SEPARATING PERSONNEL RECORDS ACCOUNTABILITY CHECKLIST – OSD CIVILIAN EMPLOYEES, DoD SERVICE MEMBERS, AND CONTRACTORS [i]

PRIVACY ACT STATEMENT

AUTHORITY: Title 10 U.S.C. § 113, Secretary of Defense; Title 36 Code of Federal Regulations (CFR) Part 1220, Federal Records, General; Title 44 U.S.C. Chapter 31, Records Management by Federal Agencies; Title 44 U.S.C. Chapter 33, Disposal of Records; DoDD 5105.53, Director of Administration and Management; DoDD 5110.04, Washington Headquarters Services (WHS).

PRINCIPAL PURPOSE(S): To ensure the accountability of federal records and information created and maintained by or on the behalf of Civilian Employees, Service Members and Contractors assigned to:

- The Immediate Offices of the Secretary of Defense, Deputy Secretary of Defense, and Executive Secretary
- Principal Staff Offices of the Secretary of Defense
- The Heads of the Defense Agencies and DoD Field Activities.

ROUTINE USE(S): In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as listed in the applicable system of records notice located at: **https://dpcld.defense.gov/Portals/49/Documents/Privacy/SORNs/OSDJS/DHRA-23-DoD.pdf**.

DISCLOSURE: Voluntary; however, there are various penalties for the unlawful removal or destruction of Federal records and the unauthorized disclosure of classified and controlled unclassified information.

SECTION I: RECORDS ACCOUNTABILITY

COMPLETED BY THE DEPARTING EMPLOYEE, SERVICE MEMBER, OR CONTRACTOR

SECTION I INSTRUCTIONS:

- The Employee/Service Member/Contractor will complete all sections applicable at least 10 business days prior to scheduled separation. This includes migrating or transitioning all records to appropriate personnel and completion of out-briefing by Component or Defense Agencies and Field Activities (DAFA) Records Management personnel [ii].
- For unscheduled separations, receive a records management exit briefing and complete Section I as soon as practicable.

a. Name of Official *(Last, First, Middle Initial)*:		**b. Estimated Departure Date** *(YYYYMMDD)*:
c. Insert Title/Position:	**d. Component**	**e. Office:**

f. Email Addresses

NIPR:	SIPR *(If Applicable)*:	JWICS *(If Applicable)*:	Other *(If Applicable)*:

g. The Employee/Service Member/Contractor has ensured federal records in their possession (regardless of format, location, device, or classification) have been located and transferred to the organization's approved filing locations or to appropriate personnel. This includes, but is not limited to, review of: • Safes, file cabinets, drawers, etc., to include home office • Paper, hard copy photos, binders, manuscripts • E-mail, text messages, chat messages or transcripts • Electronically created files, spreadsheets, databases • Official social media posts and audio and video files.	Yes ☐	No ☐
h. The Employee/Service Member/Contractor has reviewed and transferred, to the organization's approved filing locations or to appropriate personnel, all work-related content created or received on Government-Furnished Equipment (GFE) including, but not limited to, electronic messages created/received by communication tools or mobile device apps. GFE includes cellular phones, tablets, laptop computers or any other device used by the Employee/Service Member/Contractor in the conduct of official business.	Yes ☐	No ☐
i. The Employee/Service Member/Contractor has reviewed and transferred, to the organization's approved filing locations or to appropriate personnel, all work-related content created or received on authorized "Bring Your Own Devices" and personal devices or accounts including, but not limited to, non-governmental email, mobile devices, tablets, laptop computers or any other device or account used by the Employee/Service Member/Contractor in the conduct of official business.	Yes ☐	No ☐
j. The Employee/Service Member/Contractor has segregated and safeguarded all records and information subject to litigation hold/preservation notices, claims, audits, or other actions. Check "Not Applicable" if there are no known litigation holds/preservation notices relating to the Employee/Service Member/Contractor records.	Yes ☐	Not Applicable ☐
k. The Employee/Service Member/Contractor has notified the legal staff identified in the applicable litigation hold/ preservation notice of the new location of records and information in their possession, custody, or control that is responsive to/covered by a litigation hold/preservation notice. Check "Not Applicable" if there are no known litigation holds/preservation notices relating to the Employee's/Service Member's/Contractor's records.	Yes ☐	Not Applicable ☐

Certification:

By signing:

- I understand that all Federal records and information (regardless of format, location, or classification) that I created, received, maintained, or to which I have had access or may obtain access, will remain the property of, or under the control of, the United States Government, unless and until otherwise determined by an Authorized Official or final ruling of a court of law.
- I understand that I have no expectation of privacy with respect to telecommunications equipment, computers, computer networks, cellular phones, mobile devices, networking, or information processing systems authorized for my official use or issued to me to assist in carrying out my assigned responsibilities. This includes, without limitation, to records, files, documents, accounts, text and email messages, third-party communication applications and voice messages on those devices or systems.
- I agree that I shall return all records and non-record copies of records and information in my possession or come into my possession, including, and not limited to text messages, electronic messages, or other electronic communications, Federal records and information created on non-governmental email, "Bring Your Own Devices", personal devices or accounts, mobile devices, tablets, and laptop computers:
  - Upon demand by an authorized representative of the United States Government
  - Upon the conclusion of my employment or other relationship with the Department or Agency that last granted me access or that provided me access to such Federal records or information
  - Upon the conclusion of any other employment or relationship that required access to Federal records and information.
- If I do not return such materials upon demand, I understand that this may be a violation of Sections 793 and/or 18 U.S. Code § 1924.
- I certify under penalty of perjury, pursuant to 18 U.S. Code § 1621, to the truth and accuracy of all statements, answers, and representations made in the foregoing application, including all supplementary statements. The maximum penalty for the willful and unlawful destruction, damage, or alienation of Federal records is three years in prison (18 U.S. Code § 2071).

Signature of Employee/Service Member/Contractor:	Date Completed *(YYYYMMDD)*:
Name:	Office:

SECTION II: COMPONENT/DAFA RECORDS MANAGEMENT PERSONNEL AFFIRMATION

SECTION II INSTRUCTIONS:

- Identify the date of the records management exit briefing and the briefer.
- Exit briefings may be conducted by OSD Component/DAFA Records Manager(s) or delegated to the subordinate organizational records managers, custodians, or liaisons.

I acknowledge, by signing this form, I have briefed the above named Employee/Service Member/Contractor on their recordkeeping requirements for records in all media, including those records created or received on electronic mail systems, GFE, or authorized "Bring Your Own" or personal devices or accounts including, but not limited to, governmental and non-governmental email or other electronic messaging, text messages, audio, video and chat, cellular phones, tablets, laptop computers or any other device(s) or account(s) used by the Employee/Service Member/Contractor in the conduct of official business.

a. Records Management Exit Briefing

Date of Briefing *(YYYYMMDD)*:	Name of Briefer:
Office:	

b. Signature of Briefer

Signature:	Date *(YYYYMMDD)*:

SECTION III: REQUEST TO REMOVE PERSONAL FILES OR NON-RECORD COPIES OF OSD/DAFA RECORDS AND INFORMATION

SECTION III INSTRUCTIONS:

- If the Employee/Service Member/Contractor DOES NOT desire to remove personal files or non-record copies of OSD/DAFA records and information, return this form, with Section III unsigned, to the Component or DAFA RM.
- Requests to Remove Personal Files: The Employee/Service Member/Contractor will provide access to the Component or DAFA RM for verification that personal files do not contain government records or non-record copies of government records. Access may be provided by:
  - Hard copy,
  - Using a secure location such as OneDrive or SharePoint Online,
  - Sending the requested files to the Component RM, DAFA RM and OSD/RM via secure email
  - Authorized file transfer protocol (such as DoD SAFE, **https://safe.apps.mil/**).
- Requests to remove Non-Record Copies
  - DoD Contractors are not authorized to remove non-record copies of DoD records and information.
- Employee/Service Members requests for non-record copies are limited to the equivalent of 200 pages or 500 MB (non-record copies may include, but are not limited to, DoD emails, documents, images, outlook calendars, contact lists, audio, and video files).
  - For an Employee/Service Member request to remove non-record copies exceeding 200 pages/500MB, that portion of a request above the 200 page/500MB limit must be submitted to the OSD Freedom of Information Act (FOIA) Office (WHS/Freedom of Information Division (FOID)) for review (**https://www.esd.whs.mil/FOID/Submit-Request/**).

Step 1: Identify the category of materials requested:

- The Employee/Service Member will:
  - Identify and segregate all requested personal files and non-record copies of DoD emails, documents, images, audio, and video files into one of the following categories:
    - Personal Files. Materials belonging to the individual not used to conduct OSD business (either related solely to the individual's own affairs, professional development, or used exclusively for his/her convenience). Examples include personal calendars that reflect family, medical or social events not related to official duties, as well as SF-50s and training certificates, personal contact lists, thank you letters, invitations to non-official events, letters of congratulations, or letters forwarding resumes of individuals for general consideration.
    - Previously Released Materials. Unclassified information previously released to the public. Examples include Press releases, briefings, speeches, pictures, and announcements.
    - Non-Record Copies: Extra copies of documents preserved only for convenience or reference. Examples include memos, correspondence, taskers, briefings, emails, copies of Outlook calendars, reports, or studies pertaining to an event or topic of interest to the Employee/Service Member.
  - Note: The following non-records content are generally prohibited from release.
    - Classified National Security Information; to include "mosaic" or "compilation" classification.
    - Controlled Unclassified Information not authorized for public release.
    - Sensitive Personally Identifiable Information of third parties.
    - Information protected from release by the Freedom of Information Act, or other information
- The DoD Contractor will:
  - Identify and segregate all requested personal files from files related to contract performance; personal files may consist of:
    - Materials belonging to the individual not used to conduct OSD business (either related solely to the individual's own affairs, professional development, or used exclusively for his/her convenience).

Step 2: Submission Instructions:

- The Employee/Service Member/Contractor:
  - Completes Sections I and III of this form, then
  - Identifies or creates a secure location, then
  - Provides notification to:
    - Component or DAFA RM for review of Personal Files (only),
    - Employee/Service Member only: appropriate Offices of Primary Responsibility (OPRs) and Component/DAFA Security Manager for review of Previously Released and Non-Record Copies.
    - Approval/Denial Authority.

Certification:

By signing I consent to:

- Obtaining all approvals necessary regarding the clearance for release of personal or non-record copies government records and information.
- Complying with applicable laws, DoD policies, and regulations regarding the removal, defacing, alteration, or destruction of records and non-record copies.

Signature of Employee/Service Member/Contractor:	Date *(YYYYMMDD)*:

SECTION IV: REVIEW OF REQUEST TO REMOVE PERSONAL FILES OR NON-RECORD COPIES OF OSD RECORDS AND INFORMATION

Review Process:

- Component or DAFA RM will review a request to remove personal files to ensure government information including personally identifiable information (PII) not related to the requester or other sensitive information is not included.
- Component or DAFA RM may authorize personal files for release. Component or DAFA RM do not have release authority of non-record copies.
- Any non-record copies identified will be referred to the appropriate OPR.
  - The OPR will review requested materials for foreseeable harm to DoD in compliance with the DOJ-OIP Foreseeable Harm Standard or superseding guidance.
  - OPR will provide recommendations to the Approval/Denial Authority in accordance with Freedom of Information Act standards ensure the requested information does not contain the following:
    - Controlled Unclassified Information.
    - Sensitive Personally Identifiable Information of third parties.
    - Information protected from release by the Freedom of Information Act; or other information otherwise prohibited from release.
- Component or DAFA Security Manager will review requested materials to ensure both Classified National Security Information and Controlled Unclassified Information, including "mosaic" or "compilation" classification, is removed in accordance with DoDI 5230.09 and DoDM 5200.01, Volumes 1-3.
- After review by the OPR and Security Manager, the Component or DAFA RM refers the OPR's and Security Manager's recommendations to the Approval/Denial Authority. Approval/Denial Authority are the Component/DAFA Head or authorized signature authority.
- Approval/Denial Authority will review records and recommendations made by the OPR, Security Manager, and/or the Component/DAFA RM. A Component-specific list of positions authorized or delegated authority to coordinate are identified in DoDI 5025.01. Use this link for more information: **https://directives.whs.mil/issuance_process/Authorized_Component_Coordinators_CUI.pdf**. Access requires CAC / DoD PKI certificate.

Attestation:

By signing, I acknowledge, pursuant to 36 CFR 1230.12 the willful or unlawful release, removal, destruction, damage, or alienation of Federal records, documents, or information relating to the National Defense is subject to fines, penalties, or imprisonment per 18 U.S. Code § 793(f), 18 U.S.C. 641 and 18 U.S.C. 2071.

a. Review by Office of Primary Responsibility

Name of Reviewer:	Title:	Office:	Signature:

b. Recommendation by Office of Primary Responsibility:

☐ Grant in Full ☐ Grant in Part ☐ Deny in Full

c. Review by Component or DAFA Records Manager *(Personal Files and Private Correspondence only)*			
Name of Reviewer:	Title:	Office:	Signature:

d. Recommendation by Component or DAFA Records Manager:

☐ Approve ☐ Deny

e. Review by Component or DAFA Security Manager			
Name of Reviewer:	Title:	Office:	Signature:

f. Recommendation by Component or DAFA Security Manager:

☐ Grant in Full ☐ Grant in Part ☐ Deny in Full

SECTION V: APPROVAL/DENIAL AUTHORITY DECISION INSTRUCTIONS

- DoD Employee/Service Member/Contractor may not approve their own request.
- DoD Employee/Service Member will sign a Non-Disclosure Agreement for Non-Record copies Granted in Full or Part.
- The Non-Disclosure Agreement (NDA) is available here: **https://whs.sp.pentagon.mil/sites/ESD/RDD/RIM for Senior Officials/NDA for OSD Officials Requesting DoD Records_dtd_14 Jul 22.pdf?Web=1**. Access requires CAC / DoD PKI certificate.
- The Approval/Denial Authority should consult with their Component Attorney, General Counsel, or the DoD Office of General Counsel whether the release of the requested materials will affect DoD's ability to invoke legal privileges or other rights.
- Upon decision by the Approval/Denial Authority, this form and NDA will be provided to Component or DAFA Records Manager for coordination with IT Staff.

a. Review by Component Attorney or DAFA General Counsel: *(At Request of Approval/Denial Authority)*			
Name of Reviewer:	Title:	Office:	Signature:

b. Component Attorney or DAFA General Counsel Recommendation:

☐ Grant in Full ☐ Grant in Part ☐ Deny in Full

c. Approval/Denial Authority Decision:

☐ Grant in Full ☐ Grant in Part ☐ Deny in Full

d. Approval/Denial Authority Reason for Denial or Partial Release:

Records Exempt from Release under FOIA, 5 U.S.C 552

☐ B1 - Classified Information ☐ B2 - Internal Personnel Matters ☐ B3 - Information Protected by Other Statutes

☐ B4 - Business or Trade Information ☐ B5 - Privileged Information/Deliberative Process ☐ B6 - Personal Privacy

☐ B7 - Law Enforcement Records ☐ B8 - Financial Regulatory Records ☐ B9 - Geological and Geophysical Information

Records Exempt from Release due to Controlled Unclassified Information (CUI). The DoD CUI Registry is located at **https://www.dodcui.mil/Home/DoD-CUI-Registry/**

☐ Critical Infrastructure ☐ Export Control ☐ Financial

☐ Intelligence ☐ International Agreements ☐ Law Enforcement

☐ Natural and Cultural Resources ☐ North Atlantic Treaty Organization (NATO) ☐ Nuclear

☐ Patents ☐ Privacy ☐ Procurement and Acquisition

☐ Proprietary Business Information ☐ Provisional (OPSEC) ☐ Statistical

☐ Tax ☐ Transportation ☐ Other *(specify)*:

e. Approval/Denial Authority Signature		
Name:	Title:	Signature:

When personnel unexpectedly depart, records management personnel assigned to the Employee/Service Member/Contractor office will initiate the records accountability actions described in this form, immediately schedule a records management exit briefing, and complete JSP Form 6 Investigative Search Request Form to freeze the Employee/Service Member/Contractor accounts (NIPR, SIPR, JWICS or other user accounts).

SECTION I - RECORDS ACCOUNTABILITY COMPLETED BY THE EMPLOYEE/SERVICE MEMBER/CONTRACTOR

a. Name of departing Employee/Service Member/Contractor (Last, First, Middle Initial)
b. Estimated Departure Date
c. Title or Position of Employee/Service Member/Contractor
d. Name of OSD Component from which Employee/Service Member/Contractor is separating (do not use acronyms)
e. Name of Office/Division/Directorate from which the Employee/Service Member/Contractor is departing (do not use acronyms)
f. Insert email addresses
Complete g. through k. and sign acknowledgement in accordance with the stated instructions.

SECTION II - COMPONENT/DAFA RECORDS MANAGEMENT PERSONNEL AFFIRMATION

Complete the acknowledgement that the person signing has provided an exit briefing to the above-named Employee/Service Member/Contractor concerning the protection of Federal records and information in their possession (regardless of format, location, or classification), including the procedures to be followed in managing or transitioning records and information to appropriate personnel for retention.

SECTION III - REQUEST TO REMOVE PERSONAL FILES OR NON-RECORD COPIES OF OSD/DAFA RECORDS AND INFORMATION

Only complete this section if requesting to remove personal files or non-record copies of OSD/DAFA records and information. Complete the acknowledgement that the signing Employee/Service Member/Contractor has completed all stated instructions to request to remove such files.

SECTION IV - REVIEW OF REQUEST TO REMOVE PERSONAL FILES OR NON-RECORD COPIES OF OSD RECORDS AND INFORMATION

- When non-records copies are requested, reviews by OPR, Information Security /Operational Security Managers and Approval/Denial Authority are mandatory.
- Office of Primary Responsibility (OPR).
    - The DoD element that either prepares, or is responsible for, identifying records as responsive to a FOIA request. OPRs coordinate with the office of corollary responsibility (OCR) and FOIA managers to assist the initial denial authority in making decisions on FOIA requests.
    - After OPR and Security Reviews, OSD Components/DAFA RMs will refer all requests to the approval/denial authority.
- Security Manager.
    - Ensures personnel leaving DoD employment or service do not remove DoD records and information from DoD control, including non-record material meeting the threshold for mosaic" or "compilation" classification.
    - Ensures Classified National Security Information is not removed from government control per Executive Order 13526 or superseding order.
    - Ensures Controlled Unclassified Information is reviewed in accordance with DoDI 5230.09 and not released to the individual without approved decontrol per DoDI 5200.48.
- Recommendation by OPR and Security Manager:
    - OPR and Security Manager will review release for foreseeable harm to DoD and provide recommendation to Approval/Denial Authority in accordance with 5 U.S.C 552 (FOIA).
- Review by Component Attorney or DAFA General Counsel:
    - Review by Component Attorney or DAFA General Counsel is at the request of the Approval/Denial Authority.
    - Provides determination whether to permit departing employees to remove non-record copies, considers the extent to which such removal could affect the organization's ability to invoke any legal privileges, and considers the use of nondisclosure agreements in appropriate cases (per NARA Bulletin 2013-03).
    - Advise the Approval/Denial Authority of any potential legal risks that might arise from release.

SECTION V - APPROVAL/DENIAL AUTHORITY DECISION INSTRUCTIONS

- Review by Approval/Denial Authority:
    - Review records and recommendations made by OPR and Security Manager.
    - Refer to Component Attorney or DAFA General Counsel if:
        - Employee/Service Member/Contractor is identified in litigation hold or oversees functions subject to a litigation hold or pending litigation.
        - Release of requested records potentially conflicts with DoD policy, issuance, or Federal regulation.
- Approval/Denial Authority Decision:
    - Identify release decision (grant in full, grant in part, deny in full).
    - Provide reason / restrictions associated with denial in full or partial release.

[i] Office of the Secretary of Defense: As provided for in section 131 of title 10, United States Code, includes the Immediate Office of the Secretary and Deputy Secretary of Defense; the Under Secretaries of Defense; the GC, DoD; the Assistant Secretaries of Defense (ASDs); Assistants to the Secretary of Defense (ATSDs); the OSD Directors, and equivalents, who report directly to the Secretary or the Deputy Secretary of Defense, their staffs, and such other staff offices as the Secretary of Defense establishes within the Office of the Secretary of Defense to assist in carrying out assigned responsibilities.

[ii] Office of the Secretary of Defense: As provided for in section 131 of title 10, United States Code, includes the Immediate Office of the Secretary and Deputy Secretary of Defense; the Under Secretaries of Defense; the GC, DoD; the Assistant Secretaries of Defense (ASDs); Assistants to the Secretary of Defense (ATSDs); the OSD Directors, and equivalents, who report directly to the Secretary or the Deputy Secretary of Defense, their staffs, and such other staff offices as the Secretary of Defense establishes within the Office of the Secretary of Defense to assist in carrying out assigned responsibilities. Per DoDD 5105.76