and evaluation of each OSD Component's major substantive functions; formal legal opinions relating to major functions; case files, special studies of precedential significance concerning policy formulation; and annual activity reports, and any special nonrecurring reports, from field offices that are required for purpose of executive directions.

(2) Policy, Procedural, and Organization. This includes formal policy and procedural issuances (obsolete as well as current), such as regulations, orders, circulars, manuals, and other types of directives with related forms, recommendations, endorsements, clearances, and comments; organizational charts and directories (obsolete and current); annual or other periodic narrative and statistical reports on accomplishments at the organizational levels above divisions; and narrative accounts of agency's history.

(3) Executive Direction to OSD Components, DAFA, the Fourth Estate and/or DoD Wide Programs. This includes documents relating to legislation and Executive Orders proposed by OSD, DoD, other government agencies, and delegations, to include copies of hearings, bills, and statutes; continuing authorities; case files, subject matter, planning and strategic documents, and control files used to document the preparation, issuance, analysis of, reactions to, and compliance with those authoritative documents that affect and define the functions of the OSD Component. Documentation includes agendas, briefing materials, notes, and minutes, and supporting papers of meetings of interagency and extra-federal governmental bodies in which OSD participates, or relates to OSD or DoD functions.

(4) Social Networking Site (SNS) Outreach. This includes information provided to the public using non-government owned internet communication tools, such as Facebook, Twitter, and YouTube. OSD records and information solely available on non-government owned internet communication tools must be downloaded, retained, and maintained by each Component. The OSD RIM Program provides RIM personnel with guidance and procedures for archiving SNSs at https://www.esd.whs.mil/RIM/.

## 4.11. MANAGEMENT OF LEGACY PAPER RECORDS

a. OSD Components are required to transition to a paperless environment to be compliant with OMB/NARA M-23-07. When managing legacy paper records during the transition period, file folders must be established and labeled with all the information required to identify the information or papers in the folders. The best time to do that is when new files are created, or old ones are remade. Modification or deviation of file numbers is not authorized.

b. 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, and audiovisual, etc.). File arrangement is the relative positioning of information in a file. Effective file arrangement allows for easy retrieval and disposition of records.

c. Personnel will:

(1) Prepare information for filing when all actions are completed as required by a business process, federal law or regulation, DoD issuance, or when an official has requested that documentation be maintained.

(2) Ensure that each record set is complete, and that sections or related papers are retained or accounted for in both paper and electronic filing systems.

(3) 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 RDS.

(4) Remove all mail control forms, classified cover sheets, envelopes, and routing slips, except those containing remarks or information of significant record value.

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

d. Assemble related documents for filing. See Section 6 for electronic media.

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

(2) Ensure sections/tabs are in numerical or alphabetical order.

(3) Include supporting papers to include background documents and substantive drafts.

(4) Check for the completed package or final document.

e. Bring forward documents needed to conduct current business or that are 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 document 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 in which there are different transactions, such as reports of inspection of two different organizations.

f. Use a cross-reference sheet (see DD Form 2861) for documents brought forward to maintain continuity.

g. File papers loosely in the proper folder according to a filing arrangement that meets the office business needs.

h. Keep folder labels visible by neatly arranging papers in the folders. 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.

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

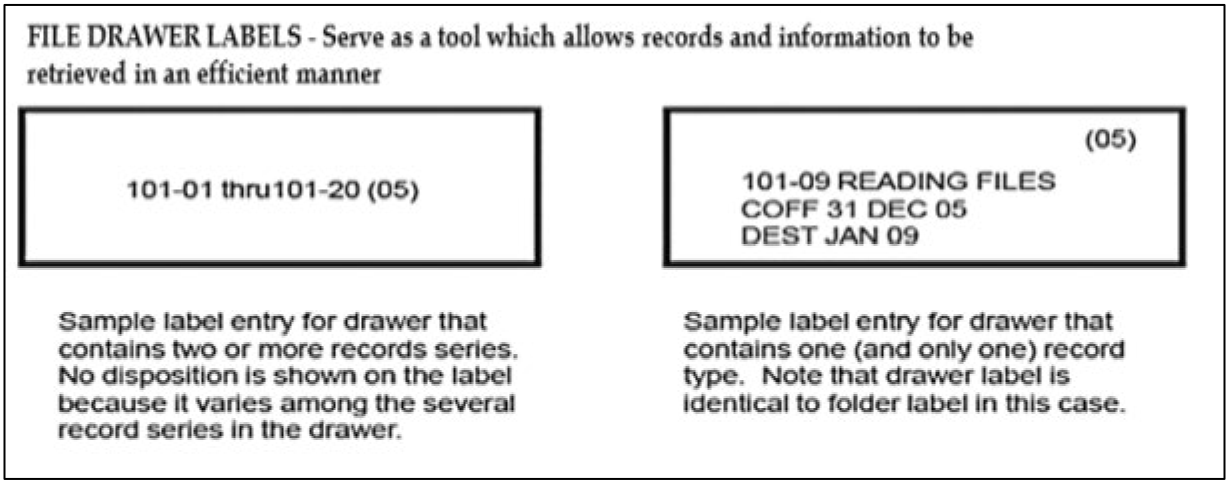
j. Avoid cluttering the files with bulky materials; separate and store in equipment suited to its size. Maintain this material in date, or serial number order. Make a cross-reference to the bulky material and annotate in a conspicuous location or with the filed papers. Mark the bulky material with storage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

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

l. Ensure that all paper record files are complete, identified, and maintained in accordance with this issuance and DoD requirements. Do not separate case files or project files and ensure the origins of the records are preserved.

## 4.13. PREPARING AND USING FILE FOLDERS AND LABELS

a. Labeling file drawers. Label file drawers to facilitate retrieval and use discretion to prevent revealing the classifications of material stored therein. Only the file numbers and inclusive dates of the material will be indicated (see Figure 3).



**FILE DRAWER LABELS - Serve as a tool which allows records and information to be retrieved in an efficient manner**

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.

Figure 3. Sample File Drawer Labeling

b. File Folders. When the material in any paper folder reaches normal capacity (approximately three-fourths of an inch in thickness for manila folders, although volume can vary for expandable or other folder types), prepare another one. Begin the second folder at a logical point, such as the beginning of a month or a calendar quarter. When there are several folders under one file number, offices can use a dummy file folder, which is an empty folder with a label that shows all the required disposition information but is not used to file documents.

The dummy folder would be filed as the first folder, and should be labeled with the file number, subject, and the general disposition instructions from the OSD RDS (e.g., 101-01.2 Actions/Operations Files, COFF CY DEST 5 years after COFF). The remaining folders would then be labeled with only the file number and year. These saves repeating the same information on the succeeding file folders. See Figure 4 for an example of file folders with a dummy folder.

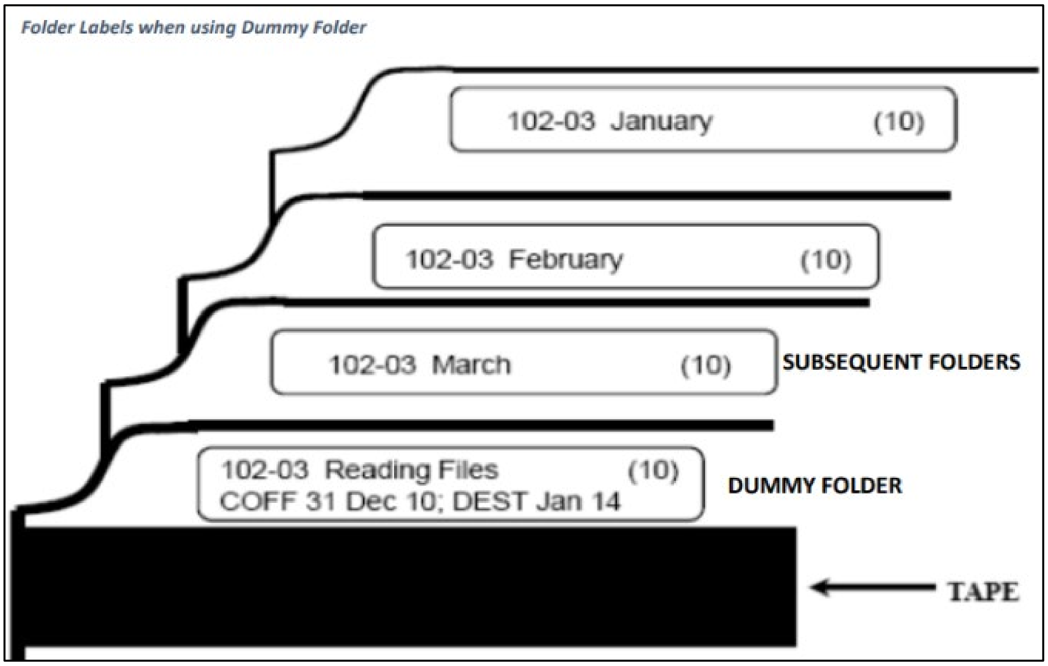
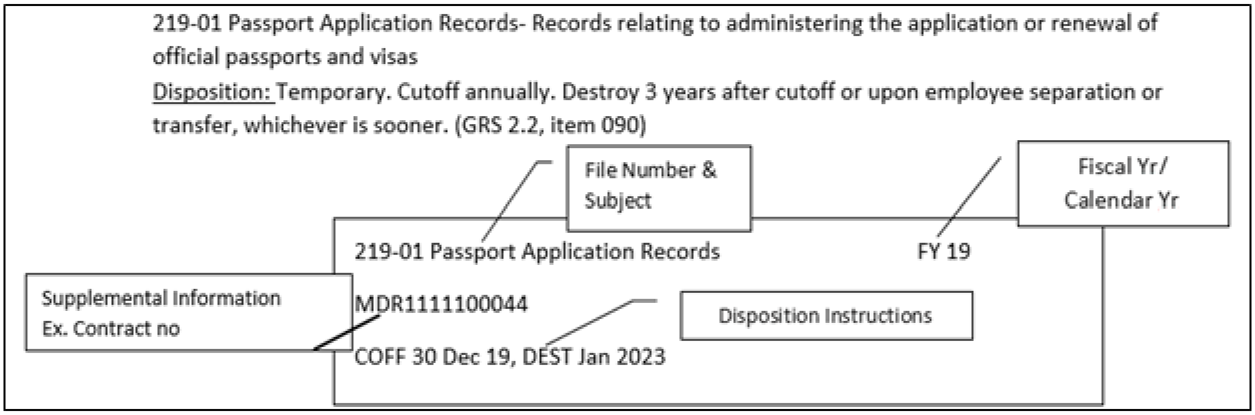


Figure 4. Example Dummy Folder

c. Preparation of Labels. Label all file folders and electronic media with the file number, title, year of accumulation, cutoff date, specific disposition instructions, and PA SORN number, if applicable. Label all binders with file number, file title, disposition instructions, and PA SORN number, if applicable. See Figures 5 – 7 for labeling examples.


219-01 Passport Application Records- Records relating to administering the application or renewal of official passports and visas

Disposition: Temporary. Cutoff annually. Destroy 3 years after cutoff or upon employee separation or transfer, whichever is sooner. (GRS 2.2, item 090)

Figure 5. File Folder Labels

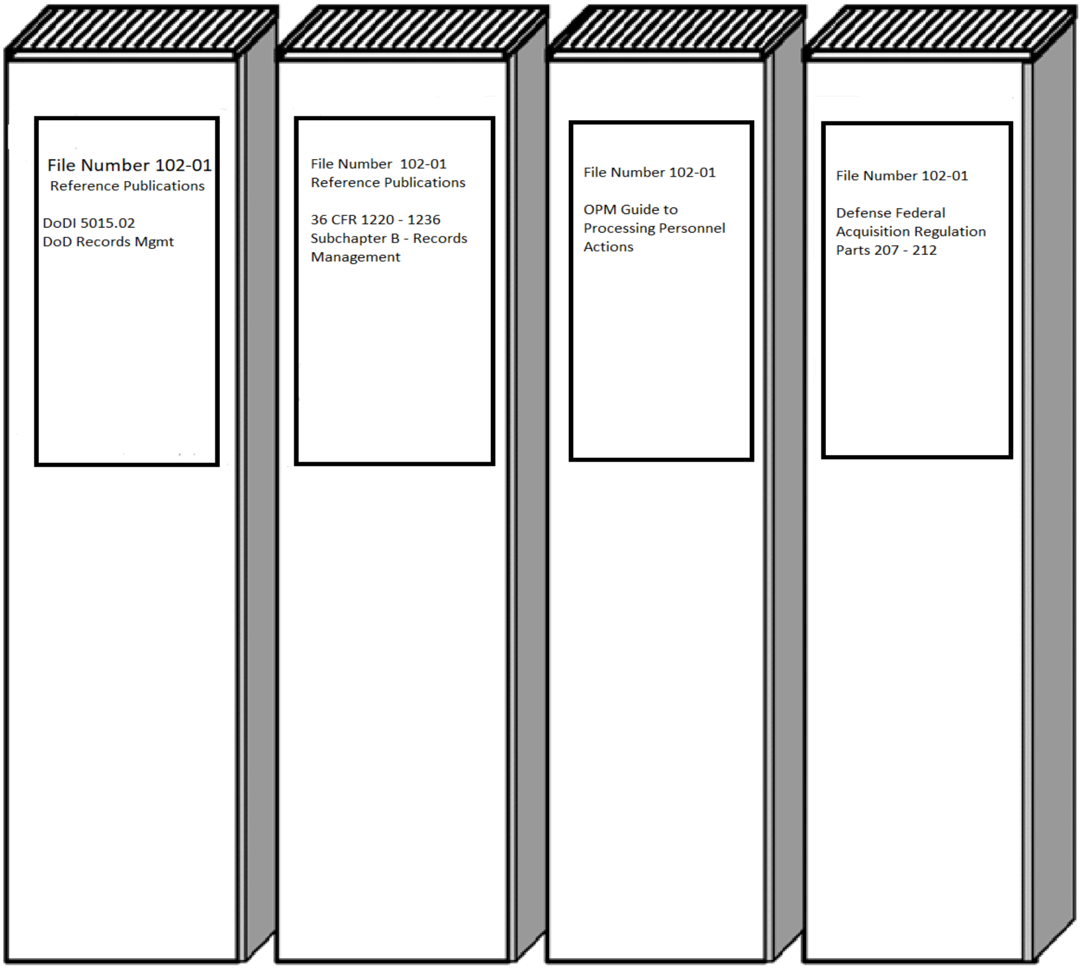
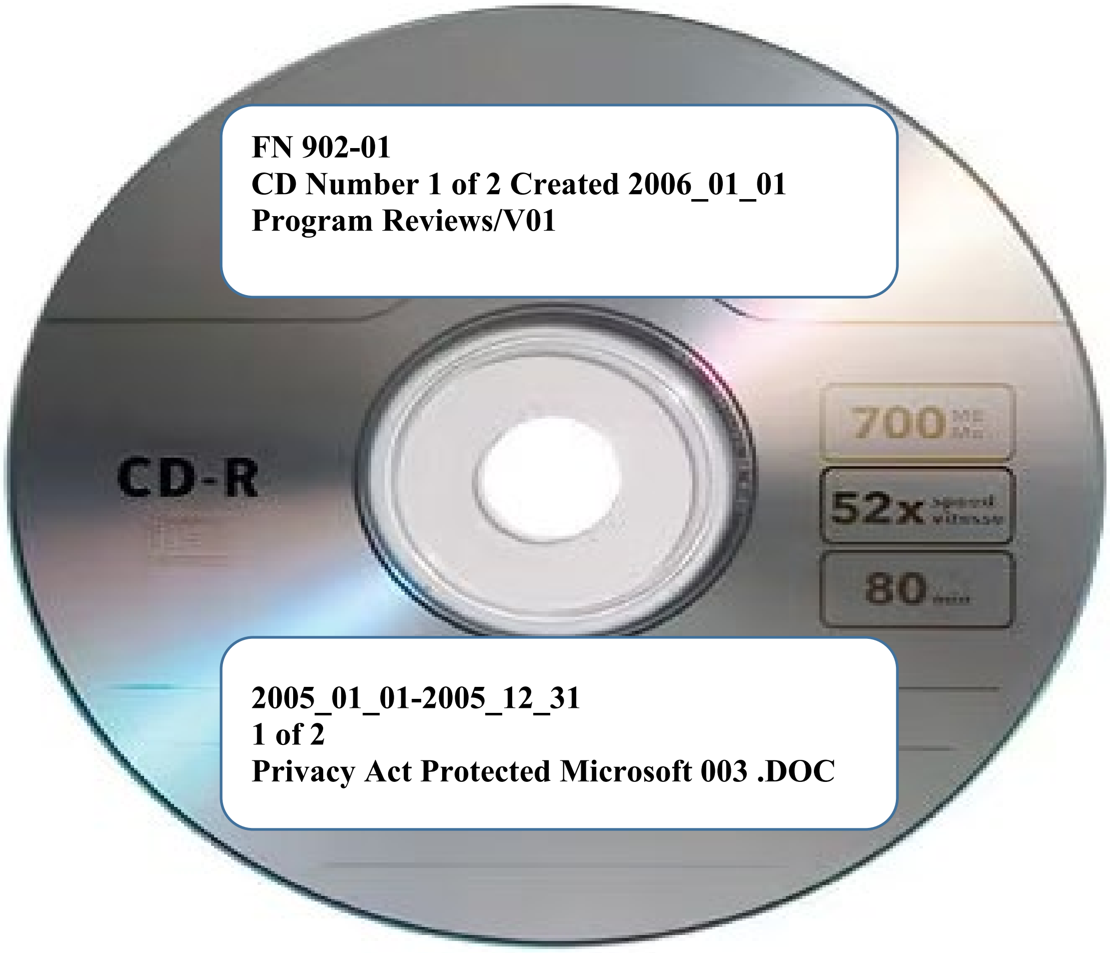


Figure 6. Binder Labels

(1) For electronic media (e.g., legacy diskettes, compact disks (CDs), digital video disks (DVDs) that have not yet been uploaded onto shared drives/SharePoint, or Defense Information Systems Agency (DISA)/Joint Services Provider (JSP)-authorized external hard drives or CDs), type identifying data on standard labels, positioning them on the media as shown in Figure 7.



FN 902-01
CD Number 1 of 2 Created 2006_01_01
Program Reviews/V01

2005_01_01-2005_12_31
1 of 2
Privacy Act Protected Microsoft 003 .DOC

Figure 7. Sample of Label Entries for Electronic Media

(a) Labels should contain file number, title, date, author or creator, cutoff date, office name, type of record or name of office (if applicable), PA SORN or security classification (if applicable), software version, and file extension.

(b) All files stored on the electronic media should have a standardized naming convention and date format (ex., YYYYDDMM). For more tips see Appendix B. In addition, the following files must be included in ASCII text format in the media:

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

(2) 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.

(2) When preparing labels, subtitles and commonly accepted abbreviations may be used. It is recommended all WHS-serviced Components use the Joint Publication 1-02, also known as DoD Dictionary of Military and Associated Terms, to standardize abbreviations used in the filing system. In addition to commonly used abbreviations, use the abbreviations in preparing labels that are included in Table 4.

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

Table 4. Abbreviations for Record and File Labels

## 4.14. CUTOFF PROCEDURES

a. Files are "cut off" at the point when a record transitions from "active" to "inactive" status (also called a "closed" file). This occurs when the file is no longer needed for current business operations and is subsequently moved to an inactive status. Commonly, paper records are retained on site until the file is transferred to an FRC, destroyed, digitized, and uploaded into an electronic recordkeeping structure, or held for reference purposes only; no new documents will be added after the cutoff date. Electronic records shall be retained on hand in the electronic recordkeeping structure until the authorized retention periods have lapsed and disposition is applied. Inactive files (paper and electronic) must be kept separate from active ones, and labeled appropriately, to guard against misfiles.

b. The OSD RDS provides the cutoff instructions for each file number. Cutoff is applied on a calendar or fiscal year basis, unless they are case or project files, which are cut off upon the completion of a certain event, such as separation of personnel, final contract payment, or project completion.

c. When applying annual cutoff (calendar or fiscal year, whichever is appropriate), all offices will cut off and separate active records from inactive records. Upon cutoff, the office will move files to an inactive file in the calendar year or fiscal year folder for the year the cutoff event occurs. Inactive files will be retained until they are eligible for destruction or transfer to NARA, in accordance with the retention period identified in the OSD RDS for the applicable file number.

d. RIM personnel will assist OSD employees with:

(1) Determining cutoff dates: calendar year files are closed on December 31, fiscal year files are closed on September 30 of each year, and project or case files are cut off in the calendar or fiscal year in which the project or case file is closed.

(2) Conducting a review and destroying all duplicate or extraneous materials.

(3) Retiring, transferring, or destroying eligible materials according to the applicable file number contained in the OSD RDS.

**SECTION 5:**

## 5.0. DISPOSITION PROCEDURES

### 5.1. GENERAL

a. The OSD RIM Program is designed to preserve records of continuing value, and systematically eliminate all other records, in accordance with a defined operational or business value to the OSD, DoD, and/or the United States, as documented in the OSD RDS.

(1) This ensures preservation of permanent and historical records and reduces the cost and effort of recordkeeping.

(2) To achieve these objectives, standard procedures have been established for the disposition of all WHS-serviced Component records.

b. Cutoff, retention periods, and the disposition for file numbers of OSD files are published in the OSD RDS as disposition instructions. Disposition instructions, including 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 General Records Schedule (GRS).

(1) In accordance with 44 USC § 3303, all approved OSD unique file numbers and applicable GRS are mandatory. Deviation from disposition instructions in the approved OSD RDS is not authorized without approval from the Archivist of the United States via the OSD Records Administrator.

(2) RIM personnel will submit recommendations for changes to cutoff, retention periods and disposition procedures to the OSD Records Administrator for approval. The OSD Records Administrator will coordinate approved requests for change(s) with NARA and alert the Component when any such changes are approved.

c. Records that do not have a NARA-approved disposition are considered unscheduled records and cannot, by law, be destroyed or deleted in accordance with 36 CFR §§ 1220-1236.

### 5.2. DISPOSITION INSTRUCTIONS

a. Types of Disposition Instructions. The OSD RDS provides the overall cut off instructions and retention periods for the records and information involved (e.g., cut off annually and destroy after 2 years, cut off upon completion and destroy after 10 years, or cut off fiscally and transfer to NARA 30 years after cutoff). The retention period begins on the next date after the file is cut off or closed, unless otherwise indicated. Examples include:

(1) Files with One-Month Retention. Files having a retention period of one month, or 30 days, will be cut off at the end of the month. Retention starts the first day of the next month; the records will be held one month in the current file area (CFA), and then destroyed. For example,

cutoff is 30 October 2023, retention starts 01 November 2023; records are retained for the full month of November and destroyed 01 December 2023.

(2) Files with One-Year Retention. Files having a retention period of one year will be cut off at the end of the calendar or fiscal year. Retention starts the next day (01 January for CY and 01 October for FY); the records will be held in the CFA for an additional year, and then destroyed.

(3) Files with Two- to 10-Year Retention. Files having a retention period of two to 10 years will be cut off at the end of the calendar or fiscal year and held after cutoff in the CFA until they are destroyed or (for legacy paper records, until the June 30, 2024, deadline in OMB/NARA M-23-07) retired to an FRC. Note: Temporary records retired to an FRC will be destroyed by the FRC (when eligible) after notice is provided to OSD, the Component concurs in the destruction, and the OSD Administrator sends the approval of destruction to the FRC. The OSD Records Administrator, in coordination with NARA, will accession permanent records from the FRC to the National Archives in College Park, Maryland (Archives II) when eligible.

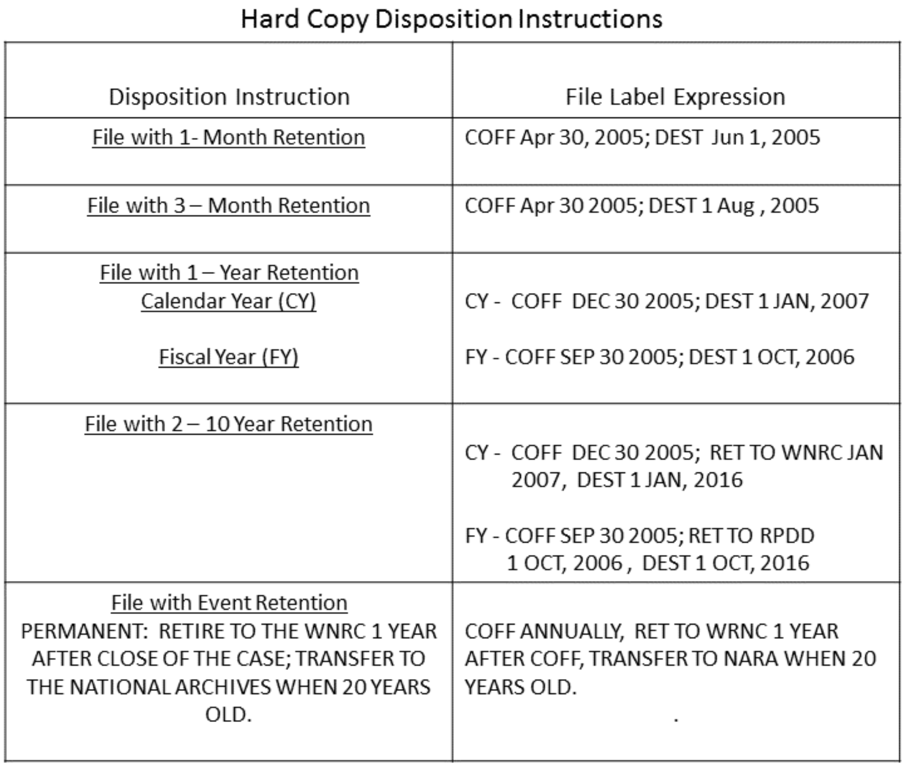
(4) Files with a Flexible Retention. Files having a flexible retention period such as delete, destroy, or transfer when five to seven years old, will be cut off at the end of the calendar or fiscal year; retained for at least five years but no longer than seven years; and destroyed or transferred as provided by the OSD RDS. The amount of time the record is retained is determined by the business needs of the office. Business needs should be prescribed in a regulation, issuance, or standard operating procedure and documented in the file plan/folder labels to ensure consistency in the retention of the record.

(5) Files with Event Retention with no Retention Period. Files having an event cutoff with immediate disposition such as cut off and destroy when superseded, obsolete, or property is turned in (temporary) or cut off and transfer to NARA when the committee disbands, treaty is signed, etc., will be maintained in the active files until the event occurs and destroyed (if the records are temporary) or transferred to NARA (if the records are permanent).

(6) Files with Event Retention with a Prescribed Retention Period. Files having an event cutoff that includes a retention period will be cut off in the year (fiscal or calendar) when the event occurs and retained for the retention period before disposition is applied. Events include being transferred to inactive files and cut off at the end of the calendar or fiscal year, held for a period specified after the event, and destroyed (if the records are temporary) or transferred to NARA (if the records are permanent).

(7) Unscheduled Files. Files having no approved retention period by NARA 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 RDS. See Section 5.5 for information on submitting new disposition schedules.

b. Labeling Legacy Paper Records with Disposition Instructions. Figure 8 provides a visual representation of how to label legacy paper records with the various types of disposition instructions outlined in paragraph a of this Section.



Hard Copy Disposition Instructions

| Disposition Instruction | File Label Expression |
|---|---|
| File with 1- Month Retention | COFF Apr 30, 2005; DEST Jun 1, 2005 |
| File with 3 – Month Retention | COFF Apr 30 2005; DEST 1 Aug , 2005 |
| File with 1 – Year Retention<br>Calendar Year (CY)<br>Fiscal Year (FY) | CY - COFF DEC 30 2005; DEST 1 JAN, 2007<br>FY - COFF SEP 30 2005; DEST 1 OCT, 2006 |
| File with 2 – 10 Year Retention | CY - COFF DEC 30 2005; RET TO WNRC JAN 2007, DEST 1 JAN, 2016<br>FY - COFF SEP 30 2005; RET TO RPDD 1 OCT, 2006 , DEST 1 OCT, 2016 |
| File with Event Retention<br>PERMANENT: RETIRE TO THE WNRC 1 YEAR AFTER CLOSE OF THE CASE; TRANSFER TO THE NATIONAL ARCHIVES WHEN 20 YEARS OLD. | COFF ANNUALLY, RET TO WRNC 1 YEAR AFTER COFF, TRANSFER TO NARA WHEN 20 YEARS OLD. |

Figure 8. Inserting Disposition Instructions onto Labels for Paper Records

c. Labeling Electronic Records with Disposition Instructions. Electronic records must have disposition labels inserted into the recordkeeping structures as outlined in Section 6.4 of this PRIMER.

## 5.3. CHANGES TO RETENTION PERIODS

a. 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, via the OSD Records Administrator, for approval.

(1) See Sections 5.4 and 5.5 for instructions for WHS-serviced Components to request the OSD Records Administrator submit a request to NARA for a change to retention periods in the OSD RDS.

(2) While awaiting NARA approval of a change to retention period, offices requesting a change in retention period should place a disposition hold on the affected records.

b. General rules when applying an approved change to the retention of a record include:

(1) 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 cutoff files affected by the change will be brought under the new retention period.

(2) 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.

## 5.4. RE-EXAMINATION OF RECORDS SCHEDULES

a. WHS-serviced Component RIM personnel will review their records schedules annually and recommend updates whenever necessary, such as when mission responsibilities change due to law, Executive Orders, or reorganization, and will submit necessary changes to the OSD Records Administrator.

b. The OSD Records Administrator will review recommendations for new or revised files, disposition procedures, or standards, and make recommendations for final approval to NARA. When establishing criteria for updating or changing a records schedule or file number, ask:

(1) Does the program office requesting the change have programmatic authority of the records? For example, the Office of the USD(A&S) (OUSD(A&S)) establishes policy for acquisitions, including procurement of goods and services, research and development, developmental testing, and contract administration, for all elements of the Department. As OUSD(A&S) has been delegated this authority by the Secretary of Defense, no other OSD Components can request changes to records series, records categories, or file numbers that fall under OUSD(A&S) purview. WHS-serviced Components can coordinate with OUSD(A&S) to revise records series, records categories, or file numbers, but OUSD(A&S) must submit the change request.

(2) Is this information needed to answer a request for information (RFI), mandatory congressional, OSD, or DoD reporting, or provide statistical analysis to Congress, DoD leadership, the President of the United States, or per federal regulations? If so, what does the responsive information consist of, and what is the average length of accumulation required to formulate the answer? For example, if a current reporting requirement for DoD is changed by the annual NDAA requesting 10 years of accumulated data, but the retention period for this information is currently 3 years, the WHS-serviced Component RIM personnel would coordinate with the program office to update the retention from 3 years to 10 years.

(3) If the retention does not meet the program requirements, does it need to be increased or decreased?

(a) If decreasing, identify which metrics are in place that document the current disposition that is no longer applicable.

(b) If increasing, identify which metrics are in place to determine why an increase is required.

(4) Are these records necessary for the protection of DoD's rights and interests, or eligibility for or proof of benefits for DoD personnel? Has your local GC or DoD GC reviewed and determined whether the retention meets legal, administrative, or financial requirements to protect DoD?

(5) Has the content and use of the records remained the same since the disposition was initially approved? If the content, purpose, and use has significantly changed from its original purpose due to mission requirements, or DoD or federal regulations, this may require a visit from NARA to determine whether a change from temporary to permanent, or the reverse, is required.

(6) How must these records be used internally and externally to DoD? WHS-serviced Component RIM personnel must consider that, while the records a WHS-serviced Component create or receive may have a short-term value, there may be a secondary need for this information by other federal agencies, the public, and non-governmental organizations, which may necessitate longer retention.

(7) Is the requested change to a disposition authority necessary? If yes, WHS-Serviced Component RIM personnel will submit a revised Standard Form (SF)-115 to the OSD RIM Program via their CRMO for submission to NARA in accordance with Section 5.5 of this PRIMER. All documentation collected to justify the request should be included with the submission.

## 5.5. SUBMITTING NEW RETENTION SCHEDULES (SF-115)

a. WHS-serviced Components will submit an SF-115 for program and operational records and information systems which are not identified in the GRS, need updates/changes (as discussed in Section 5.4), or cannot be filed under any file number in the OSD RDS. Unscheduled records and information systems will be maintained as current or active files and treated like permanent records until disposition instructions have been provided by the OSD RIM Program and approved by NARA.

b. There are two primary types of records disposition authorities: media neutral and FIS authorities. Media neutral disposition authorities are mandatory authorities that apply to the described records regardless of their medium. FIS authorities only apply to the specific electronic information systems and associated inputs and outputs described in the SF-115.

c. Draft media neutral records disposition authorities will include:

(1) Scope (i.e., applicability).

(a) Internal to Component.

(b) OSD-wide (two or more OSD Components/DAFAs).

(c) DoD-wide (two or more DoD components, e.g., OSD & Joint Staff, OSD & Military Department, or where an OSD Component is the Executive Agent).

(2) Name and basic background information of the Component submitting the SF-115.

(3) Description and purpose of the program, mission, or operation the records are created or received to support.

(4) File number: If proposing a new file number, this will be provided by OSD RIM Program. If proposing to modify the existing file number, identify the applicable file number.

(5) File title of the records (e.g., Air Operations Report). Spell out all abbreviations/acronyms.

(6) File description (e.g., "The air operations report contains information on equipment, mileage, flight hours, speed, latitude and longitudinal information on contiguous United States (CONUS) training operations over transoceanic regions").

(7) Disposition instructions.

(a) Proposed value (disposition) of the records, e.g., temporary, or permanent (see Section 4.3).

(b) Cut off instructions (e.g., cut off annually or cut off upon completion, etc.).

(c) Retention: length of time OSD or DoD retains the records in legal and physical custody to meet administrative, programmatic, legal, regulatory, or fiscal requirements after cutoff and before disposition (e.g., destroy 5 years after cutoff or transfer to NARA 25 years after cutoff, etc.).

(8) Privacy Act SORN Number, if applicable. If not applicable, indicate "N/A."

d. SF-115 for FIS records disposition authorities will include:

(1) Scope (i.e., applicability).

(a) Internal to Component.

(b) OSD-wide (two or more OSD Components/DAFAs).

(c) DoD-wide (two or more DoD components, e.g., OSD & Joint Staff, OSD & Military Department, or where an OSD Component is the Executive Agent).

(2) Name and background information of the Component submitting the SF-115.

(3) System title (spelled out) and acronym.

(4) Purpose: what is the purpose or program(s) the system was created and fielded to meet.

(5) System Interfaces: Identify sources (inputs) and outputs (feeds) to and from DoD and non-DoD information systems (if applicable). Includes manual inputs provided by users.

(6) Master file: provide example of data fields, data elements or metadata applicable to the application, database, or information system.

(7) File number: If proposing a new file number, this will be provided by OSD RIM Program. If proposing to modify the existing file number, identify the applicable file number.

(8) File Title: same as system title.

(9) File Description: Short description of the FIS purpose, content, master file and data fields.

(10) Proposed disposition instructions.

(a) Proposed value (disposition) of the records, e.g., temporary, or permanent (see Section 4.3).

(b) Cutoff instructions: the act(s) that transition FIS records and information from active to inactive or closes transactions.

(c) Retention: length of time OSD or DoD retains the records in legal and physical custody to meet administrative, programmatic, legal, regulatory, or fiscal requirements after cutoff and before disposition (e.g., destroy 5 years after cutoff or transfer to NARA 25 years after cutoff, etc.).

(11) Privacy Act SORN Number, if applicable. If not applicable, indicate "N/A."

## 5.6. IMPLEMENTING GRS

a. In accordance with 44 USC § 3303(a)(d), the Archivist of the United States is authorized to issue the GRS to provide disposition authority for records common to several or all agencies of the Federal Government. These schedules authorize agencies, after specified periods of time, to either destroy temporary records or transfer permanent records to NARA.

(1) When NARA issues a new or updated GRS, the OSD Administrator will review the GRS and update the OSD RDS, accordingly. In addition, WHS-serviced Component RIM personnel will:

(a) Review GRS items for applicability to their component's authorities and responsibilities to determine whether it is necessary to revise the OSD RDS to conform to new GRS item(s).

(b) Notify the OSD Records Administrator and request a change to the OSD RDS with the new GRS disposition authority.

(2) If the GRS item states that it is mandatory and must be followed without exception, the agency must follow the GRS and cannot use an agency authority, even if previously approved by NARA. The OSD Records Administrator will notify RIM personnel and update the OSD RDS with the new GRS disposition authority.

b. WHS-serviced Components will not deviate or alter retention periods set by the GRS without the written permission of the OSD Records Administrator.

(1) GRS flexible disposition authorities allow agencies to choose retention periods within stated parameters (e.g., Temporary. Destroy when 3 years old, but longer retention is authorized if needed for business use). The chosen retention must be included in the OSD RDS. To implement a GRS with a flexible disposition, WHS-serviced Components will define business use and submit to OSD Records Administrator for approval. The OSD Records Administrator will insert the longer retention into the OSD RDS once approved.

(2) OSD employees will coordinate with the WHS-serviced Component RIM personnel to submit requests to deviate or alter retention periods to the OSD Records Administrator. Requests must be accompanied with a justification and evidence for the deviation.

## 5.7. DAMAGE, ALIENATION, AND UNAUTHORIZED DESTRUCTION OF RECORDS

a. Each WHS-serviced Component is responsible for preventing the loss of federal records.

b. Records and information (including those contained within an FIS) destroyed or damaged due to accidental loss or destruction, such as fire or water, are to be reconstructed by the office of record.

(1) Records can be reconstructed from information retained in other file numbers, non-record materials, or computers.

(2) Include documentation concerning the reconstruction and cross-referencing materials to aid in the identification of the record.

(3) Annotate an SF-135 with any information that cannot be reconstructed and include with the rest of the file number upon retirement.

(4) Notify OSD Records Administrator of any accidental loss or destruction of records.

c. Federal records (including copies) may not be removed from the legal or physical custody of OSD or destroyed without regard to the provisions listed in AI 15 or in this PRIMER.

(1) The willful and unlawful destruction, damage, or alienation of federal records can result in a monetary fine, imprisonment, or both, pursuant to 36 CFR §§ 1220-1236, and 18 USC § 2701.

(2) CRMOs and DAFA RMs will report to the OSD Records Administrator of any unauthorized destruction or damage of official records. Reports will contain the following information in accordance with 36 CFR § 1230:

(a) A complete description of the records, including volume and dates if known.

(b) The office of origin.

(c) A statement of the exact circumstances surrounding the alienation, defacing, or destruction of the records.

(d) A statement of the safeguards established to prevent further loss of documentation.

(e) Actions taken to salvage, retrieve, or reconstruct damaged records, as well as a description of types of records that are not recoverable/irretrievably lost.

## 5.8. INVESTIGATIONS OF DAMAGED, ALIENATED OR UNAUTHORIZED DESTRUCTION OF RECORDS

When notified, WHS-serviced Component heads, Office of Primary Responsibility (OPR), or program manager shall complete the following procedures to investigate:

a. Select the investigator; an appropriate investigator should:

(1) Be able to investigate objectively without bias, be impartial and objective to gather and consider relevant facts.

(2) Not have a personal relationship with the involved parties. The outcome should not directly affect the investigator's position within the organization.

(3) Have knowledge of RIM laws and OSD and DOD guidance.

(4) Have the right temperament to conduct interviews.

(5) Be empowered by WHS-serviced Component head, OPR, or program manager to interview all personnel involved regardless of rank, status, or position.

b. The investigator will first create a plan for the investigation:

(1) Identify personnel involved.

(2) Gather evidence; if necessary, coordinate with Human Resources (HR), Inspector Generals, IT personnel, DoD law enforcement agencies (such as Naval Criminal Investigative Service or Army Criminal Investigation Division) or GC to conduct record searches of applicable personnel e-mail and text message accounts, shared drives, SharePoint and Teams sites, personal drives, and paper records.

(3) Develop interview questions (who, what, when, where, and how).

c. The investigator will then schedule and conduct interviews:

(1) Secure conference room or similar area away from supervisors and other personnel that can listen in.

(2) Inform all parties involved of the need for an investigation and explain the investigation process.

(3) Allow for time between interviews to type up notes and adjust to new information.

(4) Allow employees to write statements surrounding the incident.

d. The investigator will then review and report:

(1) Review notes from interviews, records, including text messages and e-mail records, and other information gathered to make determination of fact and provide to WHS-serviced Component head.

(2) Provide WHS-serviced Component head report summarizing facts and conclusions.

e. The WHS-serviced Component head, as well as legal counsel, should make the final determination of any employment actions that are warranted based on the investigative report.

f. The WHS-serviced Component head, OPR, or program manager will report findings to the OSD Records Administrator. Ensure the report meets requirements of 36 CFR §1230.14:

(1) Provide a summary of actions put into place to prevent future incidents and educate employees, military service members, and contractors.

(2) Summarize the incident or issues investigated, including dates and the following:

(a) Parties involved.

(b) Key factual and credibility findings, including sources referenced.

(c) Specific conclusions.

(d) Party (or parties) responsible for making the final determination.

(e) Issues that could not be resolved and reasons for lack of resolution.

(f) Employer actions taken.

g. The OSD Records Administrator determines when incidents are reported to NARA.

SECTION 6:

# 6.0. ELECTRONIC RECORDS MANAGEMENT

## 6.1. GENERAL

a. It is the responsibility of each WHS-serviced Component head and all 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 PRIMER, AI 15, and the OSD RDS.

b. Electronic records are those that information meet the definition of being a federal record, (i.e., when it is information made or received in connection with the transaction of public business and is 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) AND are created, stored and retrieved solely via electronic means.

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, text messaging devices, software programs (such as Excel or Adobe), websites and SNSs, or they may be converted from paper (via scanning) into electronic format.

(2) These records may also reside in databases or FIS.

(3) In the case of FIS, the program office responsible for the system or database must incorporate records management requirements as defined in 36 CFR § 1236 into the system design regardless of the classification of the data in accordance with OMB Circular No. A-130.

## 6.2. CATEGORIES OF ELECTRONIC RECORDS

a. Databases. Databases contain structured data which is centrally managed within the application. WHS-Serviced 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 in the OSD RDS includes input/source records, system documentation (codebooks, record layouts, etc.), system outputs, and master files.

b. Information systems. The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, per 44 USC § 3502.

c. FIS. FIS refers to an information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency per 40 USC § 11331.

d. Electronic Records. An electronic record is information recorded by a computer that is created or received in the initiation, conduct, or completion of a WHS-serviced Component's or individual's activity, including documents converted to electronic formats (also known as 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 records management application to manage them effectively throughout their life cycle.

(2) Scanned records are images, printed text, handwriting, or an object converted to a digital image by a scanning device. In accordance with 36 CFR § 1236 will have been scanned using an approved project plan (see Appendix E for a sample scanning project plan). The project plan must take into account NARA's criteria for digitizing records and ensure they are digitized in accordance with 36 CFR § 1236, Subpart E (permanent records).

(a) Paper records SHALL NOT be destroyed without an approved project plan.

(b) WHS-serviced Components will submit project plans for coordination with the OSD Records Administrator and the Component's GC. All project plans will be in writing and approved by the WHS-serviced Component head.

e. Disposing of original source records.

(1) When a WHS-serviced Component has an approved project plan that meets the standards in 36 CFR § 1236.32, Subpart E, it may destroy the original source records pursuant to the current GRS 4.5 item 010 – Source Records, or a NARA-approved OSD-specific records schedule that addresses disposition after digitization, subject to any pending legal constraint, such as a litigation hold.

(2) The WHS-serviced Component must treat the digitized versions, now the official record, in the same way it would have treated the original source records.

(3) The WHS-serviced Component must retain the digitized versions for the remaining portion of any retention period established by the applicable records schedule.

f. Websites. Websites containing unique records and information, not duplicate of records stored elsewhere, must be maintained in accordance with the OSD RDS. If websites are not identified in the schedule, then they must be scheduled in accordance with "NARA Guidance on Managing Web Records."

g. Web 2.0 (Commonly Referred to as 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. This includes, but is not limited to, wikis, blogs, and SNS like Facebook, Instagram, Myspace, X (formerly Twitter), and LinkedIn. These sites should be appraised to determine what records exist and what series in the OSD RDS apply. Additional guidance for managing Web 2.0 records is available on the RDD website and "NARA Guidance on Managing Web Records."

h. 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 Components and must be managed in compliance with this PRIMER, AI 15, and the OSD RDS; see Section 6.7 of this PRIMER for more details.

## 6.3. MANAGEMENT OF ELECTRONIC RECORDS ON ORGANIZATIONAL SHARED DRIVES AND SHAREPOINT/MICROSOFT TEAMS

a. The management of electronic records is similar to the management of legacy paper records. Official records maintained in electronic formats (e.g., digital photographs, scanned images, cellular text records, databases, FIS, websites, etc.) must be maintained per the applicable file number in the OSD RDS.

(1) If an electronic record cannot be categorized to the OSD RDS, i.e., if no file description in the OSD RDS matches the content of the records, these records are considered unscheduled, and the organization must submit an SF-115 to OSD RIM Program to schedule the record (see Sections 5.4 and 5.5 for guidance on modifying the OSD RDS). Unscheduled records will be maintained as current or active files and treated like permanent records until disposition instructions have been provided by the OSD RIM Program and approved by NARA.

(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 RDS.

(4) Maintain classified information in accordance with Executive Orders 13526 and 12829 and the OSD RDS. Files containing classified markings of NATO classified (COSMIC/AMOTAL), ACCM, or as SAP must be maintained separately from other classified material in accordance with USSAN Instruction 1-07 and DoDM 5200.01 Volumes 1-3.

(5) Maintain PII in accordance with The Privacy Act of 1974 and DoD 5400.11-R, and CUI in accordance with 32 CFR § 2002 and Executive Order 13556.

b. Offices purchasing new FIS or upgrading old ones must ensure that records management controls for the data are incorporated into the system's design in accordance with 36 CFR §§ 1220-1236, DoDI 5015.02, and OMB Circular A-130.

c. Organizational shared environments (network shared drives), SharePoint sites, or Microsoft Teams sites do not provide the functionality of a recordkeeping system. However, through a combination of manual and automated policies and procedures, a shared drive/SharePoint/Teams site can be used as a recordkeeping system.

(1) Managing records in shared drives/SharePoint/Teams' sites require direct manual intervention which can be successfully met when the basic guidelines in the below Paragraphs 6.3.c.(3)(a) through 6.3.c.(3)(f) of this Section are followed.

(2) If your agency or organization implements any type of enterprise content management system or records management application, the office staff must consider the record value of the information created and received, its classification, and actively manage the records using that system.

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

(a) Establish POCs responsible for shared drive/SharePoint/Teams site management.

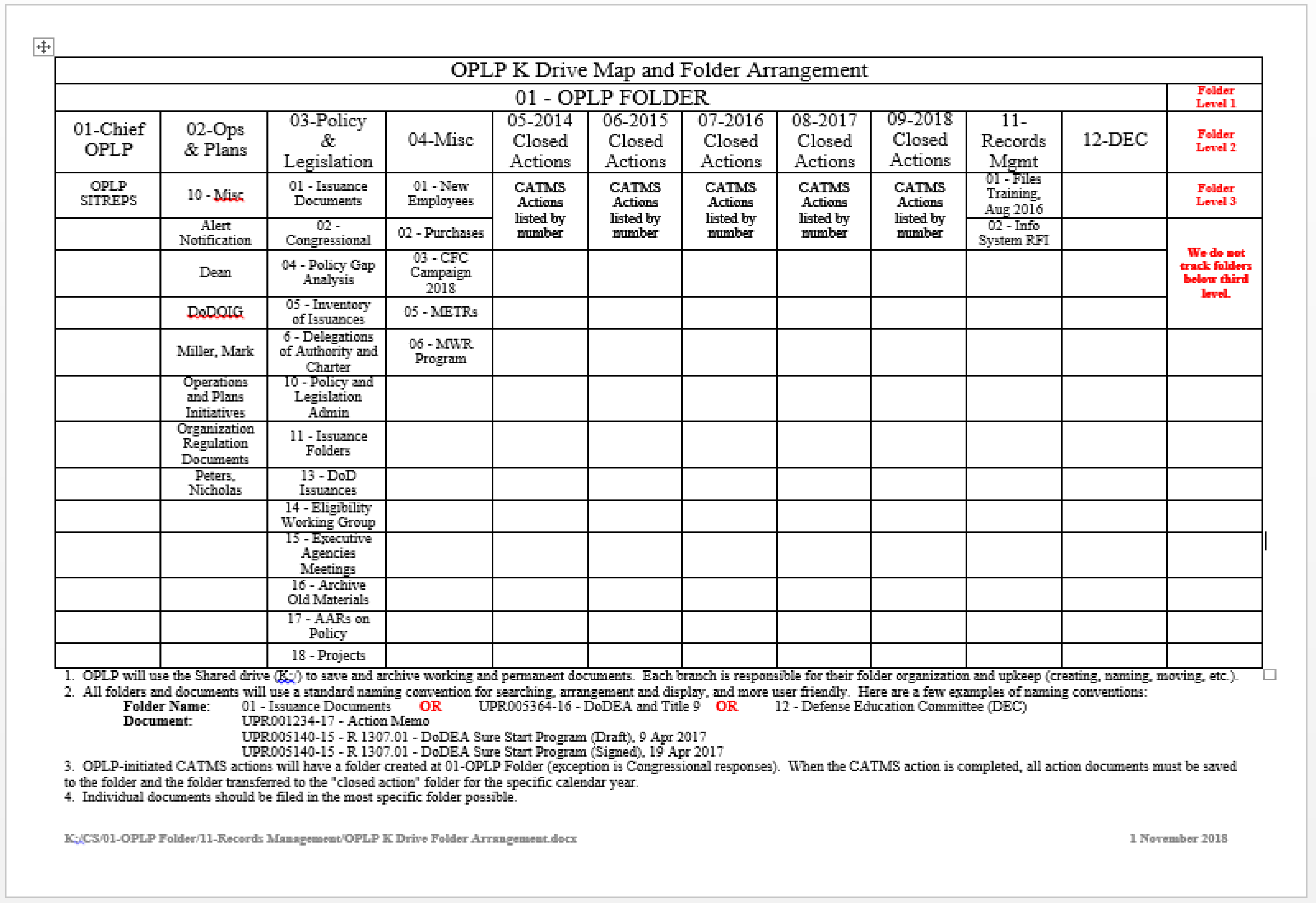
(b) Survey or inventory the information currently stored on the shared drives/SharePoint/Teams' sites to determine the status of the shared environment (unclassified, classified, PII, CUI, and personal) and identify the records to be managed. Issues to address are naming conventions (see Appendix B), establishment of compliant recordkeeping structure (see Appendix C), version control, protection for folders containing PII or CUI, access control, and preventing 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/CUI/NSI related records.

(e) Establish a standardized file structure that is aligned with the office's business processes. Structure folder and subfolders to be associated with the corresponding records schedules, including cutoff, retention, and disposition instructions (See Section 6.4 and Appendix C of this PRIMER for more information/examples of file structures incorporating disposition instructions).

(f) Create a drive map that is aligned with the office file plan. A sample drive map is included in Figure 9.



| OPLP K Drive Map and Folder Arrangement | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 01 - OPLP FOLDER | | | | | | | | | | | | Folder Level 1 |
| 01-Chief OPLP | 02-Ops & Plans | 03-Policy & Legislation | 04-Misc | 05-2014 Closed Actions | 06-2015 Closed Actions | 07-2016 Closed Actions | 08-2017 Closed Actions | 09-2018 Closed Actions | 11- Records Mgmt | 12-DEC | Folder Level 2 |
| OPLP SITREPS | 10 - Misc | 01 - Issuance Documents | 01 - New Employees | CATMS Actions listed by number | CATMS Actions listed by number | CATMS Actions listed by number | CATMS Actions listed by number | CATMS Actions listed by number | 01 - Files Training, Aug 2016 | | Folder Level 3 |
| | Alert Notification | 02 - Congressional | 02 - Purchases | | | | | | 02 - Info System RFI | | We do not track folders below third level. |
| | Dean | 04 - Policy Gap Analysis | 03 - CFC Campaign 2018 | | | | | | | | |
| | DoDOIG | 05 - Inventory of Issuances | 05 - METRs | | | | | | | | |
| | Miller, Mark | 6 - Delegations of Authority and Charter | 06 - MWR Program | | | | | | | | |
| | Operations and Plans Initiatives | 10 - Policy and Legislation Admin | | | | | | | | | |
| | Organization Regulation Documents | 11 - Issuance Folders | | | | | | | | | |
| | Peters, Nicholas | 13 - DoD Issuances | | | | | | | | | |
| | | 14 - Eligibility Working Group | | | | | | | | | |
| | | 15 - Executive Agencies Meetings | | | | | | | | | |
| | | 16 - Archive Old Materials | | | | | | | | | |
| | | 17 - AARs on Policy | | | | | | | | | |
| | | 18 - Projects | | | | | | | | | |

1. OPLP will use the Shared drive (K:/) to save and archive working and permanent documents. Each branch is responsible for their folder organization and upkeep (creating, naming, moving, etc.).
2. All folders and documents will use a standard naming convention for searching, arrangement and display, and more user friendly. Here are a few examples of naming conventions:

**Folder Name:** 01 - Issuance Documents OR UPR005364-16 - DoDEA and Title 9 OR 12 - Defense Education Committee (DEC)
**Document:** UPR001234-17 - Action Memo
UPR005140-15 - R 1307.01 - DoDEA Sure Start Program (Draft), 9 Apr 2017
UPR005140-15 - R 1307.01 - DoDEA Sure Start Program (Signed), 19 Apr 2017

3. OPLP-initiated CATMS actions will have a folder created at 01-OPLP Folder (exception is Congressional responses). When the CATMS action is completed, all action documents must be saved to the folder and the folder transferred to the "closed action" folder for the specific calendar year.
4. Individual documents should be filed in the most specific folder possible.

K:/CS/01-OPLP Folder/11-Records Management/OPLP K Drive Folder Arrangement.docx 1 November 2018

Figure 9. Sample Drive Map

## 6.4. NETWORK SHARED DRIVES/SHAREPOINT/TEAMS FILE STRUCTURES.

a. WHS-serviced Components must establish a filing structure for their electronic records, whether stored on shared drives, SharePoint sites, Teams sites, or other composite drives. Records must be organized in a standardized manner across a Component, although the Component has choices as to its scheme. Regardless of scheme chosen, electronic records must be categorized to a file number in the OSD RDS, and overview (i.e., general) and specific (i.e., calculated) disposition instructions must be inserted into the structure. Considerations include:

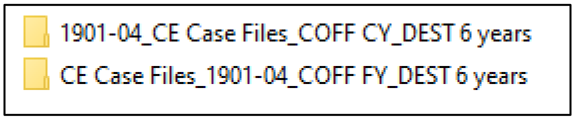
(1) File number placement. File numbers may be inserted as the start of the file name or can be inserted at the end of the file name. The chosen placement must then be applied consistently. Table 5 provides examples of both types of file number placements.

| File Number up Front | File Number at End |
|---|---|
| 1901-01_CMEC | CMEC_1901-01 |
| 1901-01_SPC | DACA_1901-02 |
| 1901-02_DACA | SPC_1901-01 |

Table 5. File Number Placement Examples.

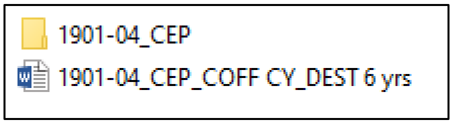
(2) Inserting disposition instructions into the structure. Both general disposition (i.e., instructions taken from the OSD RDS) and calculated disposition should be inserted into the structure.

(a) General disposition can be inserted into the folder containing the file number or inserted as a subfolder, readme text or file. Figures 10 and 11 provide examples for file number 1901-04 (cut off annually, destroy 6 years after cutoff).


1901-04_CE Case Files_COFF CY_DEST 6 years

CE Case Files_1901-04_COFF FY_DEST 6 years

Figure 10. General Disposition Inserted at File Number Level


1901-04_CEP

1901-04_CEP_COFF CY_DEST 6 yrs

Figure 11. General Disposition Inserted as a File

(b) Calculated disposition is inserted in the CY or FY cutoff subfolders within the file number folder. Abbreviations can be used in the file structure. Table 6 provides multiple different examples for calculated disposition for file number 1901-04 (cut off annually, destroy 6 years after cutoff) and file number 212-01 (cut off annually, transfer to NARA 25 years after cutoff).

| CE Case Files_1901-04 | CE Case Files_1901-04 | USD CHRON_212-01 |
|---|---|---|
| CY2021_D_CY2027 | FY2021_D FY2026 | CY2021_TFR_CY2047 |
| CY2022_D_CY2028 | FY2022_D FY2027 | CY2022_TFR_CY2048 |
| CY2023_D_CY2029 | FY2023_D FY2028 | CY2023_TFR_CY2049 |

Table 6. Calculated Disposition Examples

b. Types of Structures

(1) Multi-Office File Structure. A multi-office file structure provides centralized filing by creating a partition in which all reporting offices save their electronic records. This structured format, which displays all offices within the organization on the shared drive/SharePoint/Teams' site, utilizes either the flat file structure or subject matter file structure. The first level of filing is by office symbol (i.e., RDD_Records; FOID_Records, etc.). The second level of filing is the record folders with the file numbers. For an example, see Appendix C.

(2) Hierarchical File Structure. A hierarchical file structure is a structured format that replicates the organizational or command structure. 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 their office file plan and year of creation (calendar year or fiscal year). For an example, see Appendix C.

(3) Semi Flat File Structure. Semi flat file structures have files maintained in a manner that closely replicates the office file plan. In this arrangement, the first folder level is named after the office. The second folder level contains the file number, subject, and retention (or retention can be a subfolder or file within the second level folder). The third level folders (Cutoff folders) have the calendar year or fiscal year and destruction date. The latter two levels can be reversed or combined. For an example, see Appendix C.

(4) Subject Matter File Structure. In a subject matter file structure, the first folder level is named after the organization, but the second folder starts with its subject and contains the file number. Subfolders are arranged by year and contain the disposition instructions. For an example, see Appendix C.

(5) Functional File Structure. A functional file structure follows the functions and mission of the organization vice the office organization structure. The first folder level is the function or mission. The second folder level starts with its subject and contains the file number in parentheses. Subfolders are arranged by year and contain the disposition instructions. For an example, see Appendix C.

c. 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) To avoid exceeding the 255 characters limit, when naming files, it is highly recommended to refer to the Joint Publication 1-02, DoD Dictionary of Military and Associated Terms, to identify common DoD abbreviations and terms.

(2) For more tips on standardized naming conventions, see Appendix B and Appendix C.

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

e. 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).

f. 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.

g. Maintain permanent records in formats pursuant to 36 CFR §§ 1220-1236 and name, tag or identify the records clearly to prevent inadvertent deletions. Appropriate RIM personnel must coordinate the transfer of permanent electronic records with the OSD Records Administrator and OSD RIM Program for archiving with NARA. See Section 7.7 of this PRIMER for transfer guidance.

h. Ensure records are maintained throughout their approved life cycle as stated in 36 CFR §§ 1220-1236 and the OSD RDS.

i. Clearly identify and segregate from the official record all personal and non-record documents (e.g., personal correspondence, reference materials, and periodicals).

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

k. Identify records and all locations on the office file plan.

l. Train staff in the use of the shared drive/SharePoint/Teams' sites and in their records management responsibilities.

## 6.5. MANAGEMENT OF E-MESSAGES AND E-MESSAGING ACCOUNTS

a. According to 44 USC § 2209(c)(2), electronic messages (e-messages and e-messaging accounts) are "electronic mail and other electronic messaging systems that are used for purposes of communicating between individuals." This includes but is not limited to e-mail, text messages, chat, instant messaging (IM), social media applications, and accounts used to communicate or in the conduct of government business.

b. Depending on their content, e-messages may contain information documenting an organization's policies, programs, and activities. E-messages that are determined to be records must be preserved in accordance with regulations that are promulgated pursuant to 44 USC § 2912. E-messages are federal records if:

(1) They document evidence of a WHS-serviced Component's policies, business, or mission.

(2) The information is only available in the electronic message.

(3) The WHS-serviced Components uses the tool to convey official agency information.

(4) The e-messages are created or received in connection with the transaction of the WHS-serviced Component business, functions, or operations.

c. Functionally, electronic messaging systems are similar; all allow the transmission and receipt of messages or other content, electronically. Employees use electronic messaging systems 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.

d. Pursuant to 36 CFR § 1236, WHS-serviced Components are responsible for ensuring that records management policy, procedures, and dispositioning are incorporated into their daily business practices for electronic messaging systems.

e. WHS-serviced Components are responsible for coordinating with IT to ensure all e-messaging systems meet the requirement outlined in Subpart E and F of 36 CFR § 1236, including metadata requirements.

f. DoD authorized electronic messaging systems are provided for business use and are not to be considered personal records, although these systems may contain personal information and non-record material as part of its general use. The contents of DoD authorized electronic messaging systems are subject to FOIA, PA, records management, and security procedures. Proper business protocols that apply to any other type of communication tools, software, and applications should also be used for electronic messaging systems, such as the protection of PII.

g. Capstone is a simplified and automated approach to managing e-mail and text messages, as opposed to using either print and file systems or records management applications that require staff to file e-mail/text records individually. Using this approach, OSD can categorize, and schedule e-mail and text messages based on the work and/or position of the account owner. See Section 4.10 for more information about Capstone records.

(1) The OSD Capstone approach provides an implementable, repeatable, and defensible strategy for the management of e-mail and IM by IT service providers.

(2) Capstone officials are the only email, text messages and electronic messaging accounts that are "automatically" archived as permanent records.

(3) Email accounts of non-Capstone officials are deemed as temporary records and the emails will be destroyed by IT departments in accordance with the current version of GRS 6.1. It is the responsibility of the individual users to identify and preserve any emails, text messages, chat or social media associated with their organizations mission, functional or program records in appropriate locations outside of their email accounts.

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

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

## 6.6. MAINTENANCE OF PERSONAL STORAGE (SHARED DRIVES/ONE DRIVE)

a. OSD employees and contractors are provided with a personal storage (shared drive) or One Drive (personal cloud storage) that is inaccessible by fellow employees. These drives are designed to be used as personal storage or to share information and are often referred to as the “Name Drive,” because it is commonly named using the employees Last Name, First Initial format (Jones, B).

b. Personal storage locations should be used for personal material or professional files before joining government service. Professional files include private affairs, outside business pursuits, professional affiliations, personal social events, volunteer or community service records, or private political associations. Personal material also may include but is not limited to personal copies of employee records (e.g., SF-50, leave and earnings statements, performance evals, etc.), journals, personal correspondence, personal calendars and appointment schedules, or other personal notes.

c. Prior to departure, all OSD employees and contractors shall review these personal storage locations to ensure proper disposition of data and remove non-relevant information. OSD employees and contractors are responsible for the non-record (personal) content stored in these personal storage locations and must ensure official documents are transitioned to the appropriate organization storage locations.

## 6.7. CLOUD COMPUTING

a. Cloud computing can be separated into several service models, including but not limited to Software as a Service (SAAS), Platform as a Service (PAAS), Infrastructure as a Service (IAAS), and Storage as a Service (STAAS). Regardless of the service models, WHS-serviced Component CIOs will ensure RIM requirements are built in the applications, tools, databases, and programs developed and deployed on the OSD enterprise.

b. WHS-serviced Component CIOs will ensure cloud service providers:

(1) Are responsible for keeping the data available and accessible, and the physical environment is protected and operational.

(2) Only dispose of OSD records and information, including copies, in accordance with authorized records disposition authorities.

(3) Can store and manage OSD records and information in all formats and ensure it is secure, preserved, and accessible for as long as legally required.

(4) Conduct regular checks that ensure the integrity of long term and permanent business information is migrated as needed.

(5) Ensure that business information created, stored, and managed in the cloud:

(a) Is authentic, accurate, and trusted.

(b) Is complete and unaltered, implementing processes to ensure that business information is not inadvertently altered or incomplete.

(c) Has sufficient metadata to satisfy access and retention requirements.

(d) Is secure from unauthorized access and deletion.

(e) Is accessible, readable and can be related to other relevant business information.

(f) Is properly migrated, converted, and refreshed for managing digital information.

(g) Is properly retained and dispositioned in accordance with the OSD RDS. When records and information are due for destruction, all copies of information, including those kept on backup and other disaster recovery systems, are destroyed in accordance with authorized records disposition authorities.

(h) Is controlled and secured via guidelines for protection of OSD information in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, NIST SP 800-122, NIST SP 800-60 and NIST SP 800-37.

(6) Have documented and approved procedures to enable the migration of records and associated metadata to new storage media or formats so that records are retrievable and usable if needed to conduct agency business and to meet NARA-approved dispositions pursuant to 36 CFR §§ 1236.14 and 1236.28(f).

## 6.8. FIS

a. WHS-serviced Components will incorporate records management and archival functions into the design, development, and implementation of federal information systems.

(1) In accordance with 36 CFR § 1236 and OMB Circular No. A-130, federal agencies must record, preserve, and make accessible sufficient information to ensure the management and

accountability of agency programs, and protect the legal and financial rights of the federal government.

(2) Each WHS-serviced Component will ensure that their FIS are compliant with 36 CFR § 1236.20 and OMB No. A-130. WHS-serviced Components are to coordinate with OSD RIM Program to ensure their systems have a NARA-approved disposition schedule.

b. The functional proponents developing or purchasing information systems, including commercial off-the-shelf products, cloud computing solutions, and OSD-owned SNSs (commercial or gov't social media, wikis, blogs), are responsible for ensuring that records management functionality, policy, procedures, and dispositioning are incorporated into each system. All functional proponents will submit to the OSD RIM Program an electronic information system appraisal form (SD 828), available at https://www.esd.whs.mil/Directives/forms/sd_forms/.

c. WHS-serviced Components, CIOs, and system developers must incorporate records management controls into the FIS or integrate them into a recordkeeping system that is external to the information system itself, in accordance with 36 CFR § 1236 and DoDM 8180.01. This includes retention requirements to cover the full life cycle of information and in some cases extend beyond the disposal of information systems.

d. The following types of records management controls are needed to ensure that federal records in FIS 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.

e. Records Management Functionality. Functional proponents must integrate records management functionality and archival requirements into the design, development, and implementation of new and updated FIS.

(1) All records and information are to be retrievable and usable for as long as needed to conduct government business and mandatory retention requirements.

(2) Records are to be protected against technological obsolescence by designing and implementing migration strategies to counteract hardware and software dependencies of information systems.

(3) 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.

(4) Procedures must exist to enable the migration of records and associated metadata to new storage media or formats so that records are retrievable and usable if needed to conduct agency business and meet NARA-approved dispositions, which must be documented and approved.

f. To ensure that active digital records are readable for future use, it is recommended that a proactive migration plan be implemented. The migration plan would involve migrating records when operating systems and software applications are changed or upgraded. It is best practice to create a documentation trail when files are migrated from one system to another, and this documented file trail should include: systems and software specifications, date of migration, name, and job title of person responsible for migration, and description of any loss of information that may occur during the migration process, per 36 CFR § 1236.

g. WHS-serviced Components will include the following minimum set of controls to manage the lifecycle of information/data within each FIS per:

(1) Current version of NIST SP 800-53A. Control: DM-2, Data Retention and Disposal:

(a) Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access.

(b) Uses defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

(c) The organization, where feasible, configures its information systems to record the date PII is collected, created, or updated and when PII is to be deleted or archived under an approved record retention schedule.

(2) Current version of NIST SP 800-53. Control: MP-6(1), Media Sanitization:

(a) The organization reviews, approves, tracks, documents, and verifies media sanitization and disposal actions.

(b) Measures include organizational review and approve media to be sanitized to ensure compliance with records-retention policies.

(c) Tracking/documenting actions include, for example, listing personnel who reviewed and approved sanitization and disposal actions, types of media sanitized, specific files stored on the media, sanitization methods used, date and time of the sanitization actions, personnel who performed the sanitization, verification actions taken, personnel who performed the verification, and disposal action taken.

(3) Current version of Committee of National Security Systems Instruction (CNSSI) No. 1253. Control: AU-11(1), Audit Record Retention, Long-Term Retrieval Capability:

(a) A retention of technology to access audit records for the duration of the required retention period.

(b) Measures employed by organizations to help facilitate the retrieval of audit records include, for example, converting records to newer formats, retaining equipment capable of reading the records, and retaining necessary documentation to help organizational personnel understand how to interpret the records.

(4) Current version of CNSSI No. 1253. Control: SI-12, Information Handling and Retention. Information handling and retention requirements cover the full life cycle of information, in some cases extending beyond the disposal of information systems per records retention guidance approved by NARA in coordination with the OSD Records Administrator.

(5) WHS-serviced Components shall include the following minimum set of controls to manage the lifecycle of information/data within each FIS:

(a) Current version of NIST SP 800-53A. Control: DM-1, Minimization of Personally Identifiable Information:

(1) Identify the minimum personally identifiable information (PII) elements that are relevant and necessary to accomplish the legally authorized purpose of collection.

(2) Limit the collection and retention of PII to the minimum elements identified for the purposes described in the notice and for which the individual has provided consent; and

(3) Where feasible, and within the limits of technology, locate and remove/redact specified PII and/or use anonymization and de-identification techniques to permit use of the

retained information while reducing its sensitivity and reducing the risk resulting from disclosure.

(b) Current version of NIST SP 800-53A. Control: DM-3, Minimization of PII used in Testing, Training, And Research. The organization, where feasible, uses techniques to minimize the risk to privacy of using PII for research, testing, or training.

SECTION 7:

## 7.0. TRANSFERRING, ACCESSIONING, AND ARCHIVING OF RECORDS

### 7.1. GENERAL

a. Until the June 30, 2024, deadline in OMB/NARA M-23-07, after which FRCs will no longer accept paper records, there are two types of paper records that may be transferred to an FRC: permanent and temporary.

(1) Permanent paper records are held at the FRC for a specified period, usually 25 to 30 years, and then offered to NARA for accessioning. Permanent records have been appraised to have unique historical value to the story of the United States.

(2) Temporary paper records are held at the FRC until they are authorized for destruction and then they are disposed of by FRC personnel. The retention on temporary records is usually from 2 to 20 years after their transfer, however if they have significant value to the organization, they can be retained for 50 years or more. Only temporary records with an approved disposition authority are retired to an FRC.

(3) Unscheduled records may be transferred to the FRC if a records schedule has been submitted to NARA but not yet approved. Unscheduled records will be held at the FRC until the schedule is approved by NARA, at which point the FRC will apply the disposition instructions as described above for temporary or permanent records.

(4) Preparing records for transfer is a two-step process:

(a) First, selecting and screening the records per Sections 7.2 and 7.3 below.

(b) Second, preparing the records for actual transfer. This includes preparing the paperwork as covered in Section 9 of the AI 15, while packaging for pickup and delivery as described in Sections 7.5 and 7.6 below.

b. Permanent records that have met their disposition date (and are not already stored at an FRC) will be transferred directly to NARA via the OSD RIM Program. After the June 30, 2024, deadline in OMB/NARA M-23-07, all transfers to NARA must be in electronic format. Procedures for the transfer of electronic records to NARA are described in Section 7.7 below.

### 7.2. FILE SELECTION FOR TRANSFER TO AN FRC

To be transferred to an FRC, records must:

a. Have an approved SF-135 (see Section 7.6) and be scheduled for transfer to an FRC as indicated in the file number in the OSD RDS.

b. Be inactive or closed, i.e., they should not be needed to carry out current organizational operations.

c. Have at least a one-year retention from the date of transfer and cannot contain disposition instructions that state, “Destroy when superseded, no longer needed, or obsolete, i.e., they should not be eligible for immediate destruction, unless pre-empted by a records freeze. Records under records freeze due to litigation (see Section 6 of AI-15) can be retired to the FRC if no longer needed for current business. Records must”

## 7.3. SCREENING RECORDS PRIOR TO TRANSFER TO AN FRC

a. Permanent records, and temporary records scheduled for retention for 30 years and more, must be screened and extraneous materials removed. Remove non-record copies of documents, empty folders, folders containing temporary information, and/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 4.3).

b. Permanent files do not have to be screened while in active status. Prior to transferring to an FRC, inactive permanent files shall be screened. In deciding whether to screen, ask:

(1) Can complete folders be removed? For example, are there empty folders or contain information that is temporary, contain reference materials or redundant copies?

(2) Can disposable material be separated easily from individual folders? While screening material, referring to Section 4.9 before removing working papers.

(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 complete?

## 7.4. 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 must 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 from the FRC instead of whole boxes or accessions.

## 7.5. PACKING AND SHIPPING PROCEDURES FOR TRANSFER OF RECORDS TO AN FRC

a. 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 other than special containers**. The cubic foot GSA cartons will accommodate either letter- or legal-sized material. Special containers may be obtained for oversized materials, maps or drawings stored in tubes. In such cases, OSD RIM Program will coordinate with the FRC, including providing them with the dimensions of the special containers, and obtain its approval for using the special containers. Otherwise, non-standard boxes cannot be used.

b. Requisitioning Shipping Containers. The OSD RIM Program does not provide shipping containers for the WHS-serviced Components. Containers should be ordered directly from self-service supply centers using the stock numbers listed below. If the records will not fit into any of the containers listed below, the WHS-serviced Component should contact the OSD RIM Program for coordination with the FRC before choosing and purchasing a different container.

(1) Standard Containers. 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.

(2) Special Containers. When records being shipped are too large or too small for the standard container, 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) Microfiche Box. 14-3/4 x 6-1/2 x 4-1/2 inches, NSN: 8115-01-025-3254.

## 7.6. RECORD PREPARATION FOR TRANSFER TO THE FRC

a. The transfer of records to an FRC requires the preparation of an SF-135 (see Figure 12). Each accession of records is a block of records having the same file number, disposal authority, and disposal date. An attached box list must accompany each SF-135. Detailed instructions for completion of the SF-135 are available on the WHS RDD website (https://www.esd.whs.mil/RIM/) or can be requested from the OSD RIM Program. In addition to these instructions, OSD RIM personnel will:

(1) Describe the records adequately, including the inclusive dates in column (f) and the security classification in section 6(g) of the SF-135.

(a) Do not list classified titles or PII on the SF-135. The SF-135 and box list is considered a publicly accessible record.

(b) If records are subject to a PA SORN, the SORN number should be added to section 6(g) of the SF-135.

(c) If the records are subject to an exemption under the FOIA, such as exemption B6 for PII, B7 for Law Enforcement sensitive, etc., indicate the applicable exemptions in section 6(g) of the SF-135.

(d) If the records contain CUI, state "CUI" in section 6(f) of the SF-135, and list the CUI citations that apply (see https://www.archives.gov/cui/registry/category-list for a list of CUI designations/citations).

(2) Ensure records and information classified or marked as:

(a) NATO Classified, per USSAN Instruction 1-07. Any NATO classified records identified in DoD records after they are retired to an FRC will be handled in accordance with the DoD and NARA NATO Security Addendum to the memorandum of agreement between the DoD and NARA for records retrieval and storage services.

(b) SAP, per DoDD 5205.07.

(c) ACCM, per DoDM 5200.01 Volumes 1-3.

(3) Enter the total number of boxes in the column 6(d) on the SF-135. Except when special containers are used to package oversized materials, maps/architectural drawings, 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. Limit the number of boxes on the SF-135 to 50 cubic feet per SF-135 form.

(4) When completing column 6(h) of the SF-135, you must include the Authority Number (e.g., NC1-330-XX-XXX, N1-330-XX-XXX, DAA-0330-XXXX-XXXX, or DAA-GRS-XXXX-XXXX), which can be found in the OSD RDS in the "Authority" line for each file number (below the disposition instructions). If you cannot find the authority number or are not sure which one applies to the records you are preparing for transfer, contact the OSD RIM Program for assistance.

(5) Finish completing the SF-135 and box list. The box list should contain a folder title list of the box contents or equivalent detailed records description for every box. See Figure 12 for example box list.

b. Submit the completed SF-135 and box list via e-mail to the OSD RIM Program through the CRMO/DAFA RM of your WHS-serviced Component. The OSD RIM Program will review for completeness, enter the information into NARA's Archives and Records Centers Information System (ARCIS) database, provide the accession number (as generated by ARCIS), and submit to the appropriate FRC for processing. The FRC will review the paperwork and approve the records for transfer.

c. The OSD RIM Program will provide the CRMO/DAFA RM with a copy of the approved SF-135 containing the accession number. The WHS-serviced Component must:

(1) Place one copy in the first box of the accession before transfer.

(2) Retain one copy of the completed SF-135 and box list in your office records management files (file number 203-01).

d. 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 capability to retrieve specific papers from the FRC. When retrieval is necessary, identify the accession number and the box number that contains the specific material, along with the file title(s), if requesting individual folder(s).

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 RDS. Do not retire guide cards.

(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 records, leave 4 inches of space in each box to allow for future declassification processing.

(3) Do not pack records with different file numbers in the same box.

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

(5) Do not pack records on different media (CD-read only memory, diskettes, and microfilm) with paper records. These records will be packed separately, and the media will be identified on column (6i) of the SF-135.

(6) Maintain documentation in the original file folder if they are in good condition. Replace folders that are excessively worn or labels that are falling off. Do not place rubber bands or clips on records.

(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 from 1999 only, or from 1999 to 2001.

(8) Arrange folders in the order identified on the box list (See Figure 13). Do not disturb existing filing arrangements to make future reference easier.

(9) Do not pack binders in boxes. Remove records from the binders and place in folders and label accordingly (see Figure 5).

e. 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 (e.g., Box 1 of 5, Box 2 of 5, etc.). Each file number of records transferred will be assigned a separate accession number. See Figure 13 for placement of the accession number on the box.

## 7.7. TRANSFERS OF PERMANENT ELECTRONIC RECORDS TO NARA

a. Structured electronic records stored on shared drives or SharePoint sites. The OPR will coordinate with the OSD RIM Program to facilitate the transfer and archiving of electronic records.

(1) Only permanent electronic records shall be transferred to OSD RIM Program for archiving with NARA.

(2) Records shall be retained in original or native formats (e.g., Word, Excel, Power Point), except for e-mail records exported and captured as a part of a program, project or case file which will be converted to PDF before providing for transfer.

(3) Offices shall provide root level box list of all files being transferred. The box list will include file number, year(s) of accumulation (CY/FY), inclusive dates, and subject.

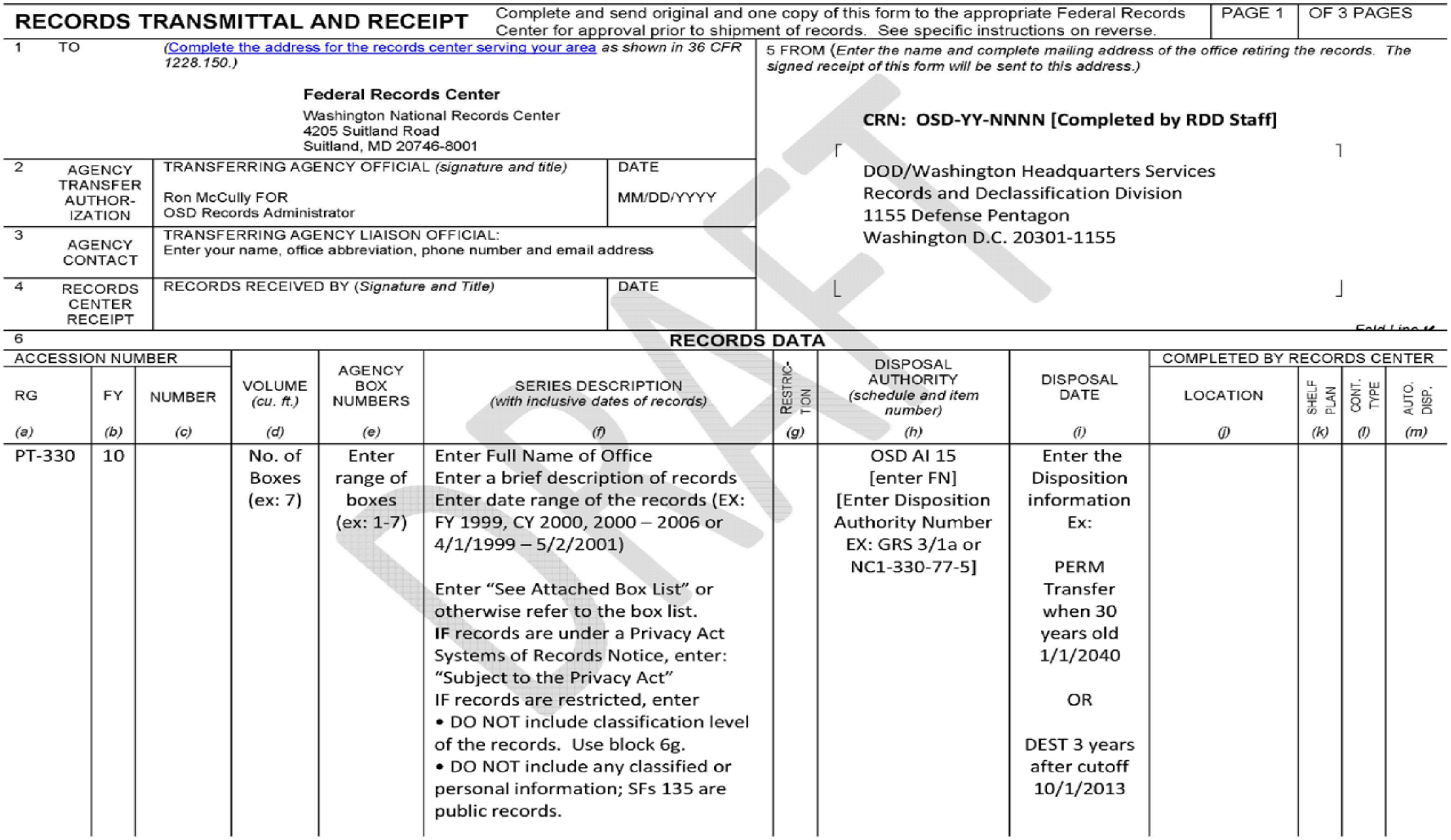
(4) Records can be saved to a DISA/JSP-compliant external hard drive or via DoD authorized File Transfer Protocol (FTP) system, such as DoD Secure Access File Exchange (SAFE), SharePoint, or OneDrive.

(5) DoD employees and contractors are not authorized to use non-DoD provided cloud storage services such as Drop Box, Google Drive, OneDrive, or other similar services to transfer or store records, working papers, or other digital information created on behalf of DoD.

(6) Storage devices, and all records contained therein, *shall no*t be password protected or encrypted when transferred to the OSD RIM Program/NARA.

(7) The OSD RIM Program will notify the OPR when NARA has accepted the permanent records. After verification of receipt by NARA, the OPR will delete/purge their local copy of the electronic records.

b. Transfer of FIS content. The OPR will coordinate with the NARA Electronic Records Division via the OSD RIM Program to transfer structured information systems and database in accordance with current guidance.



**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

2 AGENCY TRANSFER AUTHOR-IZATION — TRANSFERRING AGENCY OFFICIAL *(signature and title)*
Ron McCully FOR
OSD Records Administrator
DATE MM/DD/YYYY

3 AGENCY CONTACT — TRANSFERRING AGENCY LIAISON OFFICIAL:
Enter your name, office abbreviation, phone number and email address

4 RECORDS CENTER RECEIPT — RECORDS RECEIVED BY *(Signature and Title)* DATE

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

Fold Line

6 **RECORDS DATA**

| ACCESSION NUMBER | | | VOLUME *(cu. ft.)* | AGENCY BOX NUMBERS | SERIES DESCRIPTION *(with inclusive dates of records)* | RESTRIC-TION | DISPOSAL AUTHORITY *(schedule and item number)* | DISPOSAL DATE | COMPLETED BY RECORDS CENTER | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| RG | FY | NUMBER | | | | | | | LOCATION | SHELF PLAN | CONT. TYPE | AUTO. DISP. |
| *(a)* | *(b)* | *(c)* | *(d)* | *(e)* | *(f)* | *(g)* | *(h)* | *(i)* | *(j)* | *(k)* | *(l)* | *(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>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>PERM Transfer when 30 years old 1/1/2040<br>OR<br>DEST 3 years after cutoff 10/1/2013 | | | | |

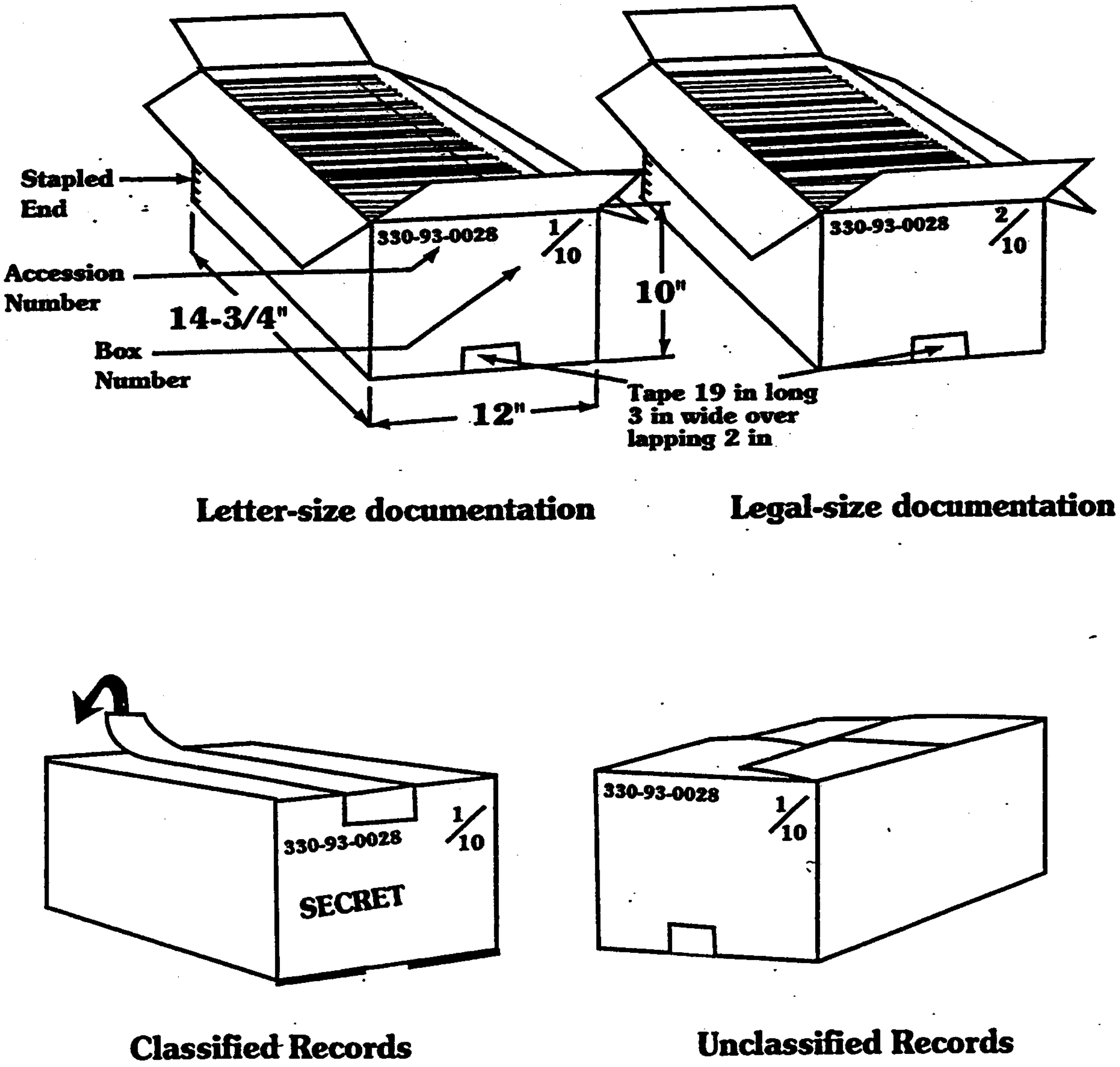
Figure 12. Example of SF-135, "Records Transmittal and Receipt"

| Office: | OASTD Public Affairs | Subject: | DoD Cooperation – Scripts and Films |
|---|---|---|---|
| NARA Job Number: NC1-330-81-001, Item 703-04.5 | | | |

| Box 1 of 4 | Folder Title |
|---|---|
| 001 | DOD FILM COLLECTION PART 2 1999 - BODY TALK 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - BOOMERANG PART 1 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - BRIDGE AT KANG SO RI 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - CABIN PRESSURE 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - COLONELS WIFE 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - CONTEMPUOUS WORDS 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - FRONT AND CENTER 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - GHOST OF CHRISTMAS PAST 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - INTO THE BREECH 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - KING OF THE GREENIE BOARD 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - LIFE OR DEATH 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - MISHAP 1999 |
| 001 | DOD FILM COLLECTION PART 2 2000 - OVERDUE AND PRESUMED LOST 2000 |
| 001 | DOD FILM COLLECTION PART 2 2000 - PEOPLE VS GUNNY 2000 |
| 001 | DOD FILM COLLECTION PART 2 2000 - PROWISES 2000 |
| 001 | DOD FILM COLLECTION PART 2 1999 - PSYCHIC WARRIOR 1999 |
| 001 | DOD FILM COLLECTION PART 2 2000 - REAL DEAL SEAL 2000 |
| 001 | DOD FILM COLLECTION PART 2 1999 - RETURN 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - ROUGE 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - RULES OF ENGAGEMENT 1999 |
| 001 | DOD FILM COLLECTION PART 2 1999 - TRUE CALLINGS 1999 |
| 001 | DOD FILM COLLECTION PART 2 2000 - WITCHES OF GULFPORT 2000 |

| Box 2 of 4 | Folder |
|---|---|
| 002 | DOD FILM COLLECTION PART 2 2000 - MEN OF HONOR 2000 |
| 002 | DOD FILM COLLECTION PART 2 2000 - RAIN 2000 |
| 002 | DOD FILM COLLECTION PART 2 2000 - RACE TO SPACE 2000 |
| 002 | DOD FILM COLLECTION PART 2 2000 - ROCKETS RED GLARE 2000 |
| 002 | DOD FILM COLLECTION PART 2 2000 - SEMPER FI 2000 |
| 002 | DOD FILM COLLECTION PART 2 2000 - U 571 2000 |

Figure 23. Example of Box List (Paper records)



Letter-size documentation

Legal-size documentation

Classified Records

Unclassified Records

Figure 34. Packing and Packaging of Records

**SECTION 8:**

## 8.0. PROTECTING OSD INFORMATION

### 8.1. GENERAL

a. NSI includes, but is not limited to, documents and materials classified accordance with Executive Order 13526, DoDI 5200.01, DoDM 5200.01 Volumes 1-3, and DoDD 5205.07.

b. OSD RIM personnel will remind OSD personnel that:

(1) All OSD employees are obligated to safeguard NSI, CUI, and PII, as described in numerous federal statutes, regulations, agency-wide directives, and DoD policies.

(2) Professional writings and other materials intended for public release are required to be submitted to the DoD security review process as specified by DoDI 5230.09.

(3) CUI and classified material will be maintained and dispositioned per the OSD RDS. Records identified as permanent per the OSD RDS will be transferred via the OSD Records Administrator in accordance with Section 7 of this PRIMER.

(4) During working hours, reasonable steps shall be taken to minimize the risk of access by unauthorized personnel (e.g., not reading, discussing, or leaving CUI unattended where unauthorized personnel are present). After working hours, CUI may be stored in unlocked containers, desks, or cabinets if Government or Government-contract building security is provided.

(5) ALL DoD unclassified information MUST BE REVIEWED AND APPROVED FOR RELEASE through standard DoD Component processes before it is provided to the public (including via posting to publicly accessible websites) in accordance with DoDI 5230.09 and applicable regulations.

### 8.2. DECLASSIFICATION OF OSD RECORDS AND INFORMATION

a. Declassification is the process of reviewing classified records and information to determine if it needs to remain classified. Per DoDI 5200.01 and DoDM 5200.01 Volumes 1-3, WHS RDD is delegated the responsibility for the administration and operation of the OSD Declassification Program.

b. The OSD Declassification Program only reviews classified records and information that meet the following requirements:

(1) Identified as permanent per their authorized file number in the OSD RDS,

(2) Are 25 years old or older, or

(3) Are specifically requested per DoDM 5230.30.

c. Automatic Declassification of NSI.

(1) Executive Order 13526 paragraph 3.3a states that records and information shall not remained classified for more than 25 years unless the records are determined exempt from automatic declassification by the agency in accordance with approved exemption authorities.

(2) WHS-serviced Components do not have the authority to apply declassification exemptions or extend classification beyond their approved security classification guide (SCG) authorizations. Therefore, it is imperative that the WHS-serviced Components alert RDD when paper or electronic classified, permanent records are nearing their disposition date, so that a review can be scheduled by RDD to apply exemptions from automatic declassification where authorized/necessary.

(3) WHS-serviced Components SHALL ensure the transfer of classified records and information to WHS RDD for declassification review per their authorized file number(s) in the OSD RDS regardless of media or format. This includes NSI created by the OCA or derivatively classified by third-party receipt or use.

## 8.3. PROTECTION OF PII.

a. DoD defines PII as information used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, biometric records, home phone numbers, other demographic, personnel, medical, and financial information. PII includes any information that is linked or linkable to a specified individual, alone, or when combined with other personal or identifying information. For purposes of this issuance, the term PII also includes personal information and information in identifiable form.

b. RIM personnel will:

(1) Ensure OSD employees who maintain records with PII comply with the applicable OSD RDS or the GRS as approved by NARA.

(2) Identify records containing PII to security managers and ensure access is limited to DoD personnel and DoD contractors who have a need to know in order to perform their duties.

(3) Remind OSD employees to:

(a) Never leave PII unattended on a desk, network printer, fax machine, or copier.

(b) Avoid transmitting PII using a fax machine unless directly to the intended recipient. If possible, scan, encrypt, or password-protect the document, and e-mail it instead.

(c) Protect against "shoulder surfing" or eavesdropping by being aware of your surroundings when processing or discussing PII and employee or contractor personnel data.

(d) Minimize the duplication and dissemination of electronic files and papers containing PII.

(e) When departing a Component, review PII eligible for destruction; for PII not eligible for destruction, transfer to an OSD employee with the need to know or who can secure it upon departure.

(f) When teleworking:

1. Do not remove records and information containing PII.

2. Do not use personal e-mail (e.g., Yahoo, Gmail, or AOL e-mail account) to conduct official business. Contractors should not utilize contractor e-mail addresses to conduct DoD business unless specifically authorized by the contract.

3. Do not send e-mails containing PII to or from your personal e-mail account, or to another person's personal e-mail account.

## 8.4. MAINTENANCE AND STORAGE OF PII ON COMPUTER NETWORK DRIVES (SHARED DRIVES) AND SHAREPOINT SITES

a. Generally, storing PII on the share drives should be avoided. If WHS-serviced Components do so, they must restrict access to those folders to those with a "need to know" by editing/setting permissions for access. RIM personnel will coordinate with supervisors, action officers, and security managers to identify the following to your WHS-serviced Component CIO or help desk:

(1) File numbers and retentions.

(2) Subject matter.

(3) Personnel who require access.

(4) Shared drive locations (file paths).

b. Review access controls at least annually or when changes to personnel and permissions occur to ensure personnel are removed or added as necessary.

c. Do not post PII anywhere on the OSD Component intranet sites, SharePoint collaboration sites, shared drives, multi-access calendars, or on the Internet (including social networking sites) that can be accessed by individuals who do not have a "need to know."

d. WHS-serviced Components will retain PII for only as long as necessary to fulfill the purpose(s) specified in public notices and in accordance with a NARA-approved record retention schedule.

e. Shared drive management roles and responsibilities are outlined in Table 7.

| Role | Responsibilities |
|---|---|
| **Section Supervisors** | • Assigns roles and responsibilities<br>• Ensures all personnel are aware of their records management responsibilities<br>• Ensures security and access rights are applied to shared drives and folders within them<br>• Develops Standard Operating Procedures |
| **Records Manager** | • Manages the implementation of these Guidelines and acts as a focal point for personnel<br>• Coordinates with personnel regarding the implementation of these guidelines<br>• Acts as the focal point with the Information Technology Branch<br>• Ensures folder structures are implemented throughout the Offices IAW AI 15<br>• Establishes and promotes naming conventions applicable at the folder, sub-folder, and file level<br>• Introduces new personnel to these guidelines and works with those leaving to ensure information is deleted and records retained<br>• Ensures the routine disposition of records using the OSD RDS<br>• Develops and disseminates records management policy and guidance<br>• Provides subject matter expertise on records management, including records disposition schedules |
| **Information Technology** | • Works with the RIM personnel or designated focal point to determine an appropriate technical configuration for shared drives<br>• Provides network and technical support, including service availability, security, capacity, migration, and backup<br>• Ensures security, sensitivity and access rights are applied to servers, software and systems used to manage shared drives |
| **All Personnel** | • Correctly files records in the correct folder structures<br>• Names information and records as per naming conventions<br>• Separates non-record drafts from final version records and files them correctly<br>• Regularly deletes out-of-date, duplicate, or unnecessary information<br>• Ensures sensitive information is appropriately filed<br>• Ensures suspicious files are not stored, and does not open those with suspect filename extensions |

Table 7. Shared Drive Management Roles and Responsibilities

## 8.5. PROTECTION OF OSD RECORDS AND INFORMATION IN FIS

a. The protection of records and information is a tenet of good records management and is a fundamental responsibility of all WHS-Serviced Components. This includes protecting the privacy of individuals and the PII collected, used, maintained, shared, and disposed of by programs and information systems.

b. Building privacy controls into FIS design and development allows WHS-Serviced Components to mitigate privacy risks to PII, thereby reducing the likelihood of FIS breaches and other privacy-related incidents.

## 8.6. PRIVACY IMPACT ASSESSMENTS (PIAs)

a. A PIA is a type of assessment conducted by an organization (typically, a government agency or corporation with access to a large amount of sensitive, private data about individuals in or flowing through its system) which audits its own processes and determines how these processes affect or might compromise the privacy of the individuals whose data it holds, collects, or processes.

b. A PIA is designed to accomplish three goals:

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

(2) Determine the risks and effects.

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

c. Each PIA will be prepared using DD Form 2930, "Privacy Impact Assessment (PIA)," and in accordance with DoDI 5400.16.

d. CRMO and DAFA RMs (not RLs) are authorized to sign PIAs as the Component records officer. CRMO and DAFA RMs will ensure the records disposition authorities cited by the program manager or designee are correct and updated as appropriate. If a records disposition authority does not exist or needs to be updated the CRMO or DAFA RM will submit an SF-115 to the OSD Records Administrator (see Section 5.4 of this PRIMER). The records disposition authority cited on the PIA must match the applicable SORN.

## 8.7. SORNs

a. In accordance with DoDD 5400.11 and the procedures in DoD 5400.11-R, each WHS-serviced Component maintaining records and information about individuals shall ensure that this data is protected from unauthorized collection, use, dissemination and/or disclosure of personal information. Records of a personal nature that are individually identifiable will be maintained in a manner that complies with the law and DoD policy.

b. A SORN is a document that describes group(s) of records under the control of any federal agency from which information is retrieved by the name of the individual or by some unique identifying number, symbol, or other identifier assigned to the individual. The Privacy Act requires each agency to distribute notice to the public of collections of PII in its systems of records, these notices are published in the Federal Register.

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

(1) Records are maintained by a Federal agency.

(2) The records contain information about an individual.

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

d. CRMOs and DAFA RMs will assist the program manager or designee with identifying the correct records disposition authority applicable to the group(s) of records identified in the SORN. If a records disposition authority does not exist or needs to be updated the CRMO or DAFA RM will submit a SF-115 to the OSD Records Administrator (see Section 5.5). The records disposition authority cited on the SORN must match the applicable SORN PIA.

SECTION 9:

## 9.0. REMOVAL OF PERSONAL AND NON-RECORD COPIES OF OSD RECORDS AND INFORMATION

### 9.1. GENERAL

a. Official e-mail and SNS accounts are provided to conduct government business and the first priority is to ensure that official records are accessible to the WHS-serviced Component prior to the departure of a Presidential Appointment (PA) or PA with Senate Confirmed (PA/PAS) official or employee.

b. DoD-provided e-mail, mobile devices, email systems, chat or messaging functions and IM accounts are not considered personal files. Non-record copies of OSD records and information, 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 Chapters 31 and 33 of 44 USC and 36 CFR §§ 1220-1236.

### 9.2. REMOVAL OF RECORDS.

a. Agency records cannot be removed from DoD custody without authorization; this includes unclassified, classified, and CUI materials, entire collections of DoD e-mails, chat, text, or IMs, and social media. Likewise, DoD employees are not authorized to remove non-record material from DoD custody without approval. This includes but is not limited to copies of paper records, working files or copies of e-mail, IM, social media, or other government materials.

b. Requests to remove non-record copies of OSD records and information will be handled in accordance with AI 15 and documented via Secretary of Defense (SD) Form 821, "Component Records Management Officer (CRMO) Checklist for Out-Processing the Departure of Presidential Appointees and Senior Officials" and SD Form 822 "Departing Employee Checklist Removal of Personal Files and Non-Record Materials from Government Custody," as appropriate.

c. Follow the procedures listed in Section 9.4 for Departing Senior Officials and 9.3 for all other Departing Employees, to include members of the Military, Civilian employees and contractors.

### 9.3. INDIVIDUAL EMPLOYEE REQUEST TO REMOVE NON-RECORD COPIES OR PERSONAL FILES

a. Employees (including political appointees) departing DoD or retiring are not authorized to remove complete collections of DoD e-mail accounts, e.g., entire inbox, sent folder, or PSTs.

b. Component heads and RIM personnel must take the following into account when considering removal:

(1) Are the records and information being requested related to the responsibilities and functions of the requestor?

(2) Will the review of the requested records interrupt day-to-day operations?

(3) Does the content of the records include any of the following?

(a) PII not related to the individual?

(b) NSI, CUI, or unclassified information that may individually or in aggregate lead to the compromise of classified information or disclosure of operations or security?

(c) Subject matter pertinent to current and pending litigation or moratoriums?

c. Records and information containing PII not related to the individual or NSI are not authorized to be released to departing employees. NSI cannot be removed from government custody.

d. Although OSD employees may be provided with non-record copies of OSD records and information, they are not authorized to be donated or transferred to any non-DoD entity, including but not limited to commercial entity, charity/non-profit, non-governmental organization, or educational activity, without the approval of the appropriate OSD authorities. Federal records including non-record copies are property of the federal government pursuant to the Federal Records Act.

e. The following materials may be removed without review:

(1) Personal calendars that reflect family, medical, or social events not related to official duties, including copies of e-mail contacts list and internet favorites.

(2) Private correspondence: thank you letters, invitations to non-official events, letters of congratulations, letters forwarding resumes of individuals for general consideration, etc.

(3) Material created by the employee before entering government service.

(4) Professional Papers: material documenting professional activities and outside business or political pursuits. Examples include non-DoD-related manuscripts and drafts for articles and books.

(5) Political materials, including speeches made before a political body that are not related to the official's duties within OSD/DoD.

(6) Volunteer and community service materials, awards, and medals.

f. WHS-serviced Component heads and RIM personnel are responsible for maintaining accountability of the records and information created and received by OSD employees and contractors assigned therein. Releases of non-record copies of OSD information must not:

(1) Diminish the records of the DoD.

(2) Violate confidentiality required by national security, privacy, or other restrictions on disclosure.

(3) Exceed normal administrative resources of the DoD.

(4) Affect the DoD's ability to invoke legal privileges

g. Contractors are not authorized to remove non-record copies of federal records or work-related e-mail. They may remove their personal records (non-work related) or employer-related information after review and approval of the Component head or authorized delegate via the SD-822.

h. OSD employees and contractors are not authorized to remove original paper records.

i. When requesting to remove non-record copies of records and information, OSD employees will:

(1) Coordinate with appointed RIM personnel to copy personal files the employee wants to retain. The employee will complete the appropriate form(s): SD 821 ("Component Records Management Officer (CRMO) Checklist for Out-processing the Departure of Presidential Appointees and Senior Officials") or SD 822 ("Departing Employee Checklist Removal of Personal and Non-Record Materials from Government Custody"), and (when applicable) SD 833 ("Departing Employee Checklist Transfer of Records between DoD/OSD Components").

(2) Coordinate with the WHS-serviced Component head or their authorized delegates to approve the appropriate form(s). The reporting office RIM personnel will retain all the forms and copies of released records.

(3) Coordinate with the Component assigned GC, security manager and the OSD RIM personnel, as applicable.

(4) Organize the files, such as sorting by subject matter, use descriptive file names and separate personal files from non-record copies of records and information.

j. Depending on the complexity and availability of personnel, Component heads or their authorized delegates at their discretion can authorize a copy of purely personal files for release, while non-record information is in the review process.

## 9.4. REMOVAL OF NON-RECORD COPIES BY POLITICAL APPOINTEES AND SENIOR OFFICIALS

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

b. Under the authority, direction, and control of ODA&M, through the Director, WHS, the OSD Records Administrator exercises approval authority for the release of non-record copies to all OSD Presidential appointees, PA/PAS officials, in accordance with 36 CFR § 1222.24(a)(6).

(1) Prior to the release of non-record copies, all OSD Presidential appointees, PA/PAS officials will sign a non-disclosure agreement provided by the OSD Records Administrator.

(2) Prior to the release of non-record copies all OSD Presidential appointees, PA/PAS officials will complete the SD Form 821. The SD Form 821 will be submitted to the OSD Records Administrator via the CRMO for signature.

(3) RIM personnel will assist the departing senior official or staff with:

(a) Segregating personal files for removal and the deletion of files not requested.

(b) Identifying of non-record information requested for removal.

(c) Coordinating with appropriate IT staff, Component security manager, Component assigned GC and appropriate program offices for the review of requested information.

(4) The WHS-serviced Component's GC will:

(a) Ensure the requested copies of non-record information is not subject to disposition suspension such as records holds, freezes, moratoriums, or preservation orders.

(b) Affect the DoD's ability to invoke legal privileges.

(c) Coordinate with Cabinet officials regarding the donation of non-record information to government or private institutions.

(5) Per DoDM 5200.01, Volume 1 and DoD I 5200.48, active Component security officers are responsible for reviewing requested information to identify content that may:

(a) Contain proprietary information or PII.

(b) Concern national or international interest.

(c) Affect national security policy, foreign relations, or ongoing negotiations.

(d) Identify a subject(s) of potential controversy among the DoD Components or with other federal agencies.

(e) Consult on requested documents and recommend releasability of OSD information,

(f) Referring records and information not approved for release to the OCA.

## 9.5. DONATION OF NON-RECORD COPIES AND PERSONAL FILES.

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

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

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

(2) These restrictions pertain to:

(a) Potential violations of personal privacy.

(b) Protection of NSI and CUI.

(c) Statements made by or to the donor in confidence.

(d) Materials or information that might prove prejudicial to the conduct of the foreign relations of the United States.

(e) Material relating to law enforcement investigations.

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

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

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

(2) Complete the SD Forms 821 and 822. The SD Forms will be submitted to the OSD Records Administrator via the CRMO.

(3) Provide the following information:

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

(b) A list containing:

1. Identification of the documents or files.

2. The inclusive dates.

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

d. Access to personal files and non-record material donated by an official to an institution for historical preservation will be in accordance with the instrument of gift signed by the official and the institution. Access to federal records by former officials which they originated, reviewed, signed, or received while serving as PA/PAS can be granted in accordance with AI 50.

**SECTION 10:**

## 10.0. MANAGING RECORDS OF DoD ADVISORY COMMITTEES

### 10.1. DoD ADVISORY COMMITTEES RECORDS MANAGEMENT PROGRAM

a. DoD advisory committees include but are not limited to:

(1) DoD- or OSD-wide federal advisory committees, whether statutory or discretionary, established pursuant to Chapter 10 of 5 USC, of Public Law 92-463, also known and referred to in this PRIMER as the "Federal Advisory Committee Act" or "FACA."

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

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

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

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

b. Most records created and received by advisory committees will fall into one of two major categories (for additional information regarding inclusive records refer to the OSD RDS, GRS 6.2, or consult with the OSD RIM Program):

(1) Operational/Mission. Records relating to the establishment and primary purpose of the Federal advisory committees, and boards, commissions, and task forces (BCTFs) include but are not limited to:

(a) Charters (original, renewal, re-establishment, and amended), enacting legislation, letters to Congress, records related to committee findings and recommendations, and organization charts.

(b) Records related to research collected or created, including, but not limited to: records related to research studies and other projects, including unpublished studies, reports, and research materials (may include electronic data), raw data files created in connection with research studies, and other projects where the information has been consolidated or aggregated for analyses, reports, or studies.

(c) Audiotapes, videotapes, and/or other recordings of meetings and hearings not fully transcribed and captioned, captioned formal and informal analog or digital photographs, and any related finding aids, of committee members and staff, meetings, or hearings.

(2) Administrative/housekeeping. Records relating to areas of an administrative nature, including routine correspondence (e.g., intra-agency, with committee members, or the public) regarding logistics (e.g., agenda planning, meeting arrangements, administrative issues), public requests for information (RFI) records, and non-substantive web content (i.e., requests for correction of incorrect links or content posted, requests for removal of duplicate information, user logs, search engine logs, and/ or audit logs).

## 10.2. MANAGEMENT OF DoD ADVISORY COMMITTEE ACT RECORDS

a. All DoD advisory committees will assign an RL for the implementation and establishment of RIM programs. The RL will provide oversight and archiving of their advisory committee's records. Records management personnel for these federal advisory committees and BCTFs will have the same duties and responsibilities of OSD CRMOs. DoD advisory committee RL responsibilities include but are not limited to:

(1) Ensuring the committee meets all records management requirements in accordance with 5 USC § 1007 of Public Law 92-463 and 41 CFR § 102-3.175.

(2) Annually notifying the OSD Records Administrator when copies of reports and other non-record materials are made available to Congress, the Library of Congress, or a similar entity.

(3) Ensuring all committee staff, including the Designated Federal Officer (DFO), paid and unpaid personnel take the OSD RIM Training for federal advisory committees within 90 days of stand up or on-boarding.

b. Heads of DoD advisory committees are responsible for ensuring each DoD advisory committees retains:

(1) Charter and membership documentation. A set of filed charters for each federal advisory committee and membership lists for each advisory committee and subcommittee.

(2) Annual comprehensive review documentation. Copies of the information provided as the agency's portion of the annual comprehensive review of FACAs, prepared in accordance with 41 CFR § 102-3.175(b).

(3) Agency guidelines. Agency guidelines are maintained and updated on committee management operations and procedures.

(4) Closed meeting determinations. Agency determinations to close or partially close advisory committee meetings required by 41 CFR § 102–3.105

c. DoD advisory committee members may not use personal e-mail accounts, unauthorized internet applications or SNSs to conduct official agency business, except when authorized by DoD 5500.07-R.

## 10.3. PROTECTION OF NSI

a. All DoD advisory committee personnel are required to manage NSI in accordance with E.O 13526, DoDI 5200.01, DoDM 5200.01 Volumes 1-3, DoDI 5200.48, and DODD 5205.07 (for more information see Section 8 of this PRIMER).

b. Personnel must pay special attention to CUI and NSI they collect and receive.

c. Federal advisory committees and BCTFs do not have release authority, unless specifically granted such authority within their charters. Without such authority, release is the responsibility of the OCA.

d. The majority of the NSI and CUI will be derivatively classified and must be returned to the office of origin as the release authority in accordance with DoDM 5200.01 Volumes 1-3.

e. DoD advisory committees may use shared network drives to maintain electronic records in their native formats, apart from e-mail. Advisory committee RLs must work with IT support offices to protect records from unauthorized access, deletion, or incorporation into the records of host Components and offices.

(1) The heads of DoD advisory committees, DFOs, IT support offices, and RLs must control access to electronic records according to below-defined criteria:

(a) Access is limited and partitioned away from other OSD Component reporting offices. Federal advisory committee records are subject to 5 USC § 1009(b) and 5 USC § 552 and must be made available to the public upon request.

(b) Intermixing DoD Component or supporting OSD Component records with federal advisory committee records puts DoD at increased risk of breach or spillage of records or unauthorized release of government information. Additional information for managing electronic records can be found in Section 6 of this PRIMER.

(2) Use of personal e-mail, SNSs or unapproved collaboration software (i.e., G-Suites/Drop box, OneDrive, etc.) to conduct government business is not authorized. Federal employees, military service members (including volunteers) cannot use their personnel e-mail and social media accounts per Public Law 113-187.

## 10.4. TRANSFERS OF DoD ADVISORY COMMITTEE RECORDS

a. DoD advisory committee records will follow procedures for archiving paper and electronic records and information per Section 7 of this PRIMER.

b. Permanent DoD advisory committee records are identified in GRS 6.2 and must be archived per the below procedures:

(1) Committee records generated by or for a FACA must be retained for the duration of the advisory committee in accordance with 41 CFR § 102-3.175(e).

(2) All terminating committees and sub-committees shall transfer permanent committee records to NARA (via the OSD RIM Program) when a committee terminates, or annually when the records are 15 years old.

(3) On termination of the DoD advisory committee, the records will be processed in accordance with the AI 15, this PRIMER, and the applicable GRS, and transferred to the OSD RIM Program.

(4) Prior to transferring records, the RL for each DoD advisory committee shall:

(a) Complete the SF-258 and inventory their records using the Checklist for Preparing Records for Transfer to NARA under GRS 6.2, Federal Advisory Committee Records. This inventory list must accompany the SF-258 and submitted to the OSD Records Administrator. This checklist is available in the FACA section of the OSD RIM Program website (https://www.esd.whs.mil/RIM/).

(b) Label and package paper records into NARA standard archiving box(es) (see Sections 4 and 7 of this PRIMER). Temporary records that have not met or surpassed their retention can be transferred to an FRC until June 30, 2024. After this date, temporary and permanent FACA materials must be electronic, either created/received electronically or digitized in accordance with 36 CFR § 1236 Subpart D (temporary records) and Subpart E (permanent records).

(c) Transfer electronic records and information (including NSI) via authorized external hard drive/DVD or transferred via and DoD-approved FTP sites/applications and submitted to the OSD Records Administrator with the above-mentioned documentation.

(d) With the exception of e-mail records, all electronic records can be maintained in their native formats. E-mail records must be converted to PDF to ensure long term access and readability. For Federal advisory committees using non-DoD e-mail system the committee shall coordinate with their IT service provider to download emails to a readable format and transfer to the OSD RIM Program.

(e) CUI and classified information will be marked per DoDM 5200.01 Volumes 1-3 and DoDI 5200.48, and annotated as appropriate on the SF-258, SF-135, and inventory list in accordance with the instructions in Section 7 of this PRIMER. The records and information containing the following types of information are not authorized for transfer to the OSD RIM Program, NARA, or any FRC, and must be returned to the OCA or the DoD SAP policy office as appropriate:

1. NATO Classified, per USSAN Instruction 1-07. Any NATO classified records identified in DoD records after they are retired to an FRC will be handled in accordance with the DoD and NARA NATO Security Addendum to the memorandum of agreement between the DoD and NARA for records retrieval and storage services.

2. SAP, per DoDD 5205.07.

3. ACCM, per DoDM 5200.01 Volumes 1-3.

(f) Classified DoD advisory committee records will be transferred to the OSD Declassification Program, where they will be reviewed for declassification in accordance with Executive Order 13526.

(g) The OSD Declassification Program will NOT make a Declassify/Exempt decision on DoD advisory committee classified records and information. Declassify/Exempt decisions are referred to the OCA.

(h) Upon completion of the Kyl-Lott review, the OSD RIM Program will transfer the Federal advisory committee records and information to NARA per GRS 6.2.

**SECTION 11:**

## 11.0. RIM EVALUATIONS

### 11.1. EVALUATIONS OF WHS-SERVICED COMPONENT RIM PROGRAMS

a. The OSD RIM Program evaluation provides a systematic method for collecting and analyzing information to judge the effectiveness and efficiency of RIM requirements, policies, and programs.

b. It is the responsibility of the OSD RIM Program is to ensure the WHS-serviced Components are maintaining their records and information in a manner that:

(1) Does not increase the risk of the destruction, compromise (breach or spillage) or alienation.

(2) Executes approved disposition authorities.

(3) Ensures the migration of electronic records and information across platforms.

(4) Identifies all records, subject matter, FIS, and content for which the WHS-serviced Components have responsibility. This includes, but is not limited to, e-mail, social media, text messages, chat, and audio/video. This also includes new programs, missions, functions, reports, or FIS received by the Component or reporting offices due to reorganization, legislation, or transfer of function.

### 11.2. OSD RIM PROGRAM EVALUATION CRITERIA

At a minimum, the OSD RIM Program will evaluate using the following criteria (see WHS Form 17):

a. RIM oversight and compliance. This includes, but is not limited to, assignment of CRMO or DAFA RM, assignment of RL(s) within reporting offices, performance of internal self-evaluations for all reporting offices within the Component, retention of documentation pertaining to the oversight of the RIM Program within the Component, and implementation of training across the Component.

b. RIM program implementation. This includes, but is not limited to, accounting for all records created, received, and maintained to fulfill the mission of the Component, implementation of file plans, identification of essential records, and protection of classified information/PII/CUI within records.

c. Disposition of records. This includes, but is not limited to, destroying temporary records when eligible, working with RDD to accession permanent records to NARA or retire legacy hard copy records to FRCs, following appropriate procedures for the unauthorized destruction, damage, or alienation of federal records, and implementation of preservation notices.

d. Hard copy records management. This includes, but is not limited to, establishing and implementing a plan to transition hard copy records to a fully electronic recordkeeping environment by June 30, 2024 in accordance with OMB/NARA M-23-07 (or requesting an exception to NARA via the OSD Records Administrator), and maintaining any legacy hard copy records in a manner consistent with the AI 15 and this PRIMER until such time as the records are transferred to an FRC/NARA prior June 30, 2024 or digitized in accordance with 36 CFR § 1236 Subparts D and E.

e. Electronic records management. This includes but is not limited to, whether electronic records are maintained in a structure consistent with the AI 15, the OSD RDS, and this PRIMER (to include e-mail, social media, text messages, etc.).

f. Procedures for departing personnel. This includes, but is not limited to, ensuring departing personnel are filing records in appropriate areas before departing, ensuring departing personnel complete SD 821 and/or SD 822 forms, ensuring senior officials receive RIM exit briefings, and ensuring OSD records and information are not removed without appropriate review and approval.

g. FIS records management. This includes, but is not limited to, ensuring the Component's FIS is scheduled or otherwise categorized to a file number in the RDS, ensuring that records management functionality is incorporated into the design, development, and implementation of its FIS, and establishing processes and procedure to manage/migrate records when an FIS is decommissioned.

## **11.3. INTERNAL WHS-SERVICED COMPONENTS RIM EVALUATIONS**.

WHS-serviced Component CRMOs and DAFA RMs will:

a. Conduct internal evaluations to ensure compliance with the AI 15, the OSD RDS, and this PRIMER.

(2) Conduct internal RIM evaluations at least every two years, or upon major reorganization.

(3) Ensure at least 10 percent of the WHS-serviced Component's reporting offices are evaluated in each evaluation period.

b. In addition to criteria in Section 11.2, WHS-serviced Components will evaluate themselves in the following areas:

(1) Creation, preservation, migration, and maintenance of electronic records. This includes the appropriate use of the shared drives, SharePoint, and/or Microsoft Teams to file records and information, and development of file plans annually to document retention and disposition of records.

(2) Review of records schedules are for accuracy and currency on an annual basis. This includes the submission of draft disposition authorities to the OSD RIM Program for new records, and records related to new program, mission, and function areas.

(3) Ensuring access controls for electronic records (including FIS) and legacy paper records are developed, implemented, and communicated to all Component personnel.

(4) Providing oversight to ensure safeguards are in place to prevent departing employees and officials from removing of OSD records and information, regardless of format, including copies of email accounts.

(5) Ensuring all records are maintained and dispositioned in accordance with the approved disposition schedules cited in the OSD RDS. This includes identification and incorporation of RIM controls into FIS, and development and implementation of internal Standard Operating Procedures (SOPs) for maintenance and disposition of Component records.

(6) Ensuring OSD employees, military service members, contractors, and volunteers have all completed annual online RIM training and that appointed CRMO/DAFA/RL personnel have successfully completed required RDD-RIM Training within 3 months of appointment.

(7) Investigating and reporting unauthorized destruction, removal, and alienation of OSD records and information, if applicable, including implementation of controls or SOP to migrate future unauthorized dispositions.

(8) Establishing procedures to include the CRMO, DAFA RM or RL/RC in the process for design, acquisition, and implementation of WHS-serviced Component FIS.

## 11.4. DOCUMENTING INTERNAL EVALUATIONS

a. All WHS-serviced Components' internal evaluations will document criteria, office(s) evaluated, results, findings, and recommendations in writing and will be signed by the Component head or designated signature authority. The Component will establish a plan of actions and milestones (POAM), also signed by the Component head or designated signature authority, to resolve all recommendations and findings

b. WHS-serviced Components may develop their own evaluation criteria documentation or use the WHS-17 or SD-823 as a basis for internal evaluations.

## 12.0. GLOSSARY

### 12.1. ACRONYMS

| | |
|---|---|
| ACCM | Alternative Compensatory Control Measures |
| AI | Administrative Instruction |
| ARCIS | Archives and Records Centers Information System |
| ASD | Assistant Secretary of Defense |
| ATSD | Assistant to the Secretary of Defense |
| BCTF | Boards, Committees and Task Forces |
| CD | Compact Disk |
| CFA | Current Files Area |
| CFR | Code of Federal Regulation |
| CIO | Chief Information Officer |
| CMO | Chief Management Officer |
| CRMO | Component Records Management Officer |
| CUI | Controlled Unclassified Information |
| CY | Calendar Year |
| DAFA | Defense Agency/DoD Field Activity |
| DD Form | Department of Defense Form |
| DFO | Designated Federal Officer |
| DM | Data Minimization and Retention |
| DoD | Department of Defense |
| DoDD | DoD Directive |
| DoDI | DoD Instruction |
| DoDM | DoD Manual |
| DVD | Digital Video Disk |
| E-mail | Electronic Mail |
| E.O. | Executive Order |
| ERA | Electronic Records Archive |
| ERM | Electronic Records Management |
| ESD | Executive Services Directorate |
| FACA | Federal Advisory Committee Act |
| FIS | Federal Information System |
| FOIA | Freedom of Information Act |
| FRC | Federal Records Center |
| FTP | File Transfer Protocol |

| | |
|---|---|
| FY | Fiscal Year |
| GC | General Counsel |
| GRS | General Records Schedule |
| GSA | General Services Administration |
| HR | Human Resources |
| IAW | In accordance with |
| IM | Instant Message |
| IT | Information Technology |
| JWICS | Joint Worldwide Intelligence Communications System |
| NARA | National Archives and Records Agency |
| NATO | North Atlantic Treaty Organization |
| NDAA | National Defense Authorization Act |
| NIST | National Institute of Standards and Technology |
| NSI | National Security Information |
| OCA | Original Classification Authority |
| OMB | Office of Management and Budget |
| OPR | Office of Primary Responsibility |
| OSD | Office of the Secretary of Defense |
| PA | Privacy Act |
| PAAS | Platform as a Service |
| PA/PAS | Presidentially Appointed-Senate Confirmed |
| PDF | Portable Document Format |
| PERM | Permanent |
| PIA | Privacy Impact Assessments |
| PII | Personally Identifiable Information |
| POAM | Plan of Actions and Milestones |
| POC | Point of Contact |
| PRIMER | Procedural Resource and Instructional Manual |
| RA | Records Administrator |
| RC | Records Custodian |
| RDS | Records Disposition Schedules |
| RFI | Request for Information |
| RIM | Records and Information Management |
| RL | Records Liaison |
| RM | Records Manager |
| SAAS | Software as a Service |

| | |
|---|---|
| SAFE | Secure Access File Exchange |
| SAO | Senior Agency Official |
| SAORM | Senior Agency Official for Records Management |
| SAP | Special Access Program |
| SCI | Sensitive Compartmented Information |
| SD | Secretary of Defense |
| SF | Standard Form |
| SIPRNET | Secret Internet Protocol Router Network |
| SNS | Social Networking Site |
| SORN | System of Records Notice |
| SP | Special Publication |
| STAAS | Storage as a Service |
| TEMP | Temporary |
| USC | United States Code |
| USD | Under Secretary of Defense |
| URL | Uniform Resource Locator |
| USSAN | United States Security Authority for NATO |
| WHS | Washington Headquarters Services |
| WNRC | Washington National Records Center |

## 12.2. DEFINITIONS

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

| | |
|---|---|
| **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 number** | The NARA or Archives and Records Centers Information System (ARCIS) assigned tracking number for the transfer of agency records to the National Archives or FRC (see Retirement). |
| **Accession** | The transfer of the legal and physical custody of permanent records from an agency to the National Archives. |
| **Active records** | See current 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. |
| **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. |
| **Centralized filing** | A system in which the records for several people or units are in one, central location: and, under the control of records personnel or in the case of large, centralized filing systems, several people. |
| **CFA** | The area where current records are physically maintained, usually in a location that provides convenient access for reference and retrieval. |
| **Classified National Security Information** | Information that has been determined pursuant to E.O. 13526, "Classified National Security Information," December 29, 2009, or any predecessor order, to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form. |
| **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" NIST SP 800-145. |
| **COFF** | Cut off is the 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. |
| **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. |
| **Cutoff instructions** | Instructions for transferring the records to a records center, if applicable. The timing should be based on the length of time after the cut off, although it may be expressed either as "Transfer ___ years after cut off" or "Transfer when ___ years old." The record center should be specified if it is an exception to the general rule. |
| **Decentralized filing** | The physical documents are located across the entire office. Documents could be stored in end users' offices, workstations, or other workroom space. |
| **Determination of Definition** | The Archivist's determination whether recorded information, regardless of whether it exists in physical, digital, or electronic form, is a record as defined in subsection (a) of 44 USC § 3301 shall be binding on all federal agencies. |
| **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:<br>• Disposal of temporary records by destruction or donation,<br>• Transfer of records to Federal agency storage facilities or FRCs,<br>• Transfer to the Archives of the United States, records determined to have sufficient historical or other value to warrant continued preservation, or<br>• 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 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/RDS contains the only authorized disposition schedule for OSD. See also" GRS. |
| **Electronic discovery** | The process of identifying, preserving, collecting, preparing, analyzing, reviewing, and producing electronically stored information ("ESI") relevant to pending or anticipated litigation, or requested in government inquiries |
| **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** | 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 also: historical value. |
| **FIS** | An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency. (40 USC § 11331) |
| **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." |
| **Files cut off** | The point when transitions from an active file to "inactive" or a "closed file" when no longer needed for current business operations are moved to an inactive status. |
| **File number** | A numerical designator which identifies the record and includes the title, description, cut off and disposition instructions |
| **File plan** | A document containing the identifying file number, title or description, location, and disposition authority of files held in an office. |
| **File series** | A file series is a group of records that are created, used, and filed as a unit because they relate to a particular subject or function, result from the same activity, or have a particular physical form |
| **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 to contract this service out to civilian enterprises. |
| **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. |
| **Inactive records** | Records that are no longer required in the conduct of current business and therefore can be transferred to an FRC/NARA or destroyed, per approved disposition schedule. |
| **Information life cycle** | Means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition, to include destruction and deletion. |
| **Information system** | Means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 USC § 3502). |
| **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:<br>• 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.<br>• Extra copies of documents (but only if the sole reason such copies are preserved is for convenience of reference).<br>• 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. |
| **Senior Officials** | • Presidentially appointed, Senate-confirmed Officials (PAS): Civilian officials appointed by the President, by and with the advice and consent of the Senate, to positions within the Department of Defense.<br>• Schedule “C.”: As defined in Section 6.2 of title 5, Code of Federal Regulations, positions established in the excepted service with duties of a confidential or policy determining character. Typically, Schedule C employees serve in General Schedule grades.<br>• Detailed Official: For the purpose of this form, a government employee of an agency or department other than the Department of Defense, who is temporarily assigned to serve in an approved billet within OSD for a specified period of time, and who is expected to return to his or her parent agency or department at the end of that period.<br>• Non-career SES: A member of the SES whose appointment is approved by the White House and the Office of Personnel Management and who serves at the pleasure of the appointing officer.<br>• Commissioned Officers: O-6 and above including General or Flag Officers, as defined in 10 USC § 101(b)(2), (b)(4) or (b)(5), or temporarily assigned to serve in an approved billet within OSD or DAFA. |
| **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. |
| **Privacy Act System of Records** | A group of records under the control of a DoD Component from which personal information about an individual is retrieved by the name of the individual, or by some other identifying number, symbol, or other identifying assigned, that is unique to the individual. |
| **PIA** | A type of assessment conducted by an organization (typically, a government agency or corporation with access to a large amount of sensitive, private data about individuals in or flowing through its system) which audits its own |

| | |
|---|---|
| | processes and sees how these processes affect or might compromise the privacy of the individuals whose data it holds, collects, or processes. |
| **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." |
| **RIM** | (Records and information management) The standardized process to create, distribute, use, maintain and dispose of records and information, regardless of media, format, or storage location, in a manner consistent with an organization's business priorities and applicable legal and regulatory requirements. |
| **Records center** | See FRC. |
| **Records control schedule** | A listing prepared by each OSD office identifying the records series, filing arrangement, and ultimate disposition of all files maintained. |
| **RDS** | 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** | (Also referred to as federal records or official 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. |
| **Reference copies** | A collection of extra copies of official records on a specific action used for ready reference are called reference copies. Includes 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.) |

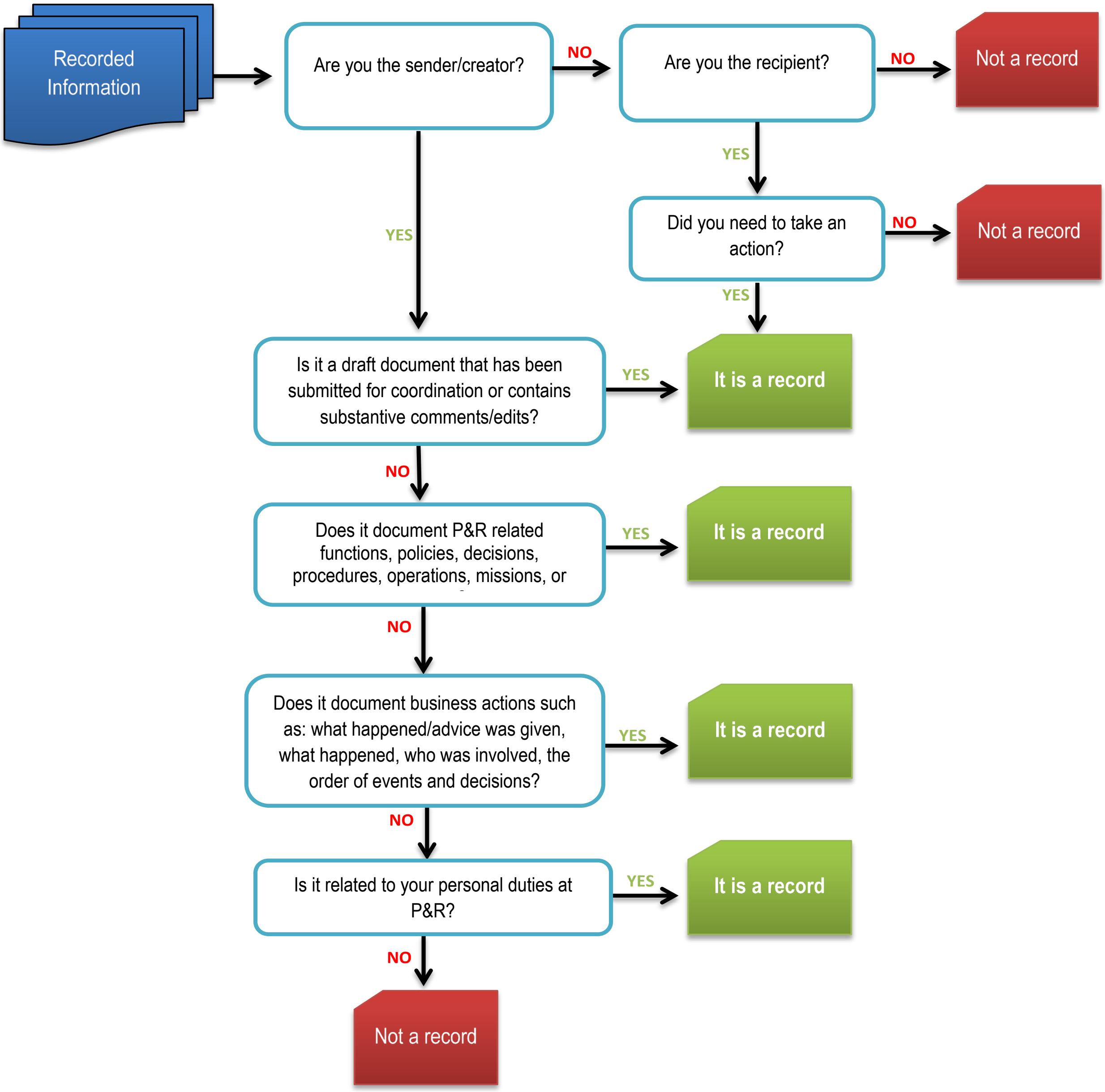
| | |
|---|---|
| **Retention period** | The time period that a specific series of records is to be kept. Also called "retention standard." |
| **Retirement** | The movement of inactive files having a permanent or long-term value to an FRC for storage, servicing, and ultimate disposition. See transfer. |
| **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." |
| **SORN** | A public notice detailing the conditions, contents, and procedures for a system of records, including system identifications, system locations, categories of records and individuals contained in the system, access procedures, and legal exemptions. |
| **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. |
| **Subject file** | elate to any type of topic, such as an action, event, person, place, project, or other subject. They are distinguished from case files, which relate to a situation affecting or relating to some investigation or administrative action. |
| **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. |
| **Temporary records** | Records designated for retention for a specified period and then authorized to be destroyed in the current file area (CFA). Temporary records are often found among housekeeping records or administrative files. |
| **Transfer** | The movement of records out of office space to a repository but not necessarily an FRC. See: retirement. |
| **Transitory** | 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. Until a final disposition is approved, all unscheduled records must be treated as permanent. |
| **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** | Documents essential to the continued functioning or reconstitution of an organization during and after an emergency and 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-interest's records that are duplicates or extra copies of originals stored off-site. |

|  |  |
|---|---|
| **Washington National Records Center** | The official off-site repository for OSD records – FRC 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/papers** | 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. |

## SECTION 13:

## 13.0. APPENDIXES

### APPENDIX A: RECORDS DECISION TREE


Recorded Information
Are you the sender/creator?
NO
Are you the recipient?
NO
Not a record
YES
Did you need to take an action?
NO
Not a record
YES
YES
It is a record
Is it a draft document that has been submitted for coordination or contains substantive comments/edits?
YES
It is a record
NO
Does it document P&R related functions, policies, decisions, procedures, operations, missions, or
YES
It is a record
NO
Does it document business actions such as: what happened/advice was given, what happened, who was involved, the order of events and decisions?
YES
It is a record
NO
Is it related to your personal duties at P&R?
YES
It is a record
NO
Not a record

## APPENDIX B: ELECTRONIC FILE ORGANIZATION TIPS

| **Common File Naming Conventions** | |
|---|---|
| **Avoid Special Characters** | . \ / : * ? “ < > \| [ ] & $ ,<br>The characters listed above are frequently used for specific tasks in an electronic environment. |
| | A forward slash is used to identify folder levels in Microsoft products, while Mac operating systems use the colon. |
| | Periods have a specific function in a file name, which is to tell the computer program where the file-name extension begins, such as .jpg and .doc. Using them in a file name could result in lost files or errors. An underscore or space can be used instead. |
| **Be Concise** | Generally, about 25 characters is a sufficient length to capture enough descriptive information for naming a record. |
| | The acceptable length of file names may be different among operating systems and software. Some systems allow up to 256 characters, while others allow far fewer. |
| | Avoid using words such as "a", "and', "of", "the" and "to" unless they contribute to the meaning of the file name. |
| | Use standard and appropriate abbreviations, when possible, to simplify the file name if other personnel will still know what the word is. The GPO STYLE MANUAL provides a useful list of common abbreviations. |
| **Use Descriptive Information** | Include all necessary descriptive information in the file name, independent of where it is stored. Files are frequently copied to other folders, downloaded, and emailed. It is important to ensure that the file name, independent of the folder where the original file lives, is sufficiently descriptive. |
| **Record Retention** | Records should be maintained according to the organization record retention schedule. |

| | |
|---|---|
| | The purpose of organizing an agency’s electronic records is to enable accessibility not only by current users, but by future users as well. Records retention schedules are applied to electronic records just as they are to paper records. |
| **Dates** | Having a relevant date associated with the file is essential. One way to prevent confusion is to embed the relevant date (the date that the file was created or revised) in the file name itself.<br>Though many operating systems store this information with the file, as users move the file among folders and computers and as the file is re-saved as[1] revisions are made, those dates change. |
| | Avoid naming a file with dates that do not make sense in relation to its original date of creation. |
| | For some types of records, it is useful to have the date at the beginning of the file name, while others might prefer it at the end. Either way, it is a useful sorting tool when the files are organized. Be sure to keep it consistent within that record type. |
| | If sorting a file chronologically is necessary for a particular record type, the date in a file name should use the international date format, which specifies numeric representations of date and time to be used in electronic format (ISO 8601).<br>The international standard date notation is: YYYY_MM_DD or YYYYMMDD, where YYYY is the year, MM is the month of the year between 01 (January) and 12 (December), and DD is the day of the month between 01 and 31. For example, January 31, 2013, is written as 2013_01_31 or 20130131. |

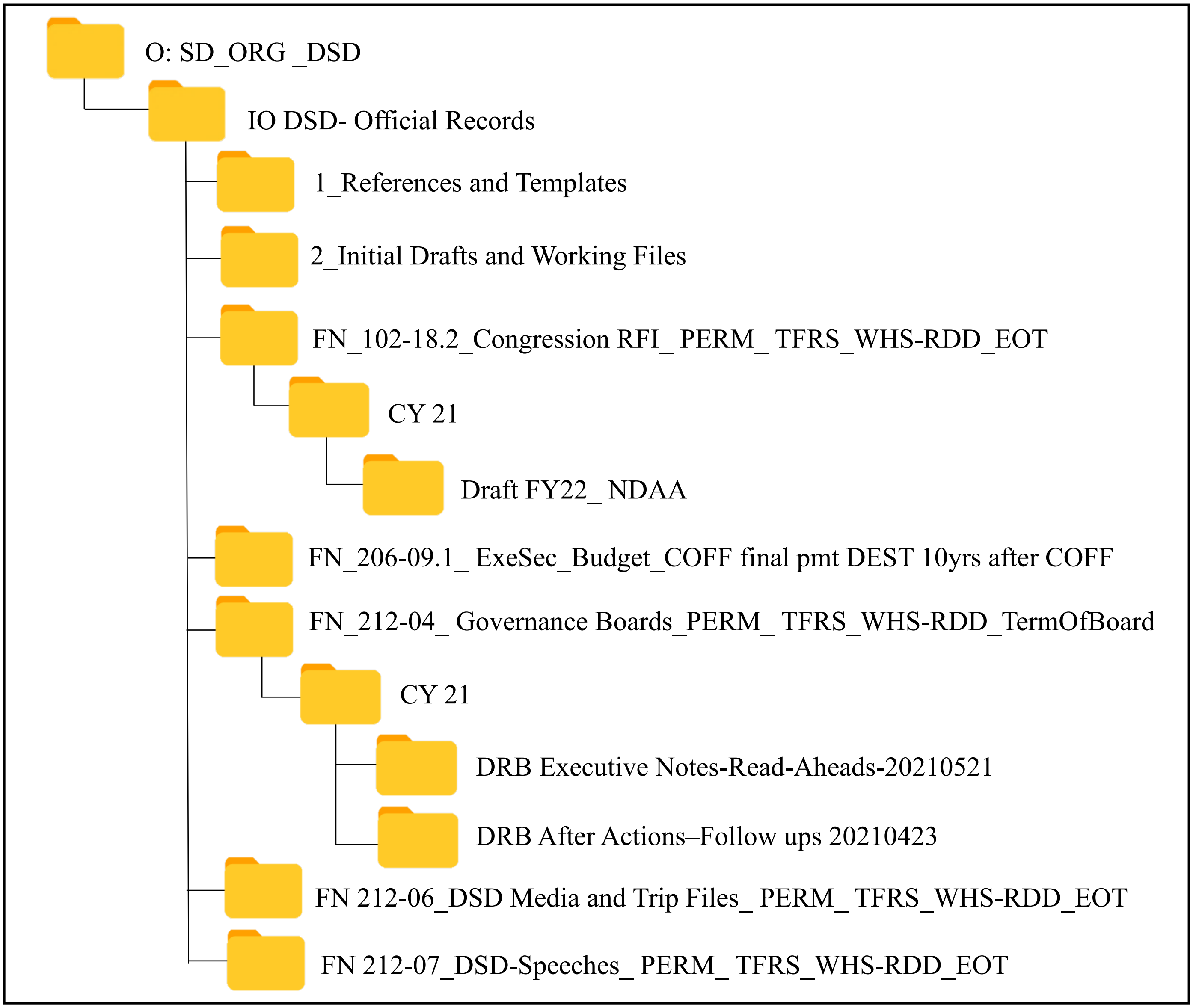
[1] Source: NIST Quality Management System Analysis – Evaluating Essential Elements[1]
https://www.nist.gov/system/files/documents/pml/wmd/labmetrology/ElectronicFileOrganizationTips-2016-03.pdf

|  |  |
|---|---|
|  | Other date formats can be used when a record will not be sorted by date or if another method will be used to organize records chronologically (e.g., file folder names by date or event). |
| **Drafts and Revisions** | To manage drafts and revisions more easily, include a version number on these documents. A file will frequently have multiple versions, especially when it is created by a workgroup. |
|  | An easy way to do this is to use the letter v to represent version number. Then, v01, v02, v03 can be added as needed to a file and the main file name can stay the same. This is more effective than other terms, such as: update, new, old, etc. |
|  | The term FINAL can also be used to indicate the final version of a record. This can be helpful to quickly identify the official version. |
| **Be Consistent** | The most important rule of file-naming is to be consistent. Some choices will need to be made about organization that affects the entire Program - where to include the date, what abbreviations to use, etc. Regardless of what the group decides, it is only effective if everyone follows the rules consistently. |
| **Exceptions** | There will be exceptions. Remember that these tips will not apply absolutely to every situation; it should be used as a guide to encourage the development of consistent folder and file-naming practices. |
| **Organized File Structure** | Support records management by providing an understandable and accessible location for all records which encourages users to work within it. |
|  | Reduces the risk of critical information being lost within a file system. |
|  | Motivates users to move records out of personal drives or email accounts where it may be deleted without anyone knowing it existed. |
| **Limitations** | A filing system does not prevent users from placing records in the wrong folder if they have access to it. A filing structure will only be effective if users are able to use it. Poorly constructed filing structure will only discourage personnel from using it and exacerbate records management |

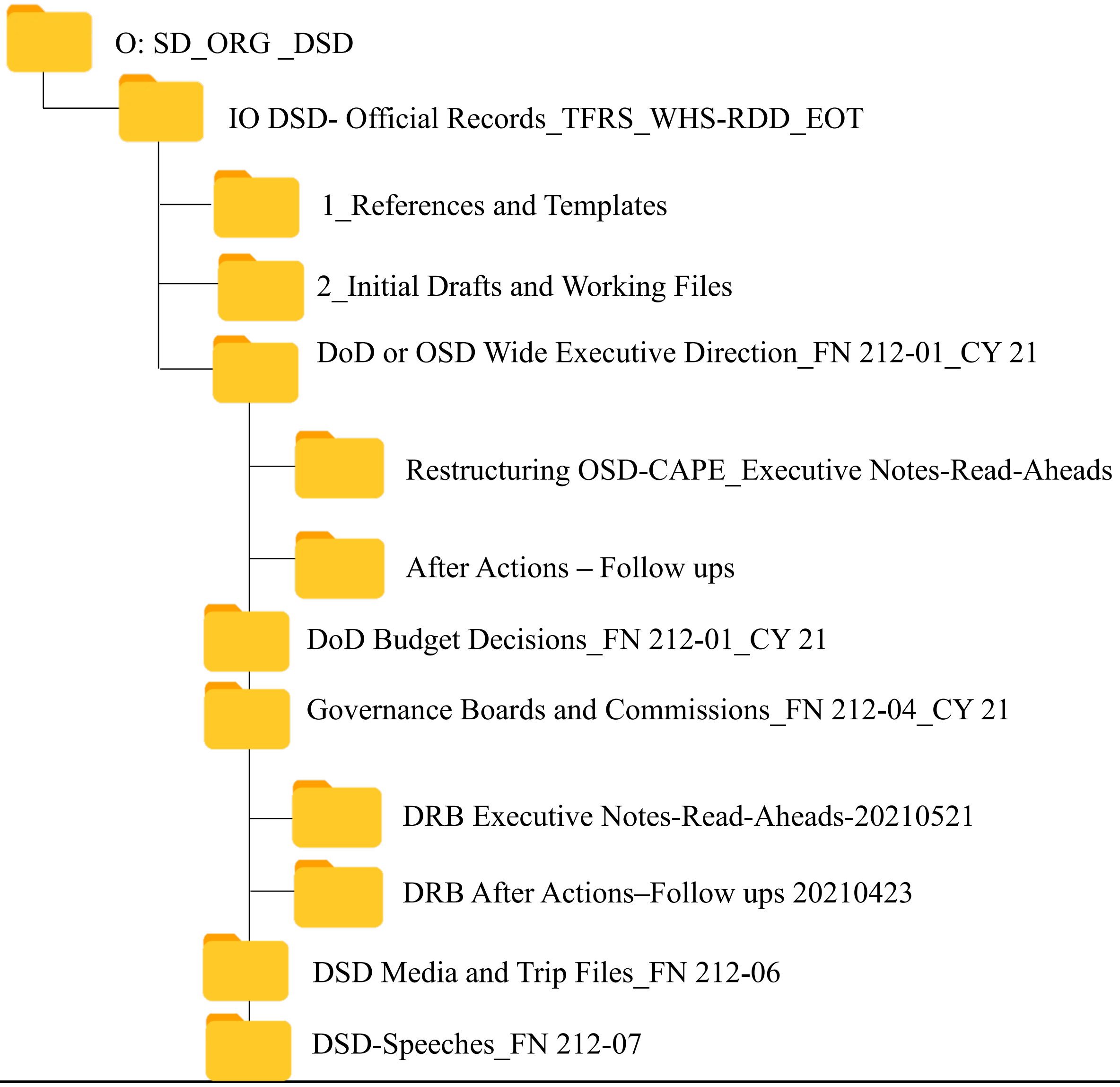
| | |
|---|---|
| **Keep it Simple** | The capture and management of electronic records into a file system, usually organized in a series of folders, requires careful planning and structure. Design a file structure hierarchy to ensure that it doesn't become too hard to find information in the hierarchy or ineffective because there are too many records in each folder. A filing structure may be modeled on the functions of an organization and may also use subject themes for parts of the structure. |
| **Folder Naming Conventions** | Folder naming conventions provide all information within the system with a coherent context and logical frame of reference. |
| | Name electronic folders for "find-ability." A record that can't be found and easily identified is a useless file. Folder names should contain information that leads to easy retrieval and identification. But don't overdo it - avoid extra-long folder names. File name elements should be |
| | Assume that you'll forget what's in the folder immediately after you create the file name when you name it. Try to use a name that will be descriptive to other people as well as yourself. |
| **Use Title Case** | Use capital letters for the principal words for filenames. |

## APPENDIX C:  NETWORK SHARED DRIVES FILE STRUCTURES

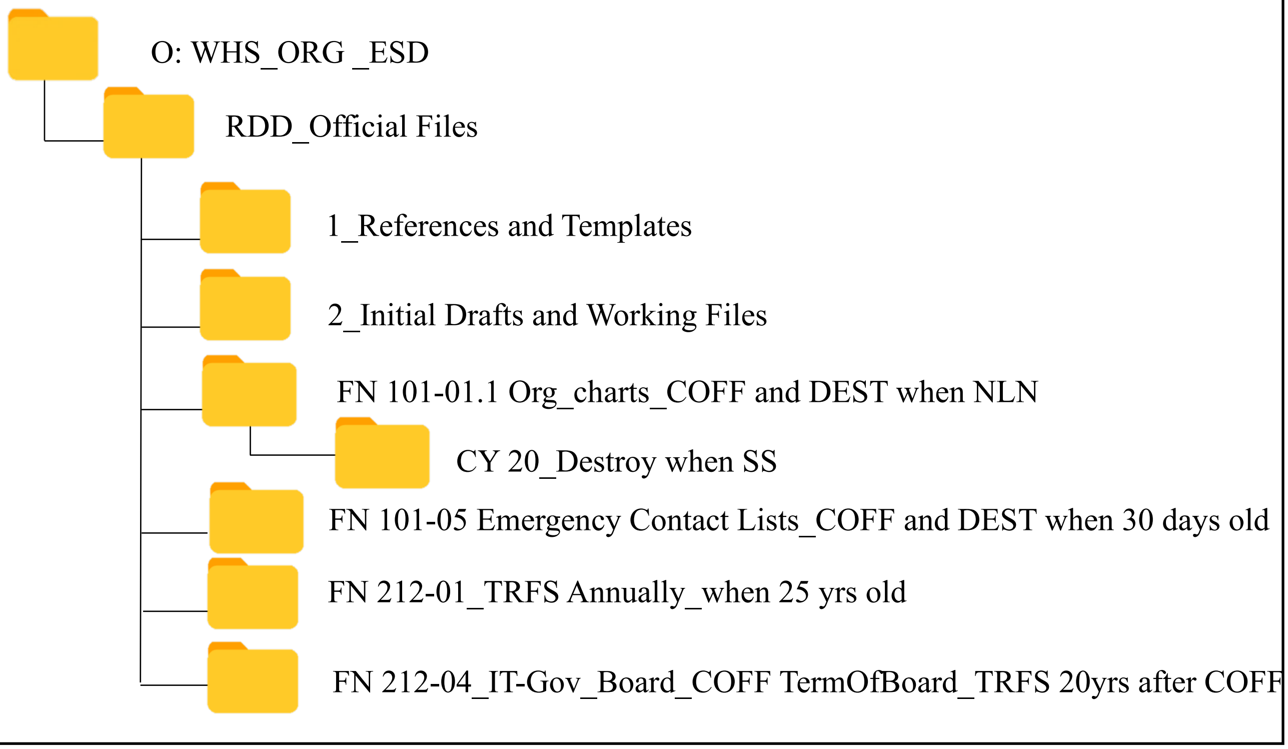
### HIERARCHICAL FILE STRUCTURE


O: SD_ORG _DSD
IO DSD- Official Records
1_References and Templates
2_Initial Drafts and Working Files
FN_102-18.2_Congression RFI_ PERM_ TFRS_WHS-RDD_EOT
CY 21
Draft FY22_ NDAA
FN_206-09.1_ ExeSec_Budget_COFF final pmt DEST 10yrs after COFF
FN_212-04_ Governance Boards_PERM_ TFRS_WHS-RDD_TermOfBoard
CY 21
DRB Executive Notes-Read-Aheads-20210521
DRB After Actions–Follow ups 20210423
FN 212-06_DSD Media and Trip Files_ PERM_ TFRS_WHS-RDD_EOT
FN 212-07_DSD-Speeches_ PERM_ TFRS_WHS-RDD_EOT

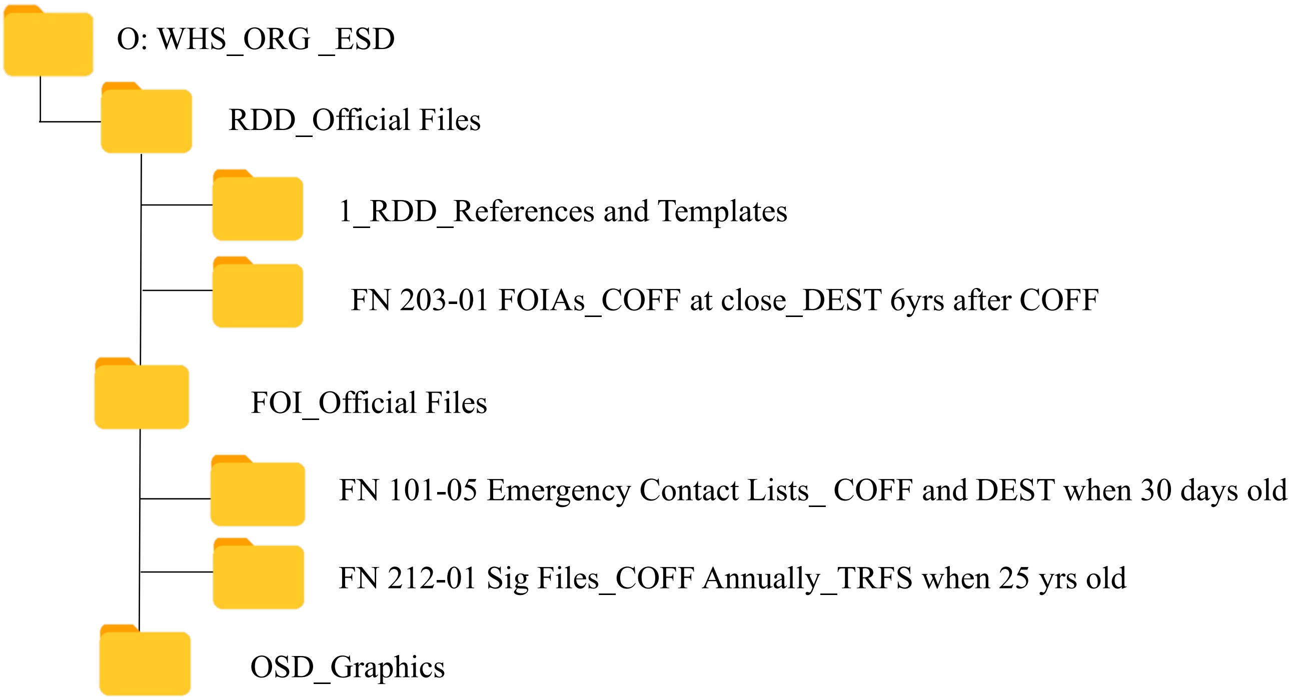
SUBJECT MATTER FILE STRUCTURE


O: SD_ORG _DSD
IO DSD- Official Records_TFRS_WHS-RDD_EOT
1_References and Templates
2_Initial Drafts and Working Files
DoD or OSD Wide Executive Direction_FN 212-01_CY 21
Restructuring OSD-CAPE_Executive Notes-Read-Aheads
After Actions – Follow ups
DoD Budget Decisions_FN 212-01_CY 21
Governance Boards and Commissions_FN 212-04_CY 21
DRB Executive Notes-Read-Aheads-20210521
DRB After Actions–Follow ups 20210423
DSD Media and Trip Files_FN 212-06
DSD-Speeches_FN 212-07

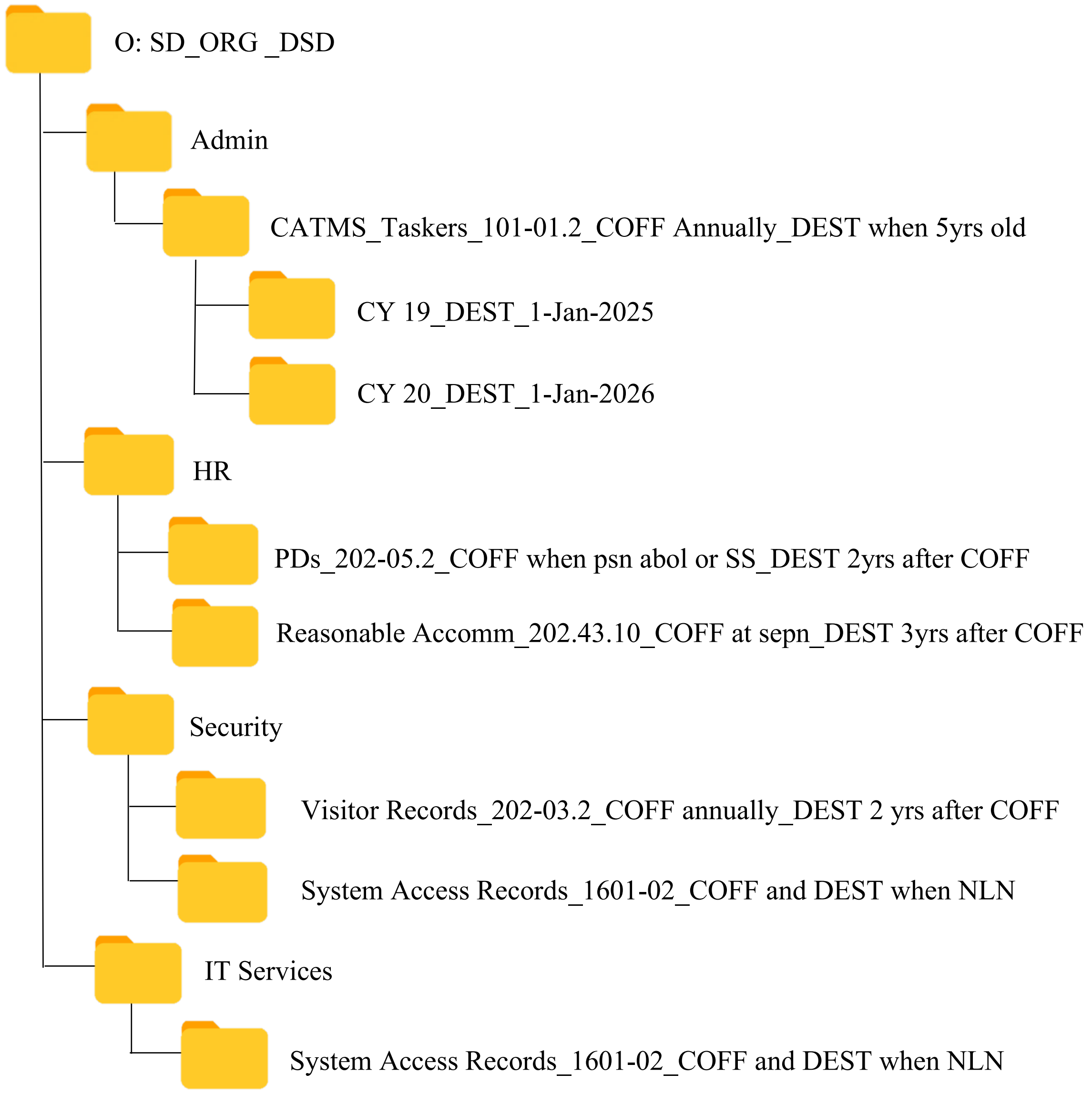
SEMI-FLAT - FILE STRUCTURE


O: WHS_ORG _ESD
RDD_Official Files
1_References and Templates
2_Initial Drafts and Working Files
FN 101-01.1 Org_charts_COFF and DEST when NLN
CY 20_Destroy when SS
FN 101-05 Emergency Contact Lists_COFF and DEST when 30 days old
FN 212-01_TRFS Annually_when 25 yrs old
FN 212-04_IT-Gov_Board_COFF TermOfBoard_TRFS 20yrs after COFF

MULTI- OFFICE FILE STRUCTURE


O: WHS_ORG _ESD
RDD_Official Files
1_RDD_References and Templates
FN 203-01 FOIAs_COFF at close_DEST 6yrs after COFF
FOI_Official Files
FN 101-05 Emergency Contact Lists_ COFF and DEST when 30 days old
FN 212-01 Sig Files_COFF Annually_TRFS when 25 yrs old
OSD_Graphics

FUNCTIONAL – FILE STRUCTURE


O: SD_ORG _DSD
Admin
CATMS_Taskers_101-01.2_COFF Annually_DEST when 5yrs old
CY 19_DEST_1-Jan-2025
CY 20_DEST_1-Jan-2026
HR
PDs_202-05.2_COFF when psn abol or SS_DEST 2yrs after COFF
Reasonable Accomm_202.43.10_COFF at sepn_DEST 3yrs after COFF
Security
Visitor Records_202-03.2_COFF annually_DEST 2 yrs after COFF
System Access Records_1601-02_COFF and DEST when NLN
IT Services
System Access Records_1601-02_COFF and DEST when NLN

## APPENDIX D. RECORDS CONVERSION TABLE

# CONVERSION TABLE: VARIOUS RECORDS FORMATS TO CUBIC FEET EQUIVALENTS

| TYPE | SIZE | VOLUME | | CUBIC FEET |
|---|---|---|---|---|
| Sheets of Paper | Letter-size | 3000 | = | 1.00 |
| Records Storage Box | Standard | 10”x 12”x 15” | = | 1.00 |
| Records Storage Box | Large/Letter-size | 10”x 12”x 36” | = | 2.00 |
| Records Storage Box | Large/Legal-size | 10”x 15”x 36” | = | 2.50 |
| Standard File Cabinet | Letter 8 ½”x11” | 1 full drawer | = | 1.50 |
| | Legal 8 ½”x14” | 1 full drawer | = | 2.00 |
| Lateral File Cabinet | Letter 8 ½”x11” | 1 full drawer | = | 3.25 |
| | Legal 8 ½”x14” | 1 full drawer | = | 4.00 |
| Shelf Files (15”x36”) | Letter 8 ½”x11” | 1 full shelf | = | 3.0 |
| | Legal 8 ½”x14” | 1 full shelf | = | 3.40 |
| Open Shelving | Letter 8 ½”x11” | 36” long | = | 2.4 |
| | Legal 8 ½”x14” | 36” long | = | 3.0 |
| Microfilm | 16mm x 100’ | 90 reels | = | 1.00 |
| | 35mm x 100’ | 44 reels | = | 1.00 |
| Index Cards | 3”x 5” | 12,000 cards | = | 1.00 |
| | 4”x 6” | 6,000 cards | = | 1.00 |
| | 5”x 8” | 4,800 cards | = | 1.00 |
| Computer Print-outs | 21”x 15” | 10 inch stack | = | 1.00 |

General Formula

To convert measurements into Cubic Feet, use the following formula:

1. Measure (in inches) and then multiply the item’s Length x Width x Height
2. Divide the total by 1728 = CUBIC FEET per item.

**One cubic foot of records weighs about 30 lbs. dry & >50 lbs. if wet.
One ton of records equals 70 cubic feet.

## APPENDIX E. SAMPLE SCANNING PROJECT PLAN

| | | | | | |
|---|---|---|---|---|---|
| | **Part I – Organization Background** | | | | |
| | | | | | |
| | | | | | |
| | **Instructions – Spell out all acronyms and abbreviations** | | | | |
| **Name of OSD Component** | Identify Parent Component | | | | |
| | | | | | |
| | | | | | |
| **Office of Primary Responsibility (OPR)** | **Identify the OSD Component office delegated primary responsibility for oversight, creation, and retention the records – Limit 1 template per OPR** | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| **Description of Records to be Scanned** | **OSD Records Disposition Schedule (OSD RDS) File Number:** | **File Title:** | **Cut Off:** | **Retention:** | **SORN (if applicable):** |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| **Date Span and Volume for Each File Number:** | **OSD RDS File Number:** | **Start Date of Records:** | **End date of Records:** | **Volume: (See Appendix C for conversion table):** | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| **DoD Issuance** | **Insert DoD Issuance(s) that define missions; authority; and assign responsibilities for records** | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| **Physical Location of Records** | **□ Pentagon** | **□ Mark Center** | **□ Fort Belvoir** | **□ Fort Meade** | |
| | **Room #** | **Room #** | **Room #** | **Room #** | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **Other: Identify City, State, Facility Address and Room #** | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| **Classification** | **Is Classified Information Present? Identify Appropriate level** | | | | | |
| | □Unclassified | □Confidential | □Secret | □Top Secret | | |
| | **Does Classified Information Contain Special Markings/Caveats?** | | | | | |
| | □ SCI | □ NATO | □ SAP | | | |
| | □ RD/FRD | □ ACCM | | | | |
| | □ Other, identify below | | | | | |
| | | | | | | |
| | **Controlled Unclassified Information (CUI)** | | | | | |
| | □Critical Infrastructure | □Defense | □Export Control | □ Financial | □Immigration | □ Intelligence |
| | □ International Agreements | □ Law Enforcement | □ Legal | □ North Atlantic Treaty Organization (NATO) | □ Natural and Cultural Resources | |
| | □Nuclear | □ Patent | □ Procurement and Acquisition | □ Privacy | □Proprietary Business Information | |
| | □ Provisional | □ Statistical | □ Tax | □ Transportation | | |
| | | | | | | |
| | | | | | | |
| **OPR Point(s) of Contact** | **Name** | **Office** | **Email Address** | **Phone #** | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | **Part II - Host Environment** | | | | | |
| | | | | | | |
| **Location of Digitized Records** | **Network Share Drive Location:**<br>□ NIPR,<br>□ SIPR,<br>□ JWICS | **If retained on share drives, does file location confirm with** Administrative Instruction 15 **and OSD PRIMER?** | | | | |
| | | □ Yes | Provide URL | | | |
| | | □ No | Provide Justification | | | |

| | | | | |
|---|---|---|---|---|
| | | □ Not Applicable | | |
| | | | | |
| | Identify Cloud Host Environment | | | |
| | **□ Cloud** | **□ Commerical** | **□ Hybrid** | **□ DISA/JSP Cloud Environment** |
| | **If Commercial or Hybrid; Identify Provider, Name of Database or Application** | | | |
| | | | | |
| | | | | |
| | **Does Commercial or Hybrid Cloud provider have documented mitigation and migration strategy?** | | | |
| | **□ Yes, Attach copy of mitigation and migration strategy.** | | | |
| | **□ No, Provide Justification on separate document.** | | | |
| | | | | |
| | **Does the Privacy Act apply?** | | | |
| | **□ Yes, Attach copy of Privacy Impact Assessment (PIA) and SORN** | | | |
| | | | | |
| | | | | |
| | **□ Approved Federal Information System (FIS), Database or Application** | | | |
| | **If retained in FIS, Database or Application** | | | |
| | □ System Name: | | | |
| | | | | |
| | □ Insert ATO System ID and Termination Date | | | |
| | | | | |
| | **Does Federal Information System (FIS), Database or Application have documented mitigation and migration strategy?** | | | |
| | □ Yes, Attach copy of mitigation and migration strategy. | | | |
| | □ No, Provide Justification on separate document. | | | |
| | **Does the Privacy Act apply?** | | | |
| | **□ Yes, Attach copy of  PIA and SORN** | | | |
| | | | | |
| | **Part III - Digitization Requirements** | | | |
| | | | | |
| **Scanning Equipment Parameters** | **Components will ensure scanning equipment can meet these minimum parameters:** | | | |
| | □ Paper Parameters | | □ Print Photographs Parameters | |
| | **Digital File Specifications** | **Attributes** | **Digital File Specifications** | **Attributes** |

| | | | | | | |
|---|---|---|---|---|---|---|
| | □ | Bit depth | 8- Or 16-Bit | □ | Bit depth | 24-bit |
| | □ | Color space | Grey Gamma 2.2, Adobe RGB 1998 | □ | Color space | AdobeRGB1998 |
| | □ | Spatial resolution | 300 dpi minimum | □ | Spatial resolution | 400 dpi minimum |
| | | | | | | |
| **Format of Scanned Images** | **Identify Authorized Format Records SHALL be captured in :** | | | | | |
| | □ | Portable Network Graphics 1.2 (PNG), | □ | Tagged Image File Format Revision 6.0 (TIFF) | | |
| | □ | JPEG 2000 Part 2 (Annex M - JPX Baseline) (JP2) | □ | Portable Document Format/Archival (PDF/A-1, PDF/A-2) | | |
| | | | | | | |
| **Metadata** | **Documents will be encoded to capture the following metadata: Before identifying metadata OPR and Contractor must coordinate review with Component security officers to avoid creating a mosaic effect[2]** | | | | | |
| | 1. Date created (Date of record(s) not date scanned. See Note) | | | | | |
| | 2. Official file title of the image(s) (Shall correspond with Box list) | | | | | |
| | 3. Office of Primary Responsibility/Owner | | | | | |
| | 4. Description. A narrative description of the content of the record, including abstracts for document-like objects or content descriptions for audio or video records.<br>□ Note: If date of record is not available. Files will be named as follows "File Title – Date of Record is Scanned (YYYYMMDD)-OPR<br>□ Ex: BDU Study UD Green vs Desert Tan Camo-20100505-ASD(M&RA) | | | | | |
| | 5. File number assigned per OSD RDS, OPR file plan or as identified by OPR representative | | | | | |
| | 6. Unique identifier to connect related record(s) that is either physically or logically required in order to form a complete record. (If appliable) | | | | | |
| | | | | | | |
| **Document Preparation** | **The OPR or Contractor will complete the following actions to prepare records for scanning:** | | | | | |
| | Step 1. Retrieve Records from Storage or Offsite Locations<br>Note: Retrieval of records from Federal Records Centers requires coordination with OSD RIM Program | | | | | |
| | Step 2. Review Boxes List or Create Folder Level Inventory List. Box Lists should contain the miminum fields: | | | | | |

[2] A mosaic effect is the gathering of disparate, seemingly innocuous pieces of information, when combined with other types of information can become significant construct or insight into DoD operations.

| | | | | |
|---|---|---|---|---|
| | □ Unabbreviated name of Office of Primary Responsibility | □ OPR Physical location and Address | □ File(s) Title | □ File Number(s) per the OSD Records Disposition Schedule |
| | □ Volume | □ Classification | □ Date Span | |
| | Step 3. Remove documents from binders, place in folders, and label folder verbatim of binders.<br>Note: Each record (case file folder or binder) will constitute one PDF file, unless greater than 500 pages in which instance the case will be broken up into multiple parts and labeled “Part 1”, “Part 2”, etc. | | | |
| | Step 4. Insert dividers or separator pages in between documents or batches of documents to indicate where each scanned file should start and stop. | | | |
| | Step 5. Ensure all documents are available or accounted for and are in the proper sequence. | | | |
| | Step 6. Denote pages with missing parts, stains, tears, or obliterations that affect the text of any irregularities that may affect legibility of the records. (review for eligility to photocopy) | | | |
| | Step 7. Remove from documents all staples, paperclips, binder clips, and anything that would interfere in the scanning process. | | | |
| | Step 8. Removing “sticky notes” when they are making text illegible or covering exist text, images, or contents of the page. Sticky notes should be affixed to another sheet and scan in immediately following the page. Sticky notes and other written text will be transcribed and attached behind affixed original record. | | | |
| | Step 9. Repair documents in a manner does not obscure text or affect legibility of the records. | | | |
| | Step 10. Separating all perforated pages (ex. computer printouts). If applicable | | | |
| | Step 11. Unfold legal documents. | | | |
| | Step 12. If tabs are found (specifically those tabs that present a hindrance to the scanning process), cut off the tabs and write the information found on the tab on the blank page to be scanned in the proper order. | | | |
| | Step 13. Identify Primary and Discretionary Access Restrictions | | | |
| | Step 14. See Part IV for Scanning Records for Network Share Drive File Structure and Document Naming Conventions | | | |
| | | | | |
| **Photocopying** | **Photocoping of documents is authorized that meet one (1) or more of the following criteria:** | | | |
| | □ Are structurally weak (such as ‘onion skin’), faded or dark, or otherwise present a hindrance to the scanning process. | □ May be damaged by scanning, such as already damaged or delicate papers. | | |

| | | |
|---|---|---|
| | □ Have substantial contrast or density variations over the area of the original and photocopying may improve the quality of the image. | □ Contain paper or ink colors that do not produce legible scanned images. Including color, halftone, and continuous tone photographs and images may not reproduce well, particularly in black and white scanning. |
| | □ Documents are too large to be scanned as a single full-sized | □ Non-standard paper sizes |
| | □ Non-standard text orientation | □ Contain negative images |
| | □ Contain text, character size, style, and weight smaller than 8-point font | □ Produced from Dot matrix printer |
| | | |

| | | |
|---|---|---|
| **Primary Access Restrictions** | **Identify Access Restrictions** | |
| | **Are Records Subject to The Privacy Act (PA)?** | |
| | □ Yes, if yes Identify PA System of Records Notice (SORN) Number | □ No |
| | PA SORN # | |
| | | |
| | **Is Classified Information Present?** | |
| | If Control Unclassified Information, Identify category | |
| | | |

| | | | |
|---|---|---|---|
| □Critical Infrastructure | □Defense | □Export Control | □ Financial |

| | | | | | |
|---|---|---|---|---|---|
| □Immigration | □ Intelligence | International Agreements | □ Law Enforcement | □ Legal | Proprietary Business Information |

| | | | | |
|---|---|---|---|---|
| □ Natural and Cultural Resources | □ North Atlantic Treaty Organization (NATO) | □Nuclear | □ Patent | □ Privacy |
| □Procurement and Acquisition | □ Provisional | □ Statistical | □ Tax | □ Transportation |
| | | | | |

| | | |
|---|---|---|
| | **Mark Level of Classified Information Present?** | |
| | □ Confidential | □ Secret |
| | □ Top Secret | |
| | | |
| | **Does Classified Information Contain Special Markings/Caveats?** | |
| | □ SCI | □ NATO |
| | □ RD/FRD | □ ACCM |
| | □ Other, identify below | |
| | | |

| | | | | |
|---|---|---|---|---|
| | | | | |
| **Discretionary Access Control** | **Define access restrictions to records by Users Internal OPR and Users External to OPR.** | | | |
| | □ Role-based access control[3] | Organization-based access control[4] | | |
| | | | | |
| | **Part IV – Procedures for Scanning Records** | | | |
| **Network Share Drive File Structure** | **Implement Organizational File Structure** | | | |
| | □ Top Level folder will identify OPR (Ex. OUSD(P&R) DHRA | | | |
| | □ Sub folders will include the OSD/RDS File Number and Title (Ex. Congressional – Routine (102-18.1) and include what is written on the folder tab or binder cover. | | | |
| | | | | |
| | | | | |
| **Scanned Records Naming Conventions** | Naming convention for each document, case file, project file is as follows:<br>“File Title – date of record YYYYMMDD-OPR<br>ex: BDU Study UD Green vs Desert Tan Camo-20100505-ASD(M&RA)<br>Note: Naming convention is applicable regards of Location of Digitized Records | | | |
| | | | | |
| | **Part V- Scanning Quality Control Procedures** | | | |
| **Quality Control Plan (QCP)** | The OPR or Contractor must design and implement a quality control (QC) plan to inspect, identify and correct errors due to malfunctioning or improperly configured digitization equipment, improper software application settings, incorrect metadata capture, or human error.<br>The QCP will include the minimum following sections: | | | |
| | | | | |
| | □ QCP Inspection Equipment Testing | □ QCP Inspection of Scanned Images | □ OCP Inspection Minimum Image Attributes | □ QCP Inspection Scan Log Example |
| | □ Example of Sampling Group | □ Rejected Images | □ Certification/Validation of Scanned Images | |
| | | | | |
| **QCP Inspection** | □ The OPR or Contractor should test all equipment used for scanning project, whether it is a multi-function printer (MFPs) or standalone scanner. At a minimum test should include the | | | |

[3] **Defined as access to authorized users based on roles and privileges..**

[4] **OrBAC is context sensitive, so the policy could be expressed dynamically. Furthermore, OrBAC owns concepts of hierarchy (organization, role, activity, view, context) and separation constraints**

| | |
|---|---|
| **Equipment Testing** | following features to ensure the equipment meets the configuration and image requirements of 36 CFR 1236. |
| | □ Test OCR capability. Scan several pages of text samples with a single font on each page in a variety of sizes, and we report accuracy in terms of the smallest size for each font that the scanner could read without a mistake. |
| | □ Test document scanning capability. Whether the scanner has an automatic document feeder (ADF) or sheet feeder; how many pages the ADF can handle; whether the scanner can duplex; whether the driver or bundled software can save a scan directly to PDF format; and whether the package can scan, OCR, and save to searchable PDF format. Additionally, the OPR/Contractor may want to test bundled document management and indexing programs (if applicable). |
| | □ Test speed for document scanning. Test the time a series of scans, using multiple-page documents for scanners with automatic document feeders (ADFs) or single pages for scanners that lack ADFs. |
| | □ Validate the number of pages per minute (ppm) for scanning in simplex (one-sided mode) and duplex (two-sided mode) to an image file format (ex. PDF); in images per minute (ipm—with one image on each side of the page). I.e., How long does it take to scan 500 pages (or max capacity) and convert to desired format? 500 pages at 6 minutes = 83 pages per minute or 5000 pages per hour. |
| | □ Testing photo scanning. Test scan quality, available metadata fields and related software like photo-album programs, the presence or absence of batch scanning features. Does the photo have to go through a sheet feeder, and if so whether the scanner offers a straight-through path and comes with a protective plastic sleeve to minimize the chances of damage? Additionally, OPR/Contractor may want to text maximum optical resolution, which determines how large an image you can print at reasonably high quality. |
| | |
| **QCP Inspection of Scanned Images** | Quality control check performed on a random sample of the total number of images. OPR will determine what percentage of images in the sample set can have errors. If errors are unacceptable due to the critical nature of the documents, then a 100 percent inspection (inspection of every image) is required, and an adequate amount of time and personnel must be assigned to the task. |
| | Post scanning, a sampling should consider the total number of documents, images scanned per hour, day, week and/or month to determine sample size. |
| | Will quality control sampling be conducted daily, weekly, monthly?<br>The following chart provides an example of sampling group based on the following:<br>□ 583 images per hour<br>□ 3,498 images per day (6 hr. day)<br>□ 17,490 images weekly |
| | |
| **OCP Inspection** | Images will be processed at the proper resolution, optical character recognition (OCR) and correctly oriented during the scanning process and meets the image requirements of 36 CFR 1236. QCP will incorporate the following minimum image attributes. OPR may include addition attributes necessary to ensure quality of images. |

| | | | | |
|---|---|---|---|---|
| **Minimum Image Attributes** | □ File name<br>□ Are the file names correct?<br>□ Are there any missing? | □ Orientation<br>□ Are the images correctly oriented?<br>□ Centered? | □ Completeness of image/cropping?<br>□ Sizing of pages?<br>□ Order of pages? | □ Readability /nothing obscuring content |
| | □ Are folder structures named properly?<br>□ Root identifies OPR?<br>□ Subfolders identifies divisions, programs, or mission records?<br>□ Identify date span of the records? | | □ Resolution<br>□ Are pages legible?<br>□ Are photo content identifiable? | □ Metadata fields complete?<br>□ Is the file description correct?<br>□ Proper grammar? |
| | □ Number of pages<br>□ Do the digital subfolders match the number of physical units, i.e., boxes, folders, books, etc.?<br>□ Does each subfolder contain the right number of files? | | | |
| | As the records are scanned, the OPR or Contractor will document the Quality Control inspection of each batch. The below example scan log can be used to document images that have passed and failed QC correct the problems when the documents are rescanned. | | | |

**SECTION 14:**

## 14.0. REFERENCES

Administrative Instruction 27, “Control of North Atlantic Treaty Organization (NATO) Classified Documents,” March 10, 2011

Administrative Instruction 50, “Historical Research in the Files of the Office of the Secretary of Defense (OSD),” July 23, 2007

Chief Information Officer Memorandum, "Use of Non-Official Electronic Messaging Accounts and Records Managements," April 6, 2006

Committee on National Security Systems Instruction No. 1253, “Security Categorization and Control Selection for National Security Systems,” current edition

Department of Commerce National Institute of Standards and Technology Special Publication 800-37, "Guide for Applying the Risk Management Framework to Federal Information Systems,” current edition

Department of Commerce National Institute of Standards and Technology Special Publication 800-53, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," current edition

Department of Commerce National Institute of Standards and Technology Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories," current edition

Department of Commerce National Institute of Standards and Technology Special Publication 800-122, "Guide to Protecting Confidentiality of Personally Identifiable Information (PII)," current edition

Department of Commerce National Institute of Standards and Technology Special Publication 800-145, “The NIST Definition of Cloud Computing,” September 28, 2011

Deputy Secretary of Defense Memorandum, "Conducting Official Business on Electronic Messaging Accounts," January 16, 2018

DoD 5015.02-STD, “Electronic Records Management Software Applications Design Criteria Standard,” April 25, 2007

DoD 5230.30-M, “DoD Mandatory Declassification Review (MDR) Program,” December 22, 2011

DoD 8910.01-M, “Department of Defense Procedures for Management of Information Requirements,” June 30, 1998

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

DoD Directive 3020.26, “Department of Defense Continuity Programs,” January 9, 2009

DoD Directive 5015.02, “DoD Records Management Program,” March 6, 2000

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

DoD Directive 5230.09, “Clearance of DoD Information for Public Release,” August 22, 2008, as amended

DoD Directive 5400.11, “DoD Privacy Program,” May 8, 2007, as amended

DoD Instruction 5025.01, “DoD Directives Program,” September 26, 2012

DoD Instruction 5200.01, “DoD Information Security Program and Protection of Sensitive Compartmented Information (SCI),” April 21, 2016.

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

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities,"
September 11, 2008

DoD Instruction 8910.01, "Information Collection and Reporting," March 6, 2007, as amended

DoD Manual 5015.df, "OSD Records and Information Management Program," DRAFT (will be published and this reference updated before this PRIMER is published)

DoD Manual 5040.06, Volume 3, "Visual Information (VI): VI Records Schedule," September 25, 2008

DoD Manual 5200.01, "DoD Information Security Program," date varies by volume

DoD and NARA NATO Security Addendum to Memorandum for Agreement (MOA), May 22, 2023

Executive Order 12829, "National Industrial Security Program," January 6, 1993

Executive Order 12906, "Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure," April 13, 1994

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

General Records Schedule 6.2, "Federal Advisory Committee Records," September 2016

Joint Publication 1-02, "Department of Defense Dictionary of Military and Associated Terms," current edition

National Archives and Records Agency, "NARA Guidance on Managing Web Records," January 2005

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

Office of Management and Budget Circular A-130, "Management of Federal Information Resources," current edition

Office of Management and Budget Memorandum, "Update to Transition to Electronic Records," December 23, 2022

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

Office of the Secretary of Defense Records Disposition Schedule, April 18, 2008

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

Title 41, Code of Federal Regulations

Title 5, United States Code

Title 18, United States Code, Chapter 101 (also known as "Records and Reports")

Title 44, United States Code

U.S. Department of Homeland Security Federal Emergency Management Agency Federal Continuity Directive 1, "Federal Executive Branch National Continuity Program Requirements," January 17, 2017

U.S. Security Authority for NATO Instruction 1-07, "Implementation of NATO Requirements, April 5, 2007

Washington Headquarters Services Form 17, (WHS-17) "OSD Record and Information Management (RIM) Pre-Evaluation," current edition