CJCSM 5760.01B Vol. I
7 June 2024

JOINT STAFF AND COMBATANT COMMAND RECORDS AND INFORMATION MANAGEMENT MANUAL: VOLUME I – PROCEDURES

JOINT STAFF
WASHINGTON, D.C. 20318

(INTENTIONALLY BLANK)

CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

SJS/IMD
DISTRIBUTION: A, B, C, S

CJCSM 5760.01B Vol. I
7 June 2024

JOINT STAFF AND COMBATANT COMMAND RECORDS AND INFORMATION MANAGEMENT MANUAL: VOLUME I – PROCEDURES

References:
See Enclosure I

1. Purpose. This manual integrates Electronic Records (eRecords) management requirements and contains procedural guidance for media neutral (electronic or paper) records management for the Joint Staff (JS) and Combatant Commands (CCMDs).

2. Superseded/Cancellation

a. CJCSM 5760.01A, "Joint Staff and CCMDs Records Management Manual: Volume 1-Procedures," (2009), is hereby superseded.

b. CJCSI 5714.01D, "Policy for Release of Joint Information," 18 April 2012 is now canceled.

3. Applicability. This manual applies to the JS, Services, Combatant Commands (CCMDs), and Chairman Controlled Activities (CCAs).

4. Procedures. See Enclosures A through H.

5. Summary of Changes

a. Aligns procedures with regulations and directives stipulated by the National Archives and Records Administration (NARA), Department of Defense (DoD) Chief of Information Officer (CIO), National Institute of Standards and technology, and International Organization for Standardization, and by reference (a).

b. Removes processes and products which are no longer relevant to the records management program.

c. Removes the title assignment "Electronic System Functional Manager" as it is already a part of assigned duty requirements for designated records liaisons and custodians who collaborate with information technologist professionals when identifying and developing electronic record management requirements.

d. Adds annual reporting requirements to risk management; essential records and Continuity of Operations (COOP).

e. Adds digitization requirements for both permanent and temporary records.

f. Adds guidance on text messaging on mobile devices and incorporates reference (d).

6. Releasability. UNRESTRICTED. This directive is approved for public release; distribution is unlimited on the Non-classified Internet Protocol Router Network (NIPRNET). DoD Components (to include the Combatant Commands), other Federal agencies, and the public may obtain copies of this directive through the Internet from the CJCS Directives Electronic Library at: <http://www.jcs.mil/library>. JS activities may also obtain access via the SIPR Directives Electronic Library Websites.

7. Effective Date. This MANUAL is effective upon signature.

For the Chairman of the Joint Chiefs of Staff:

DOUGLAS A. SIMS, II, LTG, USA
Director, Joint Staff

Enclosures
A – Policy and Key Concepts: Records and Information Management
B – Records and Information Risk Management
C – Essential Records Program
D – Organizational Messaging Service, Capstone Approach, Electronic Discovery and Text Messaging
E – Management of Records and Information
F – Electronic Records Management (Control and Digitization)
G – Records Maintenance and Disposition
H – Records Retirement, Transfer and Recall
I – References

TABLE OF CONTENTS

Page

LIST OF FIGURES

LIST OF TABLES

(INTENTIONALLY BLANK)

ENCLOSURE A

POLICY AND KEY CONCEPTS: RECORDS AND INFORMATION MANAGEMENT

1. Policy. In accordance with (IAW) reference (a), it is policy that:

a. All records regardless of media or security classification are created, maintained, used, dispositioned, and preserved to capture legal and financial business practices, as well as decisions made and missions executed, as they will retain historical value to this organization.

b. All records will be managed IAW references (b), (c), and (d).

c. All records will be maintained IAW references (e) through (i).

d. All records, regardless of classification, will be properly retained or disposed of IAW assigned retention schedules listed in reference (k).

e. All records created, sent, or received using electronic messaging will be managed IAW references (d) and (l) through (q).

f. SharePoint sites will be used to establish standardized file structures and will align with record management needs.

g. Essential records will be identified, protected, and managed to support COOP equities IAW references (r) and (t) through (v).

2. Background

a. IAW reference (c), chapter 29, section 2901, records management is the systematic control of records. It is the planning, controlling, directing, organizing, training, promoting and other managerial activities involved with respect to records creation, maintenance and use, and records disposition to achieve adequate and proper documentation of policies and transaction of the Federal Government and effective and economical management of agency operations.

b. IAW reference (c), chapter 33, section 330, records include all recorded information (regardless of format) made or received by a federal agency under federal law or in connection with the transaction of public business. Records will be preserved as evidence of this organization functions, policies, decisions, procedures, operations, or other activities of the Government.

c. Corporate records. IAW reference (c), chapter 31, sections 3101 through 3107, corporate records are “records made, received, or signed by or for, the Top 4 leadership position within the Joint Staff” (see list below). Other records could include those that are made, received, or signed by or for the Secretary, Joint Staff (SJS).

(1) Chairman of the Joint Chiefs of Staff.

(2) Vice Chairman of the Joint Chiefs of Staff.

(3) Director, Joint Staff.

(4) Vice Director, Joint Staff.

NOTE: CCMDs will follow the same protocol when identifying and managing corporate records with signatures obtained from duty-assigned Combatant Commanders, Deputy Combatant Commanders, and the Chief of Staff/Director of Staff/Joint Secretary, or equivalent positions as defined in supporting internal directives.

3. National Archives and Records Administration

a. The National Archives and Records Administration (NARA) is an organization within the Executive Branch that is charged with the preservation and documentation of government and historical records.

b. NARA:

(1) Assists federal agencies in applying standards to records while in their custody.

(2) Gathers information on records management best practices and publicizes those methodologies by hosting training and webinars and ensuring the most current information is available on <https://www.archives.gov/records-mgmt/policy>.

(3) The Federal Electronic Records Modernization Initiative is NARA’s effort to provide a government-wide, modern, cost-effective, standardized, and interoperable set of record management solutions to ensure the incorporation of electronic records management programs.

c. Statutory and Regulatory Requirements to Managing Records

(1) IAW PRT 1230 of references (b), and (w), it is unlawful to:

(a) Deface, alter, erase, damage, or destroy any record material except as authorized by the Archivist of the United States.

(b) Remove any record material from files, including electronic files and any other type of record or records storage media, except as required for the conduct of official business and only with the proper authority, or when the material is determined to be a personal file and not an official file.

(c) Remove records from files when required for the conduct of official business without documenting the removal by identifying the record (number, title or subject, and date), the responsible organization, and the date of removal.

(2) Should an event as described in 3.c.(1)(a), (b), or (c) occur, Record Liaisons (RLs) will report the incident immediately to the Joint Staff Chief Records Officer (JSCRO) for JS incidents and Command Record Managers (CRMs) for CCMD incidents by:

(a) Generating a memorandum for record (MFR) correspondence with the following information:

1. Complete description of the records (include the creation dates of the records), the classification, and their designated retention schedule.

2. The amount impacted (using terms such as kilobytes, megabytes, terabytes for electronic records and cubic inches or feet for hard copies).

3. Complete address where the record was kept.

4. A brief explanation of what happened.

5. A statement that lays out a detailed plan of how the incident will be resolved (include an approximate timeline of how long it will take to execute the plan).

4. Special Handling of Records

a. References (x) through (ee) provide guidance on proper handling of classified information and state, "all classified information shall be afforded a level of protection against unauthorized disclosure that is equal to its level of classification."

(1) Records and non-record materials that contain controlled unclassified, classified, restricted, or formerly restricted information; that include other special markings; or that are designated Special Access Program materials will be handled and maintained IAW references (z) through (cc).

(2) Nuclear Weapon Command and Control/Nuclear Weapon Command and Control-Extremely Sensitive Information. Reference (bb) describes Nuclear Weapon Command and Control-Extremely Sensitive Information (NC2-ESI) as the information regarding the authorization employment and termination of nuclear weapon operations under the NC2 program. NC2-ESI is recorded information that supports all NC2 activities. Any unauthorized disclosure of NC2-ESI could threaten the Nation's security.

(a) Recorded materials are:

1. Written material, whether printed, typed, or handwritten.

2. Painted, drawn, or printed material, charts, and maps.

3. Electronic or magnetic recording media (see reference (bb) for a detailed list of magnetic records).

(b) NC2-ESI materials will be marked with the highest classification level. NC2-ESI markings of any single item will be managed accordingly until destroyed or sanitized by using approved procedures.

(c) Recorded media used to store or process NC2-ESI will retain TOP SECRET classifications and be controlled as NC2-ESI. At no time will this media be reused on any information system or platform information technology not cleared to process, store, or transmit TOP SECRET NC2-ESI data.

(d) Record Custodians (RCs) will conduct semi-annual inventories on all NC2-ESI materials with at least 90 days in between each inventory. IAW reference (z), inventories will be maintained for two years.

(e) To ensure control and minimize the possibility of compromise, NC2-ESI will be destroyed promptly when superseded by new editions or when no longer operationally required (not to exceed 30 days). Exceptions must be approved by the Joint Staff Deputy Director for Nuclear and Homeland Defense Operations or U.S. Strategic Command Deputy Director for Nuclear Operations, J3N. A record of the procedures used to declassify or destroy NC2-ESI materials or extracts will be maintained for a period of two years after disposition of the material. IAW reference (z), it is a requirement to have two cleared people present for all destruction of NC2-ESI.

(f) IAW reference (k), each organization will maintain records of destruction IAW applicable organization security instructions and General Records Schedule (GRS). For more information regarding disposition and GRS, contact the JSCRO and designated CCMD CRM for assistance.

(g) IAW references (z) through (dd), NC2-ESI temporary and permanent records will not be retired to Federal Records Centers or any other non-DoD records repository. Such records requiring long-term storage will be stored in an agency Inactive Storage Facility (ISF).

(3) North Atlantic Treaty Organization. References (bb), (dd), and (ee) provide guidance on the handling of North Atlantic Treaty Organization (NATO) information and defines it as “information that has been generated by or for NATO, or a member or information that has been released into the NATO security system and will be controlled and safeguarded.”

(a) NATO material may be stored in the same approved security container and approved Enterprise Information Systems (EIS) as non-NATO material; however, wherever the information is maintained, there must be a clear distinction between the two records. In addition, COSMIC, ATOMAL, and special category documents must be filed separately by category.

(b) CCMDs may request an exception to the requirement to separate NATO files. The request must be made to the Chief, Central U.S. Registry, through the Joint Staff Records Officer (JSRO).

(4) Electronic Information System. PRT 1236 to reference (b), and references (d), (h), and (i) explain the acquisition, development, and enhancement of EIS and information technology (IT) services must incorporate records management and preservation considerations. Any records contained in the systems or IT services must comply to NARA-approved records disposition schedules. All systems and services which create, maintain, use,

and store information must be protected from unauthorized disclosure while ensuring availability, usability, integrity, and authenticity of information.

5. Leveraging a Data-Centric Environment

a. Reference (j) envisions fully leveraging a "data-centric" environment where "records are curated; records management processes are automated; and governance accountability is clear." Across the JS and CCMD spectrum, all designated record managers will need to become involved in the development and implementation of eRecord management functions. **All** CCMD CRMs, JS RLs, and JS ROs will need to work together to:

(1) Develop a collaborative working relationship with knowledge management (KM) and artificial intelligence (AI) technicians to enhance business practices through automation, which will make decision making easier for senior leaders.

(2) Exercise appropriate levels of judgment and care when providing recommendations to the development, deployment, and use of AI capabilities.

(3) Take a proactive approach and participate in self-learning opportunities such as virtual events, online training sessions, seminars, and workshops.

6. Release of Information. This assigns responsibilities for the release of papers, books, maps, photographs, machine-readable materials, and any other materials or information, regardless of physical form or characteristics, originated by the Joint Staff and joint military activities (herein referred to individually and collectively as "joint information"). The table below was absorbed from reference (gg) and provides a list (independent of Enclosure I) of directives that govern various types of release of information.

Type of Joint Information	Directive(s) Governing Release
Information requested by Congress, its committees, staff, and investigators	– DoDI 5400.04, “Provision of Information to Congress”, March 17, 2009 – CJCSI 5501.01H series, “Congressional Liaison Policy”, October 26, 2022
Information requested by auditors and inspectors of the General Accountability Office or the Office of the DoD Inspector General	– 5a U.S.C Complied Act PL 95-452, “Inspector General Act of 1978”, October 12, 1978 – 31 USC, Subtitle I, Chapter 7, Sub-Chapter II, Section 716, “Availability of Information, and Inspection of Records”, April 3, 1980 – DoDI 7050.3 CHG1, “OIG of DoD Access to Records and Information”, April 24, 2020 – DoDI 7650.01, CHG2 “GAO and Comptroller General Request for Access to Records”, May 15, 2018 – JSI 5717.01 series, “Guidance for Support of GAO and DoD IG Activities”
Information requested under the Freedom of Information Act (FOIA)	– DoDD 5400.07, “DoD Freedom of Information (FOIA) Program” April 5, 2019 – JSI 5713.01E, “Freedom of Information Act (FOIA) Program”), June 15, 2022
Information subject to the Privacy Act	– 5 USC Section 552a, Privacy Act of 1974 – DoDD 5400.11, “DoD Privacy Program” – JSM 5240.01C, “Joint Staff Personnel Security Program”, January 2, 2018
Information released on publicly accessible Web sites	– DoDI 5200.48, “Controlled Unclassified Information (CUI), March 6, 2020
Other information requested by or proposed for release to the public, to include release through the news media	– DoDD 5122.05, “Assistant Secretary of Defense for Public Affairs” August 7, 2017 – DoDI 5230.09 CHG1, “Clearance of DoD Information for Public Release”, February 9, 2022 – JSI 5410.01B, “Clearance and Reporting of Speeches and Other Public Information” May 18, 2012
Information concerning planning, programming, budgeting, and execution (PPBE)	– DoDD 7045.14 CHG1, “Planning, Programming, Budgeting and Execution (PPBE) Process”, August 29, 2017 – CJCSI 8501.01B, “Chairman of the Joint Chiefs of Staff, Combatant Commanders, and Joint Staff Participation in the Planning, Programming, Budgeting, and Execution System”, December 15, 2021

Table 1. Release of Information and Directive Governance

7. Request Transfer of Information. Transfer of information will be conducted IAW PRT 1236 of reference (b), Chapter 29 of reference (c), and references (h), (i), (l), (m), (w), and (gg) through (jj). All transfer requests for copies of records

or access to information from JS and CCMDs will be processed IAW agency directives, DoD, and Federal regulations. The following steps provide a guideline for JS personnel who are departing and request copies or access to information. Steps to requesting JS copies or access to information:

a. Once the senior official departure date has been established, the JS RCs will assist senior leaders in identifying the information wanting to be transferred and will create and conduct an inventory of what is being copied.

b. RCs will advise requesters that any information located on NIPRNET desktops and placed in a cloud-based repositories are expected to remain accessible if remaining within the DoD.

c. RCs will relay the request to the RLs and provide a copy of the inventory to the RLs so it can be sent to the JS Release of Information Officer (JSRoIO).

d. JS RLs will contact the JSRoIO via e-mail at <js.pentagon.dom.list.sjs-imd-researchers>, SUBJECT: ATTN: Release of Information Officer and request assistance. The e-mail will have attached: a copy of the inventory with completed forms JS Form 32, "Records and Information Management Exit Checklist for Departing Joint Staff Members" (Figure 1) and JSP Form 11, "Data Write Authorization (DWA) and Transfer Request Form" (Figure 2). **Allow 24 hours to receive a response**.

e. The JSRoIO will review the complete package and will contact the requesting RL.

f. The JSRoIO will discuss the request with the JSCRO, who will approve or disapprove the transaction.

g. If the request for information is found to be valid and is approved by the JSCRO, the JSRoIO will provide the requesting RL with a Continuity of Operation memorandum and will provide further instruction on fulfilling the request.

h. **If** required, the RLs will assist the requester in submitting a "remedy ticket" to the Defense Information Systems Agency (DISA) help desk.

i. The JSRoIO will remain in contact with the requesting RL until the request is complete and all RM requirements are met.

NOTE: JS personnel should allow 2 weeks for processing **if** submitting a remedy ticket to the Joint Service Provider (JSP). Figure 1 shows the forms that will be used when submitting requests. CCMDs may use optional forms such as SD 822, “OSD Separating Personnel Records Accountability Checklist” (Figure 3) and SD 833, “Departing Employee Checklist Transfer of Records Between DoD/OSD Components” (Figure 4).

j. Submit request to the CCMD’s CRM for approval through their command ROs.

(1) The following is an approved list of materials that can be removed from all DoD agencies.

(a) Any unclassified information that is not an original.

(b) Books and papers that relate to new duty assignments.

(c) Copies of reference materials.

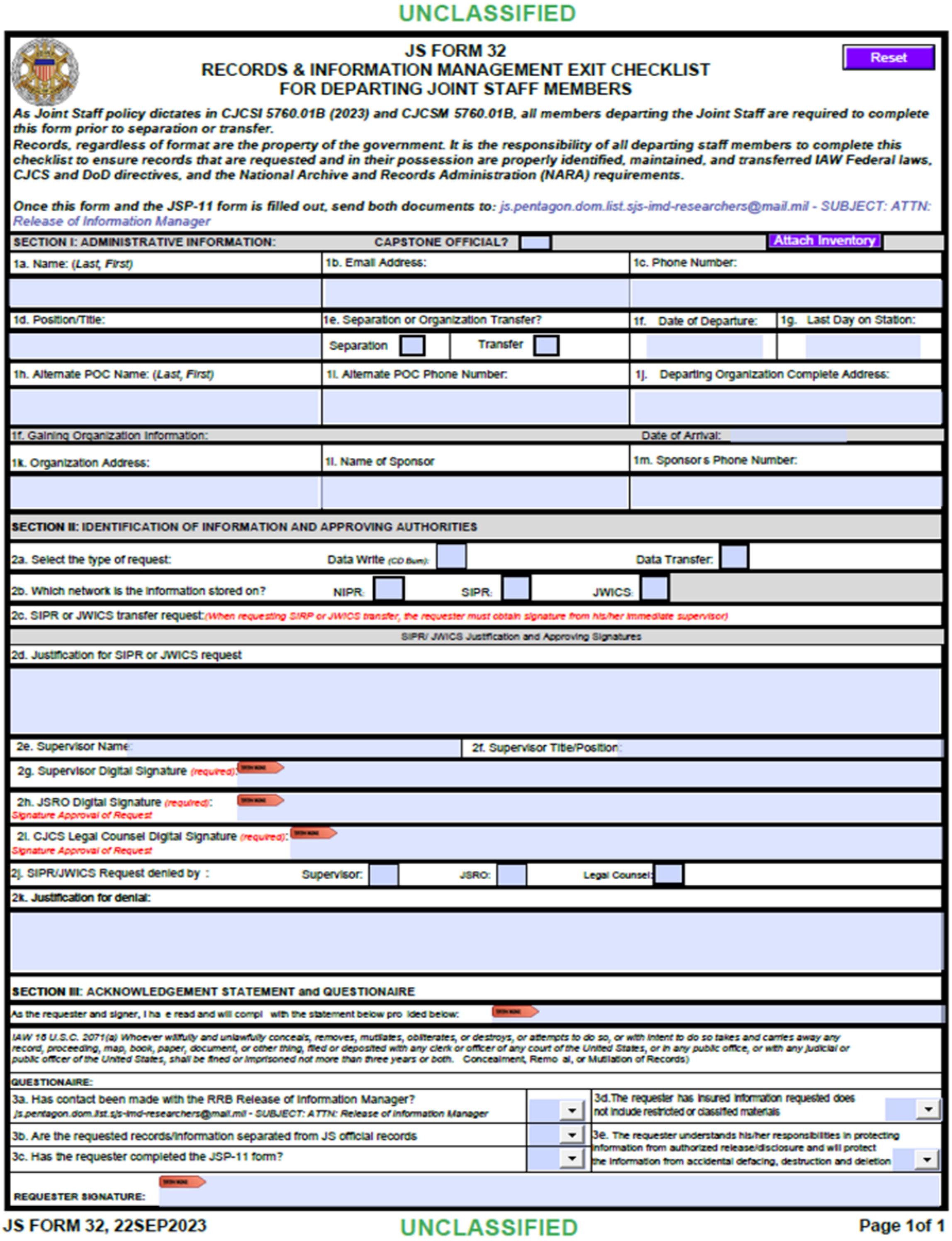
(d) Personnel Data.

(e) Training material.

(2) Senior officials who require and request release of information stored on classified networks must work with RLs, who will contact their appointed ROs prior to any coordination with IT providers.

(3) Senior officials transferring outside DoD channels are allowed to remove their own personal data. If there is a requirement to remove more, the departing official can do so by submitting a formal FOIA request.

(4) <u>Requesting Personal Storage Table files</u>. Personal storage table (PST) files are used to store Microsoft Outlook calendar events, contacts, and email messages. When senior officials request transfer of PST files, it is best to recommend a request for information that targets specific date ranges, topics, and/or events.



UNCLASSIFIED

JS FORM 32
RECORDS & INFORMATION MANAGEMENT EXIT CHECKLIST
FOR DEPARTING JOINT STAFF MEMBERS

Reset

As Joint Staff policy dictates in CJCSI 5760.01B (2023) and CJCSM 5760.01B, all members departing the Joint Staff are required to complete this form prior to separation or transfer.
Records, regardless of format are the property of the government. It is the responsibility of all departing staff members to complete this checklist to ensure records that are requested and in their possession are properly identified, maintained, and transferred IAW Federal laws, CJCS and DoD directives, and the National Archive and Records Administration (NARA) requirements.

Once this form and the JSP-11 form is filled out, send both documents to: *js.pentagon.dom.list.sjs-imd-researchers@mail.mil - SUBJECT: ATTN: Release of Information Manager*

SECTION I: ADMINISTRATIVE INFORMATION: **CAPSTONE OFFICIAL?** □ Attach Inventory

1a. Name: *(Last, First)*	1b. Email Address:	1c. Phone Number:	
1d. Position/Title:	1e. Separation or Organization Transfer?	1f. Date of Departure:	1g. Last Day on Station:
	Separation □ Transfer □		
1h. Alternate POC Name: *(Last, First)*	1i. Alternate POC Phone Number:	1j. Departing Organization Complete Address:	

1f. Gaining Organization Information: Date of Arrival:

1k. Organization Address:	1l. Name of Sponsor	1m. Sponsor s Phone Number:

SECTION II: IDENTIFICATION OF INFORMATION AND APPROVING AUTHORITIES

2a. Select the type of request: Data Write *(CD Burn)*: □ Data Transfer: □

2b. Which network is the information stored on? NIPR: □ SIPR: □ JWICS: □

2c. SIPR or JWICS transfer request:*(When requesting SIRP or JWICS transfer, the requester must obtain signature from his/her immediate supervisor)*

SIPR/ JWICS Justification and Approving Signatures

2d. Justification for SIPR or JWICS request

2e. Supervisor Name: 2f. Supervisor Title/Position:

2g. Supervisor Digital Signature *(required)*:

2h. JSRO Digital Signature *(required)*:
Signature Approval of Request

2i. CJCS Legal Counsel Digital Signature *(required)*:
Signature Approval of Request

2j. SIPR/JWICS Request denied by : Supervisor: □ JSRO: □ Legal Counsel: □

2k. Justification for denial:

SECTION III: ACKNOWLEDGEMENT STATEMENT and QUESTIONAIRE

As the requester and signer, I ha e read and will compl with the statement below pro ided below:

IAW 18 U.S.C. 2071(a) Whoever willfully and unlawfully conceals, removes, mutilates, obliterates, or destroys, or attempts to do so, or with intent to do so takes and carries away any record, proceeding, map, book, paper, document, or other thing, filed or deposited with any clerk or officer of any court of the United States, or in any public office, or with any judicial or public officer of the United States, shall be fined or imprisoned not more than three years or both. Concealment, Remo al, or Mutilation of Records)

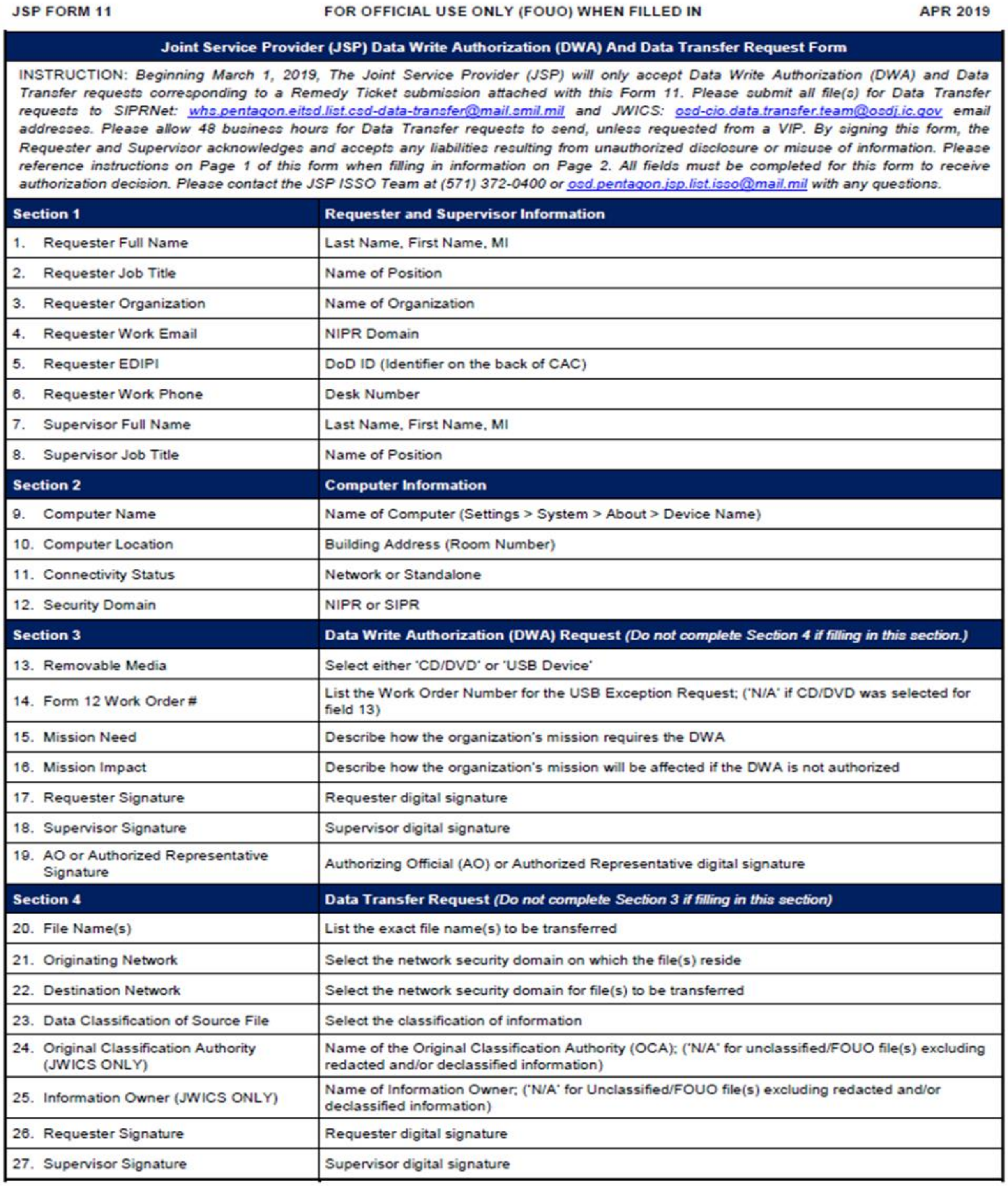
QUESTIONAIRE:

3a. Has contact been made with the RRB Release of Information Manager? *js.pentagon.dom.list.sjs-imd-researchers@mail.mil - SUBJECT: ATTN: Release of Information Manager*	▼	3d.The requester has insured information requested does not include restricted or classified materials	▼
3b. Are the requested records/information separated from JS official records	▼	3e. The requester understands his/her responsibilities in protecting information from authorized release/disclosure and will protect the information from accidental defacing, destruction and deletion	▼
3c. Has the requester completed the JSP-11 form?	▼		

REQUESTER SIGNATURE:

JS FORM 32, 22SEP2023 UNCLASSIFIED **Page 1of 1**

Figure 1. JS Form 32, “Records & Information Management Exit Checklist”



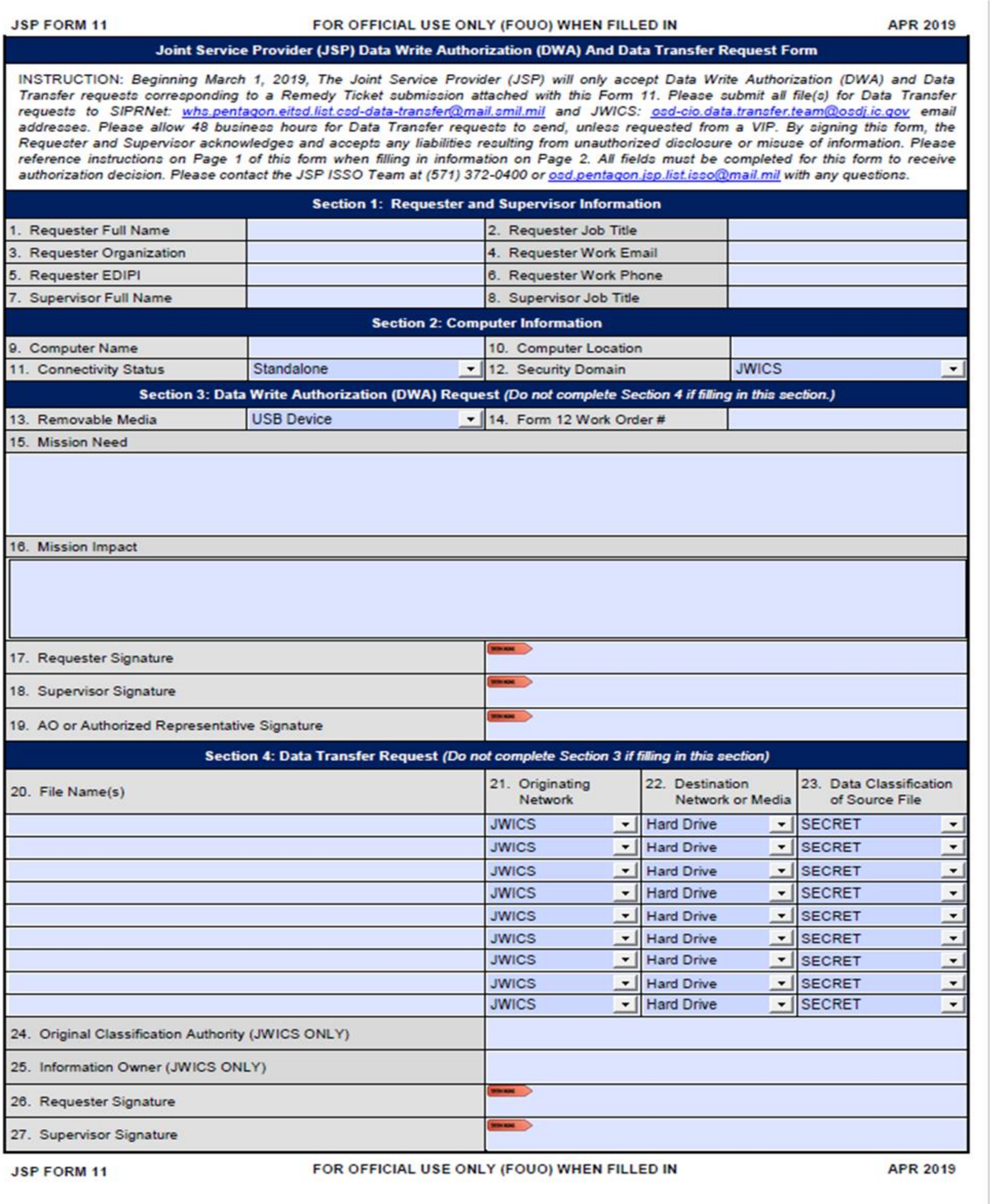
JSP FORM 11 FOR OFFICIAL USE ONLY (FOUO) WHEN FILLED IN APR 2019

Joint Service Provider (JSP) Data Write Authorization (DWA) And Data Transfer Request Form

INSTRUCTION: *Beginning March 1, 2019, The Joint Service Provider (JSP) will only accept Data Write Authorization (DWA) and Data Transfer requests corresponding to a Remedy Ticket submission attached with this Form 11. Please submit all file(s) for Data Transfer requests to SIPRNet: whs.pentagon.eitsd.list.csd-data-transfer@mail.smil.mil and JWICS: osd-cio.data.transfer.team@osdj.ic.gov email addresses. Please allow 48 business hours for Data Transfer requests to send, unless requested from a VIP. By signing this form, the Requester and Supervisor acknowledges and accepts any liabilities resulting from unauthorized disclosure or misuse of information. Please reference instructions on Page 1 of this form when filling in information on Page 2. All fields must be completed for this form to receive authorization decision. Please contact the JSP ISSO Team at (571) 372-0400 or osd.pentagon.jsp.list.isso@mail.mil with any questions.*

Section 1	**Requester and Supervisor Information**
1. Requester Full Name	Last Name, First Name, MI
2. Requester Job Title	Name of Position
3. Requester Organization	Name of Organization
4. Requester Work Email	NIPR Domain
5. Requester EDIPI	DoD ID (Identifier on the back of CAC)
6. Requester Work Phone	Desk Number
7. Supervisor Full Name	Last Name, First Name, MI
8. Supervisor Job Title	Name of Position
Section 2	**Computer Information**
9. Computer Name	Name of Computer (Settings > System > About > Device Name)
10. Computer Location	Building Address (Room Number)
11. Connectivity Status	Network or Standalone
12. Security Domain	NIPR or SIPR
Section 3	**Data Write Authorization (DWA) Request** ***(Do not complete Section 4 if filling in this section.)***
13. Removable Media	Select either 'CD/DVD' or 'USB Device'
14. Form 12 Work Order #	List the Work Order Number for the USB Exception Request; ('N/A' if CD/DVD was selected for field 13)
15. Mission Need	Describe how the organization's mission requires the DWA
16. Mission Impact	Describe how the organization's mission will be affected if the DWA is not authorized
17. Requester Signature	Requester digital signature
18. Supervisor Signature	Supervisor digital signature
19. AO or Authorized Representative Signature	Authorizing Official (AO) or Authorized Representative digital signature
Section 4	**Data Transfer Request** ***(Do not complete Section 3 if filling in this section)***
20. File Name(s)	List the exact file name(s) to be transferred
21. Originating Network	Select the network security domain on which the file(s) reside
22. Destination Network	Select the network security domain for file(s) to be transferred
23. Data Classification of Source File	Select the classification of information
24. Original Classification Authority (JWICS ONLY)	Name of the Original Classification Authority (OCA); ('N/A' for unclassified/FOUO file(s) excluding redacted and/or declassified information)
25. Information Owner (JWICS ONLY)	Name of Information Owner; ('N/A' for Unclassified/FOUO file(s) excluding redacted and/or declassified information)
26. Requester Signature	Requester digital signature
27. Supervisor Signature	Supervisor digital signature

Figure 2. JS Form 11, "JSP Data Write Authorization and Data Transfer Request Form"



JSP FORM 11 FOR OFFICIAL USE ONLY (FOUO) WHEN FILLED IN APR 2019

Joint Service Provider (JSP) Data Write Authorization (DWA) And Data Transfer Request Form

INSTRUCTION: *Beginning March 1, 2019, The Joint Service Provider (JSP) will only accept Data Write Authorization (DWA) and Data Transfer requests corresponding to a Remedy Ticket submission attached with this Form 11. Please submit all file(s) for Data Transfer requests to SIPRNet: whs.pentagon.eitsd.list.osd-data-transfer@mail.smil.mil and JWICS: osd-cio.data.transfer.team@osdj.ic.gov email addresses. Please allow 48 business hours for Data Transfer requests to send, unless requested from a VIP. By signing this form, the Requester and Supervisor acknowledges and accepts any liabilities resulting from unauthorized disclosure or misuse of information. Please reference instructions on Page 1 of this form when filling in information on Page 2. All fields must be completed for this form to receive authorization decision. Please contact the JSP ISSO Team at (571) 372-0400 or osd.pentagon.jsp.list.isso@mail.mil with any questions.*

Section 1: Requester and Supervisor Information

1. Requester Full Name		2. Requester Job Title	
3. Requester Organization		4. Requester Work Email	
5. Requester EDIPI		6. Requester Work Phone	
7. Supervisor Full Name		8. Supervisor Job Title	

Section 2: Computer Information

9. Computer Name		10. Computer Location	
11. Connectivity Status	Standalone	12. Security Domain	JWICS

Section 3: Data Write Authorization (DWA) Request *(Do not complete Section 4 if filling in this section.)*

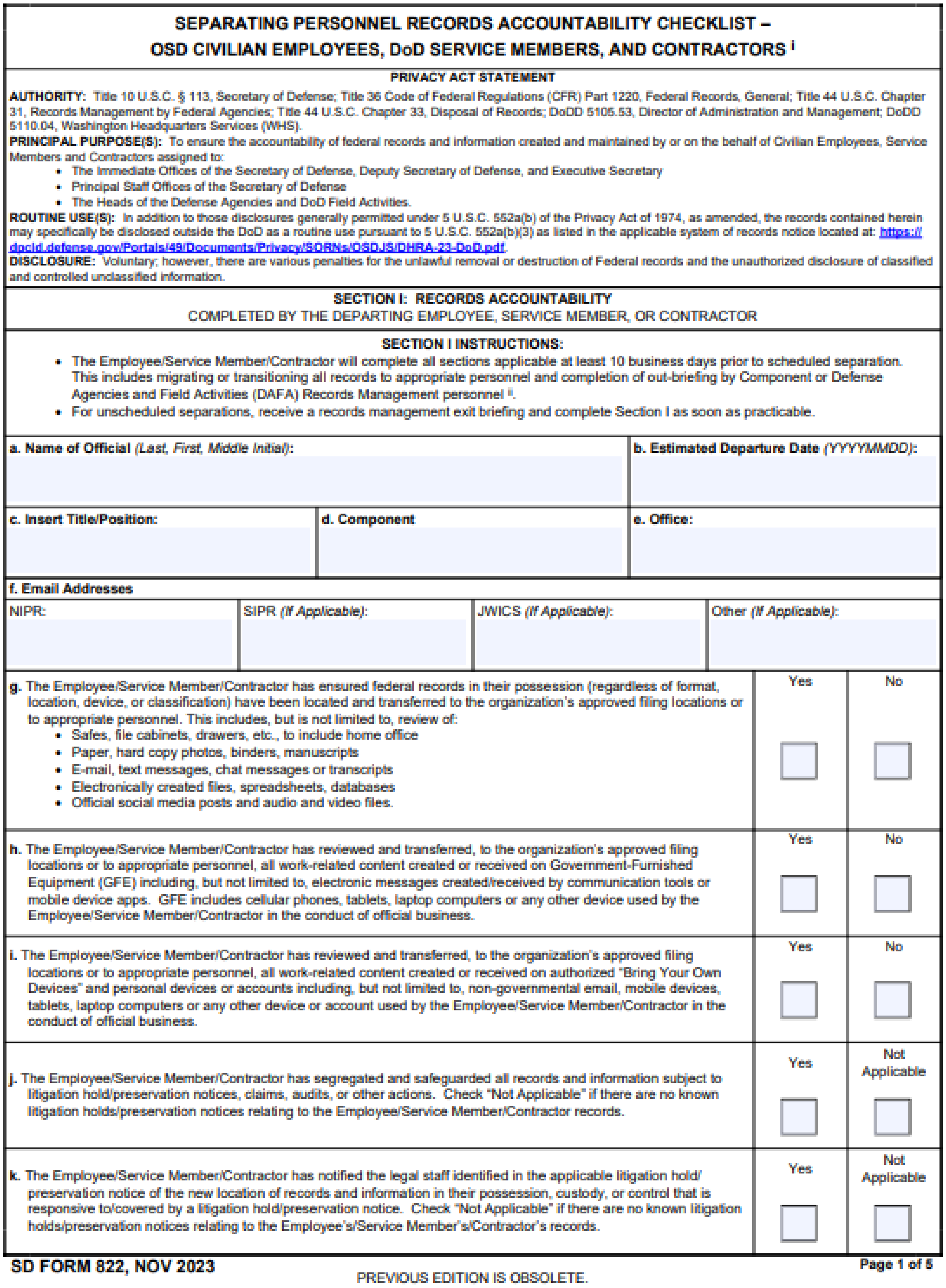
13. Removable Media	USB Device	14. Form 12 Work Order #	
15. Mission Need			
16. Mission Impact			
17. Requester Signature			
18. Supervisor Signature			
19. AO or Authorized Representative Signature			

Section 4: Data Transfer Request *(Do not complete Section 3 if filling in this section)*

20. File Name(s)	21. Originating Network	22. Destination Network or Media	23. Data Classification of Source File
	JWICS	Hard Drive	SECRET
	JWICS	Hard Drive	SECRET
	JWICS	Hard Drive	SECRET
	JWICS	Hard Drive	SECRET
	JWICS	Hard Drive	SECRET
	JWICS	Hard Drive	SECRET
	JWICS	Hard Drive	SECRET
	JWICS	Hard Drive	SECRET
	JWICS	Hard Drive	SECRET
24. Original Classification Authority (JWICS ONLY)			
25. Information Owner (JWICS ONLY)			
26. Requester Signature			
27. Supervisor Signature			

JSP FORM 11 FOR OFFICIAL USE ONLY (FOUO) WHEN FILLED IN APR 2019

Figure 2 (con't).



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)*:

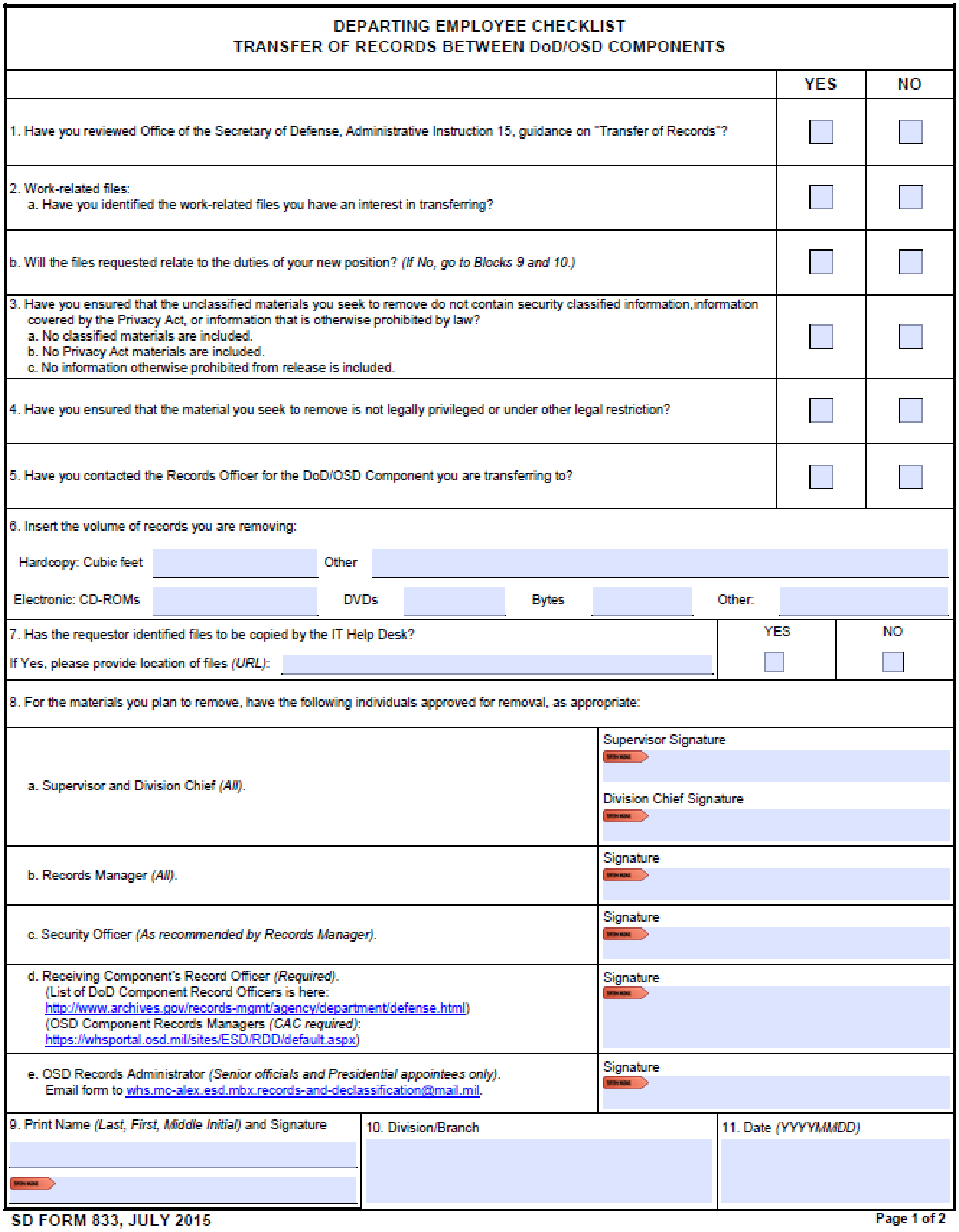
g. The Employee/Service Member/Contractor has ensured federal records in their possession (regardless of format, location, device, or classification) have been located and transferred to the organization's approved filing locations or to appropriate personnel. This includes, but is not limited to, review 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 □

SD FORM 822, NOV 2023

PREVIOUS EDITION IS OBSOLETE.

Page 1 of 5

Figure 3. SD 822, "Separating Personnel Records Accountability Checklist"



DEPARTING EMPLOYEE CHECKLIST
TRANSFER OF RECORDS BETWEEN DoD/OSD COMPONENTS

	YES	NO
1. Have you reviewed Office of the Secretary of Defense, Administrative Instruction 15, guidance on "Transfer of Records"?	□	□
2. Work-related files: a. Have you identified the work-related files you have an interest in transferring?	□	□
b. Will the files requested relate to the duties of your new position? *(If No, go to Blocks 9 and 10.)*	□	□
3. Have you ensured that the unclassified materials you seek to remove do not contain security classified information,information covered by the Privacy Act, or information that is otherwise prohibited by law? a. No classified materials are included. b. No Privacy Act materials are included. c. No information otherwise prohibited from release is included.	□	□
4. Have you ensured that the material you seek to remove is not legally privileged or under other legal restriction?	□	□
5. Have you contacted the Records Officer for the DoD/OSD Component you are transferring to?	□	□

6. Insert the volume of records you are removing:

Hardcopy: Cubic feet ______ Other ______

Electronic: CD-ROMs ______ DVDs ______ Bytes ______ Other: ______

	YES	NO
7. Has the requestor identified files to be copied by the IT Help Desk? If Yes, please provide location of files *(URL)*: ______	□	□

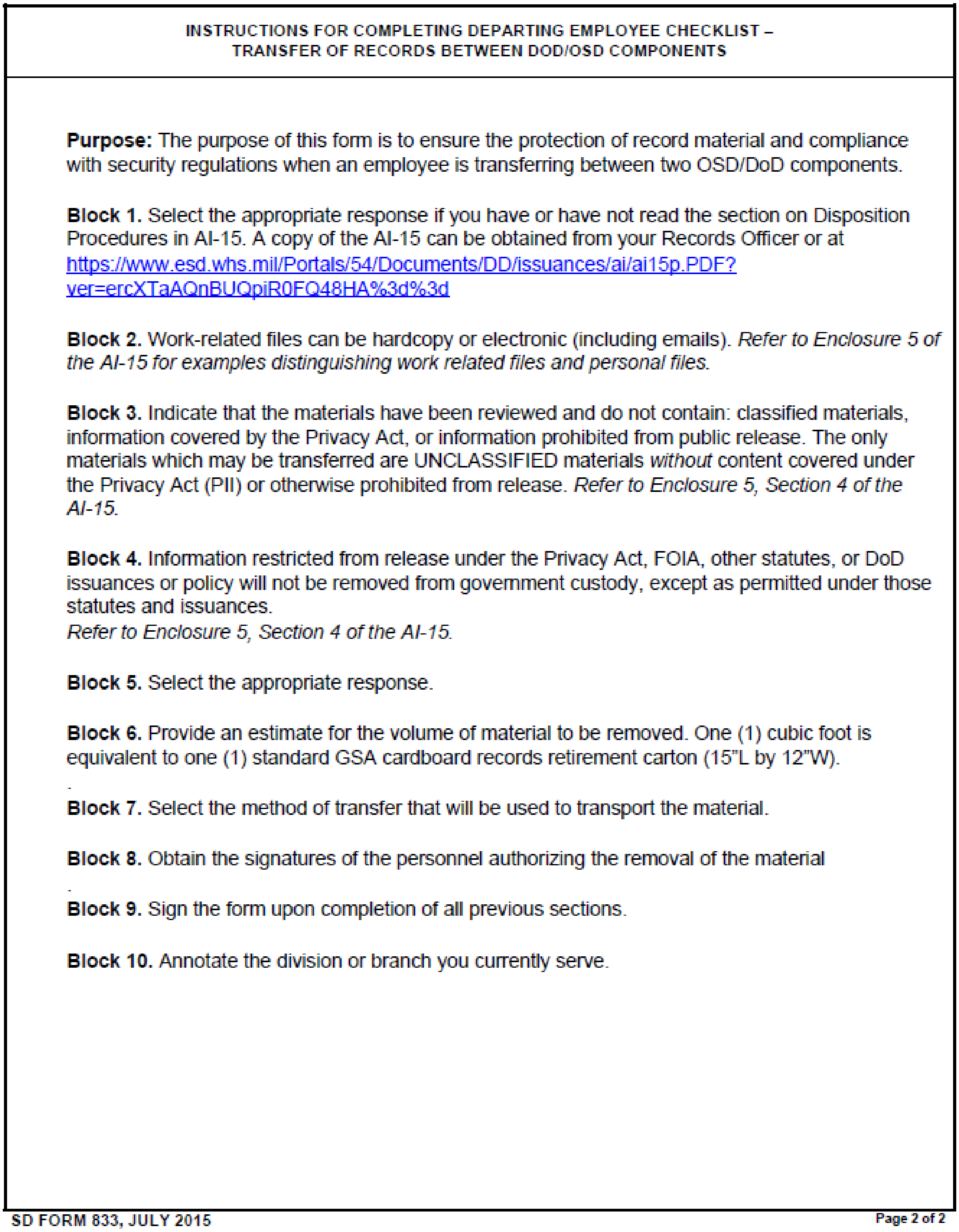
8. For the materials you plan to remove, have the following individuals approved for removal, as appropriate:

a. Supervisor and Division Chief *(All)*.	Supervisor Signature Division Chief Signature
b. Records Manager *(All)*.	Signature
c. Security Officer *(As recommended by Records Manager)*.	Signature
d. Receiving Component's Record Officer *(Required)*. (List of DoD Component Record Officers is here: http://www.archives.gov/records-mgmt/agency/department/defense.html) (OSD Component Records Managers *(CAC required)*: https://whsportal.osd.mil/sites/ESD/RDD/default.aspx)	Signature
e. OSD Records Administrator *(Senior officials and Presidential appointees only)*. Email form to whs.mc-alex.esd.mbx.records-and-declassification@mail.mil.	Signature

9. Print Name *(Last, First, Middle Initial)* and Signature	10. Division/Branch	11. Date *(YYYYMMDD)*

SD FORM 833, JULY 2015 Page 1 of 2

Figure 4. SD Form 833, "Transfer of Records Between DoD/OSD Components"



INSTRUCTIONS FOR COMPLETING DEPARTING EMPLOYEE CHECKLIST –
TRANSFER OF RECORDS BETWEEN DOD/OSD COMPONENTS

Purpose: The purpose of this form is to ensure the protection of record material and compliance with security regulations when an employee is transferring between two OSD/DoD components.

Block 1. Select the appropriate response if you have or have not read the section on Disposition Procedures in AI-15. A copy of the AI-15 can be obtained from your Records Officer or at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/ai/ai15p.PDF?ver=ercXTaAQnBUQpiR0FQ48HA%3d%3d

Block 2. Work-related files can be hardcopy or electronic (including emails). *Refer to Enclosure 5 of the AI-15 for examples distinguishing work related files and personal files.*

Block 3. Indicate that the materials have been reviewed and do not contain: classified materials, information covered by the Privacy Act, or information prohibited from public release. The only materials which may be transferred are UNCLASSIFIED materials *without* content covered under the Privacy Act (PII) or otherwise prohibited from release. *Refer to Enclosure 5, Section 4 of the AI-15.*

Block 4. Information restricted from release under the Privacy Act, FOIA, other statutes, or DoD issuances or policy will not be removed from government custody, except as permitted under those statutes and issuances.
Refer to Enclosure 5, Section 4 of the AI-15.

Block 5. Select the appropriate response.

Block 6. Provide an estimate for the volume of material to be removed. One (1) cubic foot is equivalent to one (1) standard GSA cardboard records retirement carton (15"L by 12"W).
.

Block 7. Select the method of transfer that will be used to transport the material.

Block 8. Obtain the signatures of the personnel authorizing the removal of the material
.

Block 9. Sign the form upon completion of all previous sections.

Block 10. Annotate the division or branch you currently serve.

SD FORM 833, JULY 2015

Page 2 of 2

Figure 4 (con't)

(INTENTIONALLY BLANK)

ENCLOSURE B

RECORDS AND INFORMATION RISK MANAGEMENT PROGRAM

1. Introduction. The Records and Information Risk Management Program (RIRMP) is a process of identifying JS and CCMD record risks, prioritizing risks, and deciding how to mitigate risks by identifying records management practices (creation, capture, access to, storage or disposal of records) with the organization's legal and financial activities. The following describes how the Joint Staff ROs, RLs, and RCs will manage risk. CCMD CRMs may adopt these practices into their processes, procedures, and standard operating procedures (SOPs).

2. Goals of RIRMP

a. Align risk management methodologies. Align risk management methodologies with references (t) and (u) to help facilitate consistency across the Joint Staff to improve risk communication and decision-making processes.

b. Define Risks. Directorate senior leaders will empower appointed RLs and RCs and require them to define risks clearly and concisely quantitatively and qualitatively by communicating risk probably with their potential impacts.

c. Advocate protection of information. Directorate senior leaders and ROs will work together to advocate the responsibility everyone has to protect records and information from risks. RLs will support advocating efforts by educating and establishing working relationships.

d. Establish scaling methodologies of risk. Once the risk is defined, RLs and RCs will work together to scale and report risks by identifying, analyzing, evaluating, and communicating risks and mitigation measures to ROs.

e. Establish constant monitoring of risk mitigation plans. Once the risk and mitigation plans are in place, RCs will be responsible for constant monitoring of the plan and will communicate to the RLs any changes needing to be made.

3. Framework. To retain consistency across the Joint Staff, the Joint Risk Analysis Methodology (JRAM) has three main components that RCs will use when assessing risks to records.

a. Risk Appraisal. When conducting inventories, RCs will gather knowledge and understanding of records and will assess which records are at risk and will scale the risks by utilizing the Joint Staff Risk Assessment for Records and Information Matrix.

b. Risk Management. Based on the risk scaling results, RCs will be responsible for communicating the risk to the RLs and together they will develop plans to manage and mitigate the risk. The RLs will communicate the findings and mitigation plans to the ROs, who will communicate the findings and mitigation plans to senior leaders. Senior leaders will then make the decision to accept, avoid, mitigate, or transfer the risk.

c. Risk Communication. Risks and plans of mitigation will be communicated through designated record managers to senior leadership.

4. Risk assessment

a. Risk Identification. Risk identification helps RCs recognize potential and actual threats to records. Mandatory annual inventories, along with JS reporting requirements, will help to keep records safe.

b. Risk Evaluation. RCs will evaluate the risk and compare them to the consequence.

5. Risk factors

a. Threats or Hazards. Threats or hazards alone or in combination have the potential to cause harm to the record.

(1) Threats. Threats are state or non-state entities with the capability of causing harm.

(2) Hazards. Hazards are actions, decisions, or security, environmental, demographic, political, technical, or social conditions with potential to cause harm.

b. Drivers of Risk. Drivers of risk are factors or variables that influence the likelihood, impact, or timing of risks. Drivers are the root causes or sources of risks, such as retrieval challenges, unnecessary retention of data, or noncompliance of record disposition. Understanding the drivers of risks can help RCs, RLs, and ROs with senior leader input, prioritize, mitigate, or avoid them.

6. Trustworthy Records

a. IAW reference (pp), “trustworthy records” are records that will capture business legal and financial requirements. Trustworthy records have four characteristics:

(1) Reliability. A reliable web site is one whose content can be trusted as a full and accurate representation of the transactions, activities, or facts to which it attests and therefore can be depended upon during subsequent transactions or activities.

(2) Authenticity. An authentic web site is one that is proven to be what it purports to be and to have been created by the agency with which it is identified. Web site-related records should be created by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.

(3) Integrity. The integrity of a web content record refers to it being complete and unaltered.

(4) Usability. A usable web site is one that can be located, retrieved, presented, and interpreted. In retrieval and use, you should be able to directly connect the web site to the business activity or transaction that produced it. You should be able to identify both the site and its content within the context of broader business activities and functions. The links between content, contextual, and structural web site-related records that document agency web site activities should be maintained. These contextual linkages should provide an understanding of the transactions that created and used them.

7. Reporting Frequency

a. Risk assessments will be conducted on an annual basis and will align with the annual inventory requirements.

b. Risk assessments can be completed more frequently than annually. A risk assessment is required when there is a change to how the information is managed or when EIS undergoes changes such as upgrades or when new software is introduced. A risk assessment is also required when there is a threat to information and its supported system that could cause detrimental impacts to the JS operations and its functionalities.

8. Submitting Procedures

a. Prior to any SAV, risk assessments and their supporting documents (inventory list, essential records list) will be submitted to <js.pentagon.dom.list.sjs-imd-researchers@mail.mil> for staff review and evaluation for JS RMs.

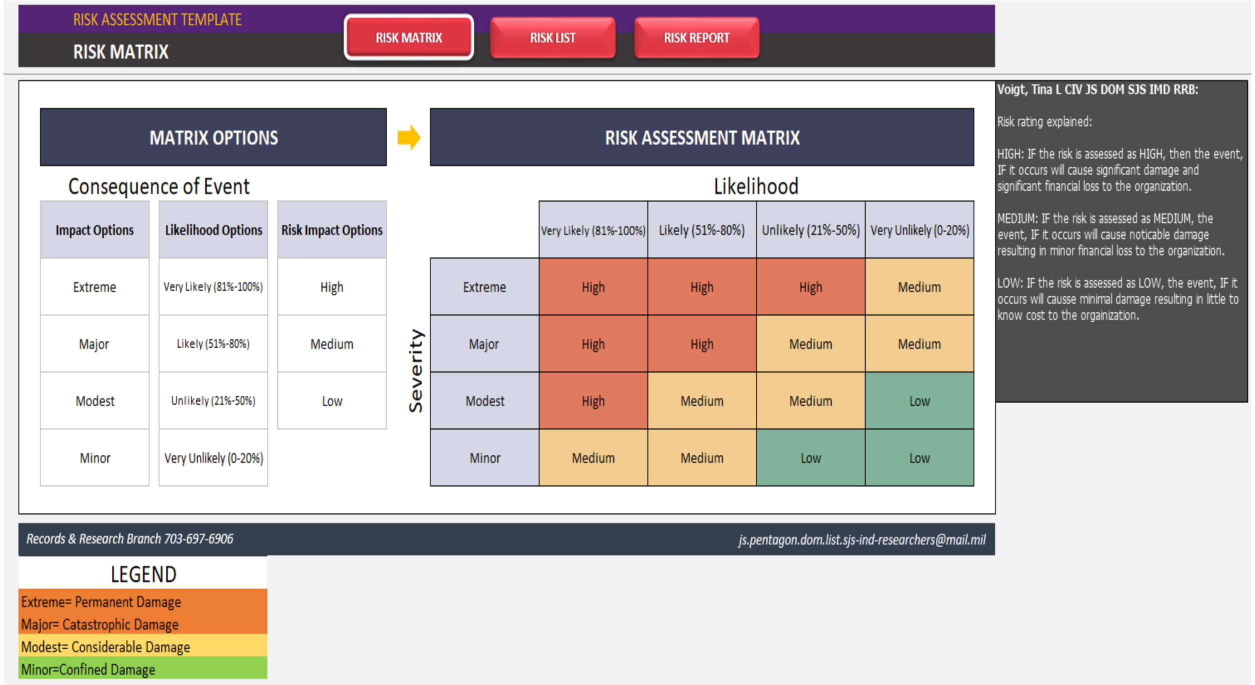
b. Add the Joint Staff Directorate for Command, Control, Communications and Computers (C4)/Cyber, J-6 if the assessment shows detrimental concerns to C4 and cyber functions.

c. CCMD CRMs will follow guidance from their assigned commands.

9. Document Requirements

a. The documents provided in this section will be used by JS RLs and RCs. CCMD CRMs are encouraged to use the Joint Staff Risk Assessment for Records and Information Matrix; however, it is not a requirement.

b. By following the instructions provided on the Risk Assessment Template (Figures 5–7) and the instructions on JS Form 30V3 (Figure 8), each organization will be able to effectively scale and communicate risk and provide recommendations to mitigate them. RCs will email their findings to <js.pentagon.dom.list.sjs-imd-researchers@mail.mil>.



MATRIX OPTIONS

Consequence of Event

Impact Options	Likelihood Options	Risk Impact Options
Extreme	Very Likely (81%-100%)	High
Major	Likely (51%-80%)	Medium
Modest	Unlikely (21%-50%)	Low
Minor	Very Unlikely (0-20%)	

RISK ASSESSMENT MATRIX

Likelihood

Severity	Very Likely (81%-100%)	Likely (51%-80%)	Unlikely (21%-50%)	Very Unlikely (0-20%)
Extreme	High	High	High	Medium
Major	High	High	Medium	Medium
Modest	High	Medium	Medium	Low
Minor	Medium	Medium	Low	Low

Voigt, Tina L CIV JS DOM SJS IMD RRB:

Risk rating explained:

HIGH: IF the risk is assessed as HIGH, then the event, IF it occurs will cause significant damage and significant financial loss to the organization.

MEDIUM: IF the risk is assessed as MEDIUM, the event, IF it occurs will cause noticable damage resulting in minor financial loss to the organization.

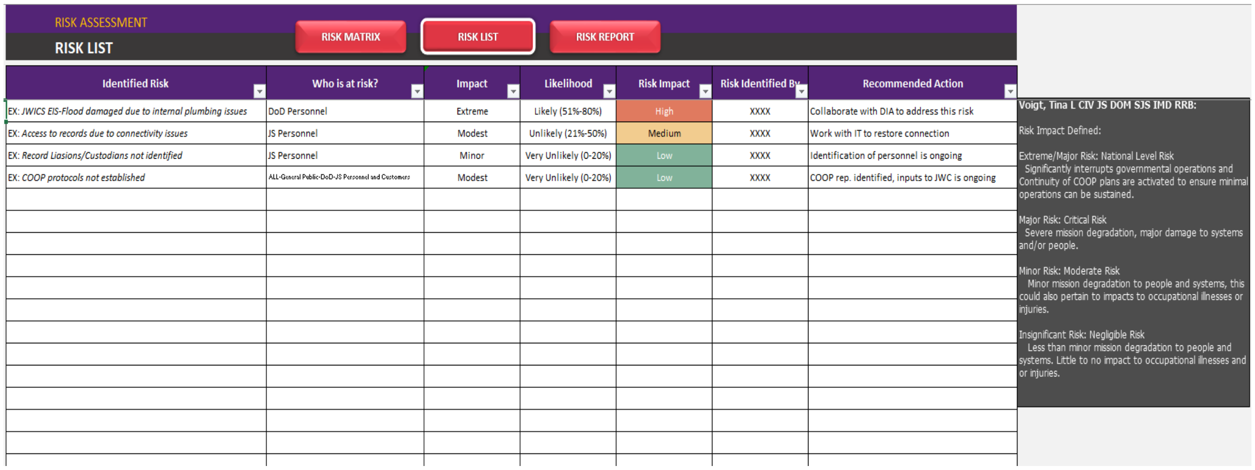
LOW: IF the risk is assessed as LOW, the event, IF it occurs will causse minimal damage resulting in little to know cost to the orgainization.

Records & Research Branch 703-697-6906 js.pentagon.dom.list.sjs-ind-researchers@mail.mil

LEGEND

Extreme= Permanent Damage
Major= Catastrophic Damage
Modest= Considerable Damage
Minor=Confined Damage

Figure 5. Joint Staff Risk Assessment Template-Risk Matrix



Identified Risk	Who is at risk?	Impact	Likelihood	Risk Impact	Risk Identified By	Recommended Action
EX: *JWICS EIS-Flood damaged due to internal plumbing issues*	DoD Personnel	Extreme	Likely (51%-80%)	High	XXXX	Collaborate with DIA to address this risk
EX: *Access to records due to connectivity issues*	JS Personnel	Modest	Unlikely (21%-50%)	Medium	XXXX	Work with IT to restore connection
EX: *Record Liasions/Custodians not identified*	JS Personnel	Minor	Very Unlikely (0-20%)	Low	XXXX	Identification of personnel is ongoing
EX: *COOP protocols not established*	ALL-General Public-DoD-JS Personnel and Customers	Modest	Very Unlikely (0-20%)	Low	XXXX	COOP rep. identified, inputs to JWC is ongoing

Voigt, Tina L CIV JS DOM SJS IMD RRB:

Risk Impact Defined:

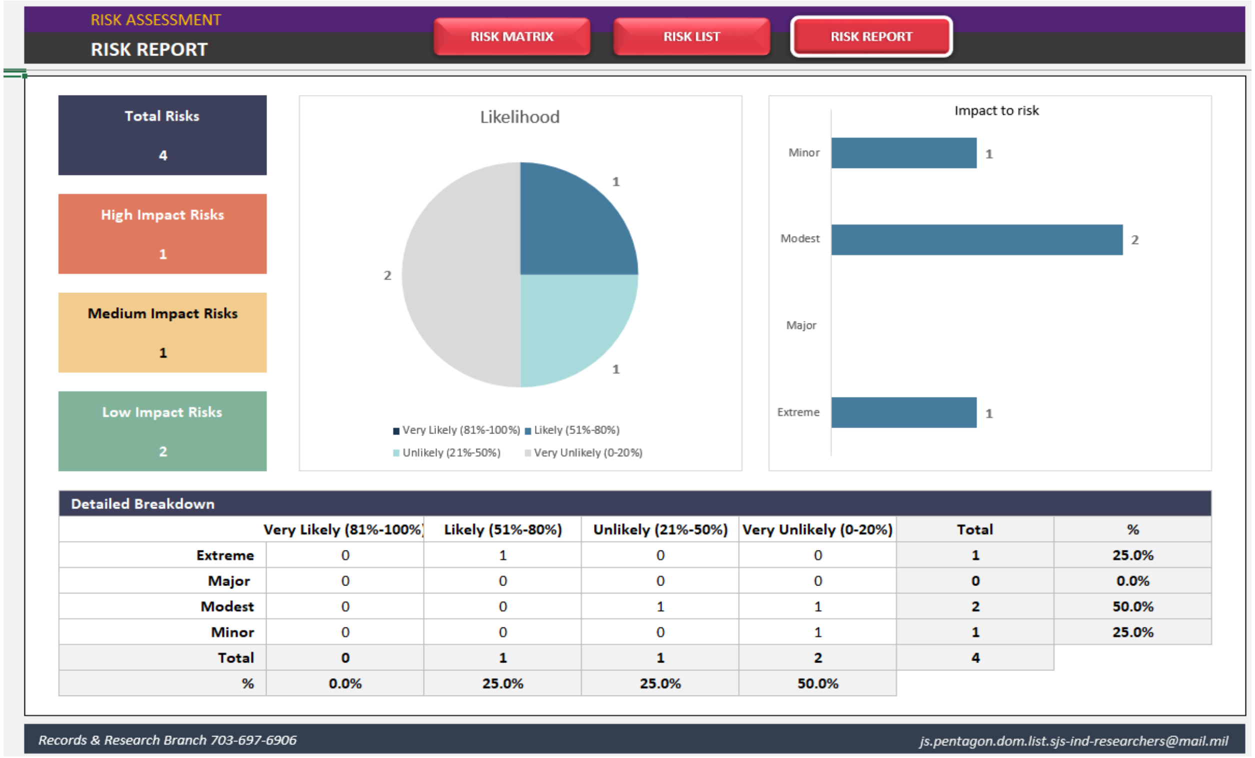
Extreme/Major Risk: National Level Risk
Significantly interrupts governmental operations and Continuity of COOP plans are activated to ensure minimal operations can be sustained.

Major Risk: Critical Risk
Severe mission degradation, major damage to systems and/or people.

Minor Risk: Moderate Risk
Minor mission degradation to people and systems, this could also pertain to impacts to occupational illnesses or injuries.

Insignificant Risk: Negligible Risk
Less than minor mission degradation to people and systems. Little to no impact to occupational illnesses and or injuries.

Figure 6. Joint Staff Risk Assessment Template-Risk List



Total Risks
4

High Impact Risks
1

Medium Impact Risks
1

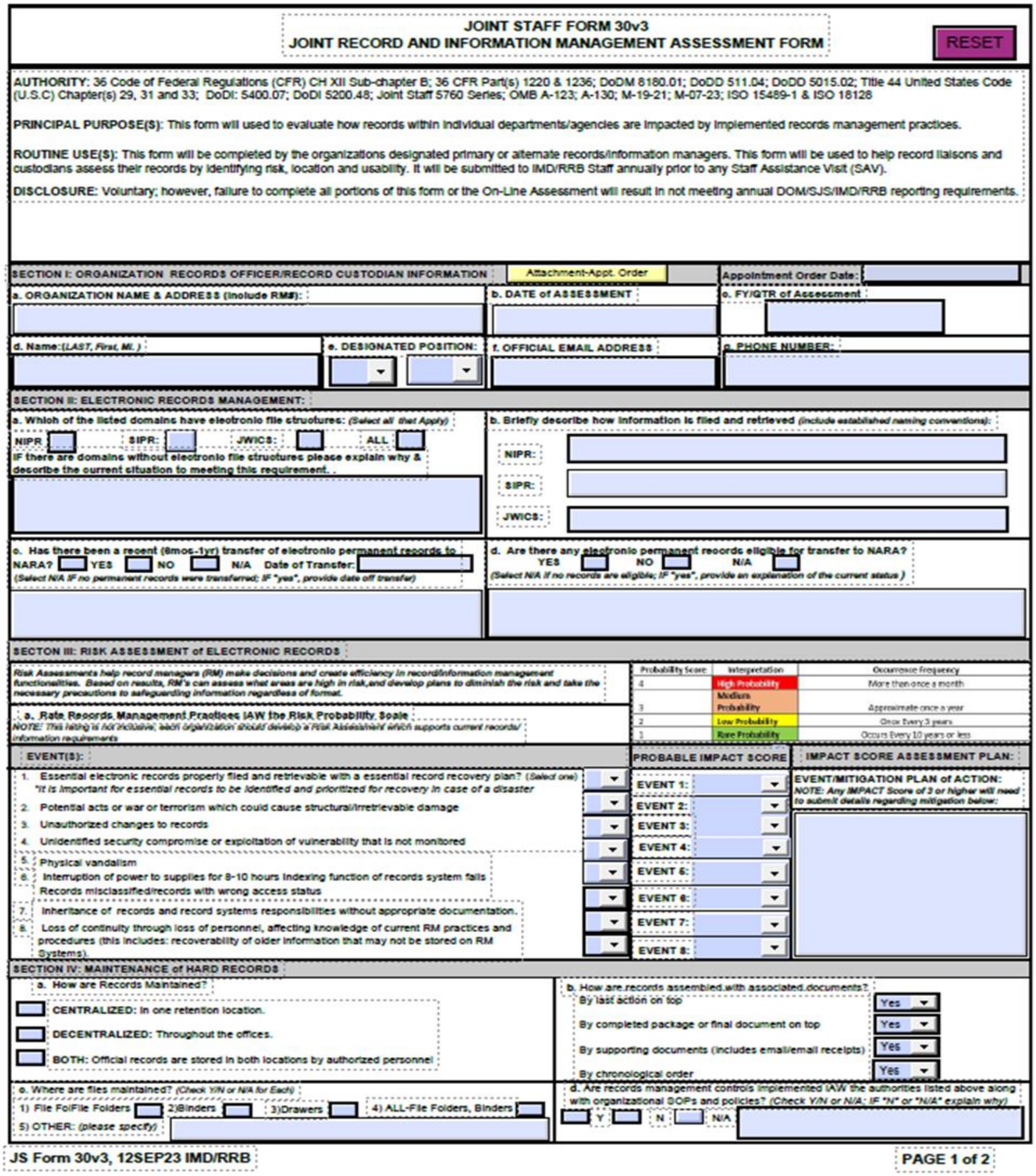
Low Impact Risks
2

Detailed Breakdown

	Very Likely (81%-100%)	Likely (51%-80%)	Unlikely (21%-50%)	Very Unlikely (0-20%)	Total	%
Extreme	0	1	0	0	1	25.0%
Major	0	0	0	0	0	0.0%
Modest	0	0	1	1	2	50.0%
Minor	0	0	0	1	1	25.0%
Total	0	1	1	2	4	
%	0.0%	25.0%	25.0%	50.0%		

Records & Research Branch 703-697-6906 *js.pentagon.dom.list.sjs-ind-researchers@mail.mil*

Figure 7. Joint Staff Risk Assessment Template-Risk Analysis Report



JOINT STAFF FORM 30v3
JOINT RECORD AND INFORMATION MANAGEMENT ASSESSMENT FORM

RESET

AUTHORITY: 36 Code of Federal Regulations (CFR) CH XII Sub-chapter B; 36 CFR Part(s) 1220 & 1236; DoDM 8180.01; DoDD 511.04; DoDD 5015.02; Title 44 United States Code (U.S.C) Chapter(s) 29, 31 and 33; DoDI: 5400.07; DoDI 5200.48; Joint Staff 5760 Series; OMB A-123; A-130; M-19-21; M-07-23; ISO 15489-1 & ISO 18128

PRINCIPAL PURPOSE(S): This form will used to evaluate how records within individual departments/agencies are impacted by implemented records management practices.

ROUTINE USE(S): This form will be completed by the organizations designated primary or alternate records/information managers. This form will be used to help record liaisons and custodians assess their records by identifying risk, location and usability. It will be submitted to IMD/RRB Staff annually prior to any Staff Assistance Visit (SAV).

DISCLOSURE: Voluntary; however, failure to complete all portions of this form or the On-Line Assessment will result in not meeting annual DOM/SJS/IMD/RRB reporting requirements.

SECTION I: ORGANIZATION RECORDS OFFICER/RECORD CUSTODIAN INFORMATION Attachment-Appt. Order Appointment Order Date: ☐

a. ORGANIZATION NAME & ADDRESS (include RM#): ☐

b. DATE of ASSESSMENT ☐

c. FY/QTR of Assessment ☐

d. Name:(*LAST, First, MI.*) ☐

e. DESIGNATED POSITION: ☐ ▼ ☐ ▼

f. OFFICIAL EMAIL ADDRESS ☐

g. PHONE NUMBER: ☐

SECTION II: ELECTRONIC RECORDS MANAGEMENT:

a. Which of the listed domains have electronic file structures: *(Select all that Apply)*
NIPR ☐ SIPR: ☐ JWICS: ☐ ALL ☐
IF there are domains without electronic file structures please explain why & describe the current situation to meeting this requirement. .
☐

b. Briefly describe how information is filed and retrieved *(include established naming conventions)*:
NIPR: ☐
SIPR: ☐
JWICS: ☐

c. Has there been a recent (6mos-1yr) transfer of electronic permanent records to NARA? ☐ YES ☐ NO ☐ N/A Date of Transfer: ☐
(Select N/A IF no permanent records were transferred; IF "yes", provide date off transfer)
☐

d. Are there any electronic permanent records eligible for transfer to NARA?
YES ☐ NO ☐ N/A ☐
(Select N/A if no records are eligible; IF "yes", provide an explanation of the current status)
☐

SECTON III: RISK ASSESSMENT of ELECTRONIC RECORDS

Risk Assessments help record managers (RM) make decisions and create efficiency in record/information management functionalities. Based on results, RM's can assess what areas are high in risk,and develop plans to diminish the risk and take the necessary precautions to safeguarding information regardless of format.

Probability Score	Interpretation	Occurrence Frequency
4	🟥 High Probability	More than once a month
3	🟧 Medium Probability	Approximate once a year
2	🟨 Low Probability	Once Every 3 years
1	🟩 Rare Probability	Occurs Every 10 years or less

a. Rate Records Management Practices IAW the Risk Probability Scale
NOTE: This listing is not inclusive; each organization should develop a Risk Assessment which supports current records/ information requirements

EVENT(S):		PROBABLE IMPACT SCORE	IMPACT SCORE ASSESSMENT PLAN:
1. Essential electronic records properly filed and retrievable with a essential record recovery plan? *(Select one)* *"It is important for essential records to be identified and prioritized for recovery in case of a disaster*	☐ ▼	EVENT 1: ☐ ▼	EVENT/MITIGATION PLAN of ACTION: *NOTE: Any IMPACT Score of 3 or higher will need to submit details regarding mitigation below:* ☐
2. Potential acts or war or terrorism which could cause structural/irretrievable damage	☐ ▼	EVENT 2: ☐ ▼	
3. Unauthorized changes to records	☐ ▼	EVENT 3: ☐ ▼	
4. Unidentified security compromise or exploitation of vulnerability that is not monitored	☐ ▼	EVENT 4: ☐ ▼	
5. Physical vandalism	☐ ▼	EVENT 5: ☐ ▼	
6. Interruption of power to supplies for 8-10 hours indexing function of records system fails Records misclassified/records with wrong access status	☐ ▼	EVENT 6: ☐ ▼	
7. Inheritance of records and record systems responsibilities without appropriate documentation.	☐ ▼	EVENT 7: ☐ ▼	
8. Loss of continuity through loss of personnel, affecting knowledge of current RM practices and procedures (this includes: recoverability of older information that may not be stored on RM Systems).	☐ ▼	EVENT 8: ☐ ▼	

SECTION IV: MAINTENANCE of HARD RECORDS

a. How are Records Maintained?
☐ CENTRALIZED: In one retention location.
☐ DECENTRALIZED: Throughout the offices.
☐ BOTH: Official records are stored in both locations by authorized personnel

b. How are records assembled with associated documents?
By last action on top Yes ▼
By completed package or final document on top Yes ▼
By supporting documents (includes email/email receipts) Yes ▼
By chronological order Yes ▼

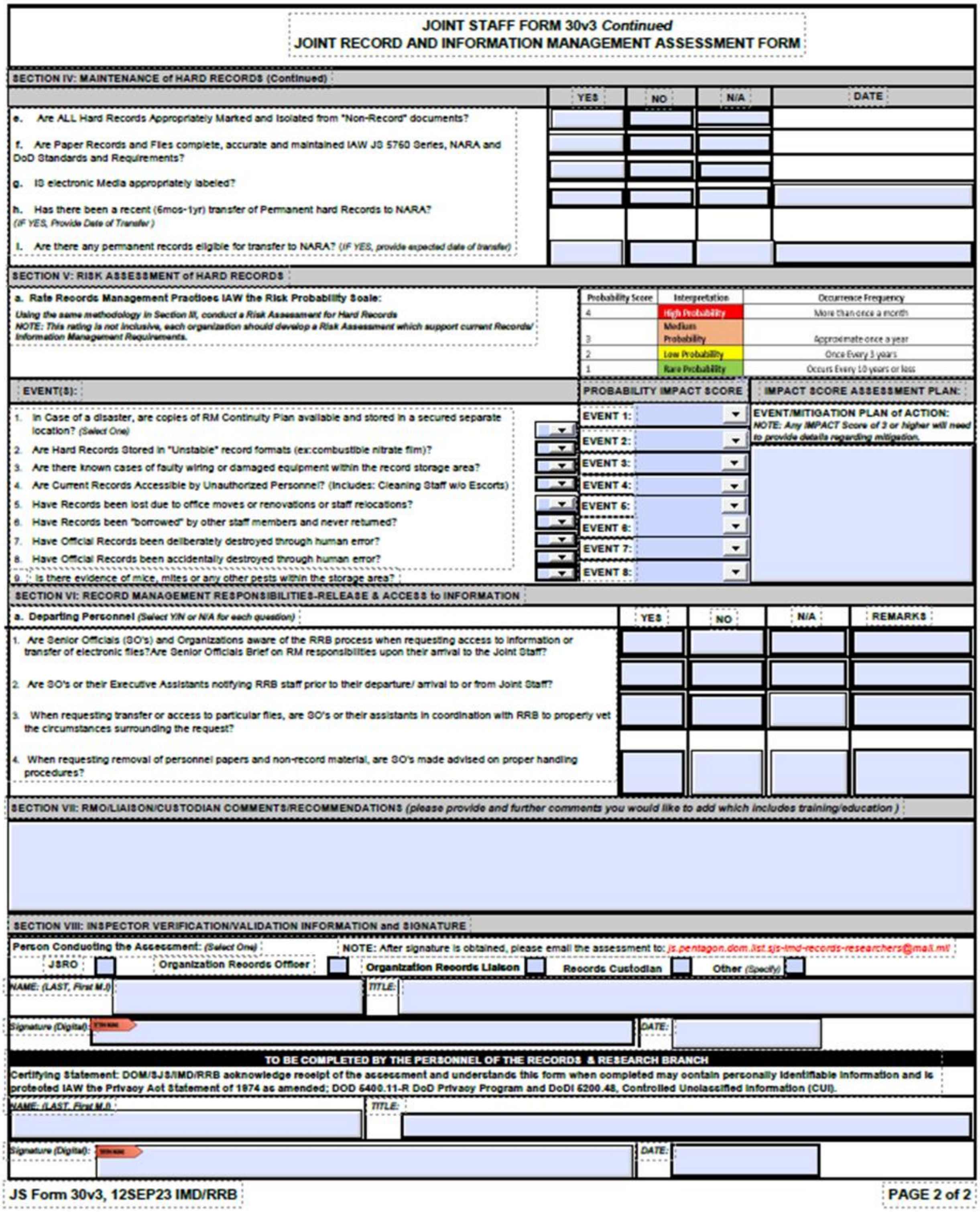
c. Where are files maintained? *(Check Y/N or N/A for Each)*
1) File Fol/File Folders ☐ 2)Binders ☐ 3)Drawers ☐ 4) ALL-File Folders, Binders ☐
5) OTHER: *(please specify)* ☐

d. Are records management controls implemented IAW the authorities listed above along with organizational SOPs and policies? *(Check Y/N or N/A; IF "N" or "N/A" explain why)*
☐ Y ☐ N ☐ N/A ☐

JS Form 30v3, 12SEP23 IMD/RRB

PAGE 1 of 2

Figure 8. JS Form 30v3 Record & Information Management Assessment Form



JOINT STAFF FORM 30v3 *Continued*
JOINT RECORD AND INFORMATION MANAGEMENT ASSESSMENT FORM

SECTION IV: MAINTENANCE of HARD RECORDS (Continued)

	YES	NO	N/A	DATE
e. Are ALL Hard Records Appropriately Marked and Isolated from "Non-Record" documents?				
f. Are Paper Records and Files complete, accurate and maintained IAW JS 5760 Series, NARA and DoD Standards and Requirements?				
g. IS electronic Media appropriately labeled?				
h. Has there been a recent (6mos-1yr) transfer of Permanent hard Records to NARA? *(IF YES, Provide Date of Transfer)*				
I. Are there any permanent records eligible for transfer to NARA? *(IF YES, provide expected date of transfer)*				

SECTION V: RISK ASSESSMENT of HARD RECORDS

a. Rate Records Management Practices IAW the Risk Probability Scale:

Using the same methodology in Section III, conduct a Risk Assessment for Hard Records
NOTE: This rating is not inclusive, each organization should develop a Risk Assessment which support current Records/ Information Management Requirements.

Probability Score	Interpretation	Occurrence Frequency
4	High Probability	More than once a month
3	Medium Probability	Approximate once a year
2	Low Probability	Once Every 3 years
1	Rare Probability	Occurs Every 10 years or less

EVENT(S):		PROBABILITY IMPACT SCORE	IMPACT SCORE ASSESSMENT PLAN:
1. In Case of a disaster, are copies of RM Continuity Plan available and stored in a secured separate location? *(Select One)*	▼	EVENT 1: ▼	**EVENT/MITIGATION PLAN of ACTION:** ***NOTE: Any IMPACT Score of 3 or higher will need to provide details regarding mitigation.***
2. Are Hard Records Stored in "Unstable" record formats (ex:combustible nitrate film)?	▼	EVENT 2: ▼	
3. Are there known cases of faulty wiring or damaged equipment within the record storage area?	▼	EVENT 3: ▼	
4. Are Current Records Accessible by Unauthorized Personnel? (Includes: Cleaning Staff w/o Escorts)	▼	EVENT 4: ▼	
5. Have Records been lost due to office moves or renovations or staff relocations?	▼	EVENT 5: ▼	
6. Have Records been "borrowed" by other staff members and never returned?	▼	EVENT 6: ▼	
7. Have Official Records been deliberately destroyed through human error?	▼	EVENT 7: ▼	
8. Have Official Records been accidentally destroyed through human error?	▼	EVENT 8: ▼	
9. Is there evidence of mice, mites or any other pests within the storage area?	▼		

SECTION VI: RECORD MANAGEMENT RESPONSIBILITIES-RELEASE & ACCESS to INFORMATION

a. Departing Personnel *(Select Y/N or N/A for each question)*	YES	NO	N/A	REMARKS
1. Are Senior Officials (SO's) and Organizations aware of the RRB process when requesting access to information or transfer of electronic files?Are Senior Officials Brief on RM responsibilities upon their arrival to the Joint Staff?				
2. Are SO's or their Executive Assistants notifying RRB staff prior to their departure/ arrival to or from Joint Staff?				
3. When requesting transfer or access to particular files, are SO's or their assistants in coordination with RRB to properly vet the circumstances surrounding the request?				
4. When requesting removal of personnel papers and non-record material, are SO's made advised on proper handling procedures?				

SECTION VII: RMO/LIAISON/CUSTODIAN COMMENTS/RECOMMENDATIONS *(please provide and further comments you would like to add which includes training/education)*

SECTION VIII: INSPECTOR VERIFICATION/VALIDATION INFORMATION and SIGNATURE

Person Conducting the Assessment: *(Select One)*

NOTE: After signature is obtained, please email the assessment to: *js.pentagon.dom.list.sjs-imd-records-researchers@mail.mil*

JSRO □ Organization Records Officer □ **Organization Records Liaison** □ Records Custodian □ Other *(Specify)* □

NAME: (LAST, First M.I) *TITLE:*

Signature (Digital): *DATE:*

TO BE COMPLETED BY THE PERSONNEL OF THE RECORDS & RESEARCH BRANCH

Certifying Statement: DOM/SJS/IMD/RRB acknowledge receipt of the assessment and understands this form when completed may contain personally identifiable information and is protected IAW the Privacy Act Statement of 1974 as amended; DOD 5400.11-R DoD Privacy Program and DoDI 5200.48, Controlled Unclassified Information (CUI).

NAME: (LAST, First M.I) *TITLE:*

Signature (Digital): *DATE:*

JS Form 30v3, 12SEP23 IMD/RRB **PAGE 2 of 2**

Figure 8 (con't)

(INTENTIONALLY LEFT BLANK)

ENCLOSURE C

ESSENTIAL RECORDS MANAGEMENT PROGRAM

1. Purpose

a. IAW reference (ll), "viable continuity programs include comprehensive processes for identification, protection, and accessibility of electronic and hardcopy essential records at primary, alternate and devolution locations."

b. IAW reference (r), essential records are needed to continue operations and protect the legal and financial rights of the organization. The Essential Records program (ERM) is an integral part to the success of COOP, as it defines how this organization will function when faced with emergency or other than emergency situations.

2. Goals and Objectives of Essential Records Management

a. Ensure the records categorized as essential are accessible, easily retrievable, and remain usable (free from damage) at all alternate operating locations during continuity of operation situations.

b. Ensure records identified as essential protect the rights and interests of the CJCS and CCMDs.

c. Ensure current essential inventory lists location are made known to those who would be using during a COOP event.

d. Ensure all designated RCs, RLs, and ROs and CCMD CRM ROs understand their role and responsibilities when managing essential records and establish guidance by creating SOPs that align with those responsibilities and COOP protocols.

e. Ensure record digitization requirements are adhered to across the JS and CCMDs by working with local DISA JSP representatives to ensure systems are being backed up or restored and information remains retrievable and usable.

3. Types of Records Critical to the JS and CCMDs

a. Reference (b), PRT 1223 defines essential records as "records an agency needs to meet operational responsibilities under national security emergencies or other emergency condition (emergency operating record) or to protect the legal and financial rights of the government and those affected by Government activities."

b. Listed below are the two categories of records that are categorized essential within the DoD.

(1) Emergency Operating Records. These include records (to include databases and essential data) essential to the continued functioning or the reconstitution of DoD mission-essential functions during and after a continuity event.

(2) Legal and Financial Records. These include records (to include databases and essential data) critical to carrying out essential legal and financial functions, and essential to the protection of the legal and financial rights of individuals who are directly affected by that agency's activities.

c. Under federal regulations, essential records must be accessible by continuity personnel from designated alternate facilities 0–8 hours (immediately), 8–12 hours (semi-immediate), 12–24 hours, 24–72 hours, and 72 hours to 30 days or more after activation of continuity plans.

d. Essential records must be integrated into all DoD continuity plans, policies and procedures, and will include:

(1) Ongoing training programs for all designated RLs and RCs, to include identification, inventory, protection, storage, access, and updating essential records and data.

(2) RLs and RCs, supported by the JSCRO or CCMD CRM ROs, will participate in annual COOP exercises to test accessibility and usability of information.

e. RLs will work with ROs to identify essential mission information managers and will train and educate them on responsibilities when assessing flow and accessibility of information. Training focus will be on the ease of retrieval as it pertains to the type of information and the time of need to access it.

f. Designated ROs will work with the heads of operational activities and communicate to RLs and RCs how to support COOP environments in real-world scenarios and during COOP exercises.

g. At a minimum, RCs will identify essential records and:

(1) Identify real-time and potential risks.

(2) Identify off-site storage locations and requirements.

(3) Identify survivability and usability of records regardless of format.

4. Steps to Identifying Essential Records

a. Determining what is and what is not essential can be a difficult task. As mentioned in Enclosure B, a risk assessment will align with annual inventory and SAV timelines, which helps to identify and categorize records as essential. The list below provides considerations when identifying and categorizing a record as being essential.

(1) Consider the following when identifying and categorizing records as essential.

(a) Are records required in emergency situations?

(b) Are records required to continue basic functions in emergency situations?

(c) If lost, damaged, or deemed unusable, will the record require an abundance of resources to recreate?

(d) Does the record protect the financial and legal business of the Joint Staff?

b. If no determination can be made, contact appointed JSCRO for JS concerns or the RRB <js.pentagon.dom.list.sjs-imd-researchers@mail.mil> for assistance. CCMD CRM ROs will follow organization protocols.

5. Steps for Categorizing Records as Essential

a. It is a requirement to categorize records as essential by:

(1) Conducting Research. Research policies, regulations, and other formal documents that require action from the JS.

(2) Knowing Mission Essential Functions. RCs must have knowledge of the Chairman's Mission Essential Functions (MEFs) as well as their own directorates MEFs as they should align with the CJCS.

(3) Identifying Records. Records are identified during inventories and captured in GRSs.

(4) Identifying Stakeholders. Knowing the stakeholders will help to understand the need and use of the record.

(5) Monitoring Changes. Continue to monitor for changes once records have been deemed essential. Any changes made to the organization can alter the categorization of the record.

b. Examples of Mission Essential Records include:

(1) SOPs and policies.

(2) Continuity plans and other emergency operation plans.

(3) Personal and payroll records.

(4) Vendor agreements and contracts.

(5) Memorandums of agreement/understanding.

(6) Delegations of authorities.

c. Examples of the CJCS Mission Essential Records include:

(1) Global Force Management.

(2) Situation monitoring.

(3) Planning.

(4) Force direction.

(5) Decision making support.

(6) Continuous connectivity (among the President, CCMDs, Secretary of Defense).

(7) Nuclear weapon monitoring.

d. For COOP to be successful, information must be accessible and retrievable at alternate operating locations 24/7. For protecting records—especially those that fall under Privacy Act of 1974 and Health Insurance Portability and Accountability Act 1996 laws—RCs must follow JSRO, ERM, COOP, JS J-6, JSP, and DISA plans and procedures for proper handling protocols.

e. When protecting information, JS RMs and CCMD CRMs are required to:

(1) Ensure information is backed up onto a secondary server.

(2) Ensure at alternate sites contingency plans are in place to support information retrieval should systems malfunction. Examples of contingent retrieval could be the use of compact disks (CDs) or hard drives.

(3) During the reconstitution phase (after the event has concluded), RCs and RLs will take an active role and assist their directorate in returning to normal operations.

f. After each COOP event, RCs and RLs will be required to capture their experiences by providing lessons learned feedback on JS Form 31 (see Figure 10) and CCMDs CRMs will capture their experiences IAW organization and unit guidelines.

6. COOP Procedures

a. RCs and RLs will manage/preserve records that were created from COOP events. At a minimum, the list below provides records that must be inventoried and preserved.

(1) Accident case files (includes nuclear, biological, chemical).

(2) Agreements.

(3) Command reports, incident reports, health reports, special reports, maps, and overlays.

(4) Counterintelligence files.

(5) Daily staff journals.

(6) Document registers and indexes.

(7) Operation plans (operations orders, warning orders, planning orders, fragmentary orders, execute orders).

(8) Meeting and teleconference minutes.

(9) Procedural documents that cover loss, theft, recovery, and survey of equipment.

b. Responsibilities when Operating under COOP Environments

NOTE: CCMD CRMs will provide guidance responsibilities as it pertains to established COOP plans.

(1) JS RLs will:

(a) Notify the personnel (and/or units/separate offices) involved in the operation of their responsibilities to manage operational records.

(b) Provide a central repository for collecting and safeguarding operational records.

(2) Senior leaders who provide oversight during COOP events will:

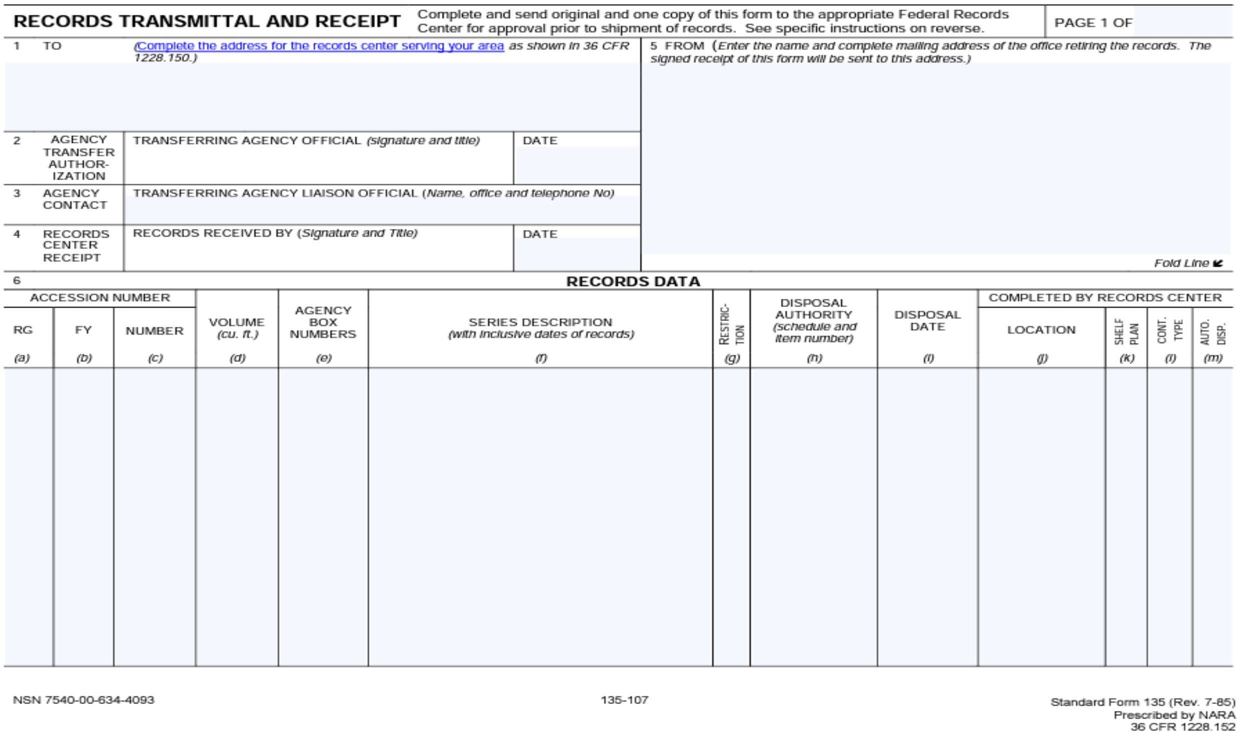
(a) Provide for the preservation of official operational records including designating a records management single point of contact at the appropriate organizational level.

(b) When the records are no longer needed for current operations, ensure they are shipped to the central repository by the JS RLs.

(3) JS RCs will provide direct support to COOP activities and will:

(a) Identify operational records and inventory them on SF 135, July 1985, “Records Transmittal and Receipt”, as shown below (see Figure 9).

(b) Collect and transfer records to the central repository monthly. Local commanders may elect to retain records required for operations until the next collection cycle or until no longer needed; however, all records will be transferred prior to re-deployment.



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

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

2 AGENCY TRANSFER AUTHORIZATION — TRANSFERRING AGENCY OFFICIAL *(signature and title)* — DATE

3 AGENCY CONTACT — TRANSFERRING AGENCY LIAISON OFFICIAL (*Name, office and telephone No)*

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.)*

Fold Line

6 **RECORDS DATA**

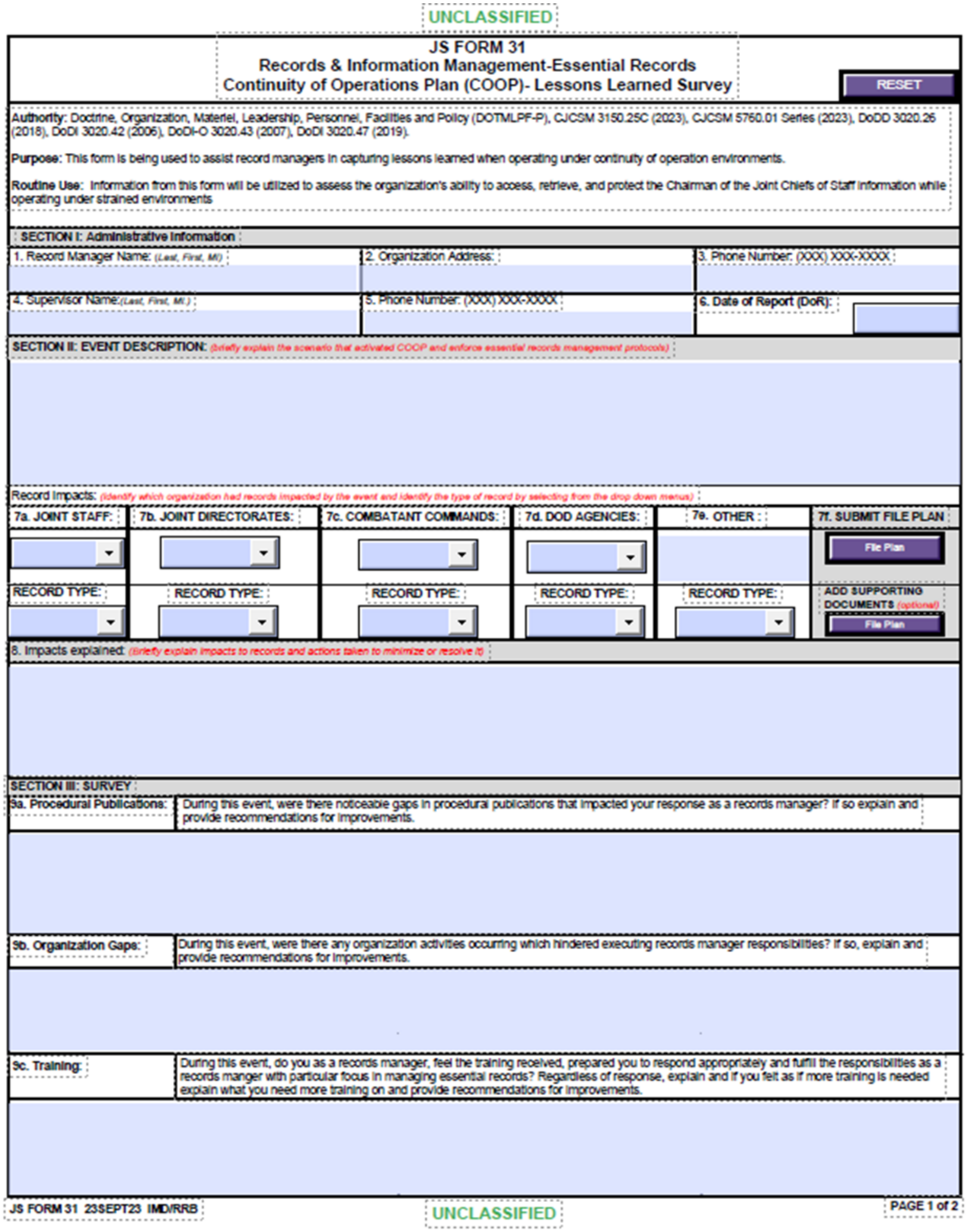
ACCESSION NUMBER			VOLUME *(cu. ft.)*	AGENCY BOX NUMBERS	SERIES DESCRIPTION *(with inclusive dates of records)*	RESTRIC-TION	DISPOSAL AUTHORITY *(schedule and item number)*	DISPOSAL DATE	COMPLETED BY RECORDS CENTER			
RG	FY	NUMBER							LOCATION	SHELF PLAN	CONT. TYPE	AUTO. DISP.
(a)	*(b)*	*(c)*	*(d)*	*(e)*	*(f)*	*(g)*	*(h)*	*(i)*	*(j)*	*(k)*	*(l)*	*(m)*

NSN 7540-00-634-4093

135-107

Standard Form 135 (Rev. 7-85)
Prescribed by NARA
36 CFR 1228.152

Figure 9. SF 135, "Records Transmittal and Receipt"



UNCLASSIFIED

JS FORM 31
Records & Information Management-Essential Records
Continuity of Operations Plan (COOP)- Lessons Learned Survey

RESET

Authority: Doctrine, Organization, Materiel, Leadership, Personnel, Facilities and Policy (DOTMLPF-P), CJCSM 3150.25C (2023), CJCSM 5760.01 Series (2023), DoDD 3020.26 (2018), DoDI 3020.42 (2006), DoDI-O 3020.43 (2007), DoDI 3020.47 (2019).

Purpose: This form is being used to assist record managers in capturing lessons learned when operating under continuity of operation environments.

Routine Use: Information from this form will be utilized to assess the organization's ability to access, retrieve, and protect the Chairman of the Joint Chiefs of Staff information while operating under strained environments

SECTION I: Administrative Information

1. Record Manager Name: *(Last, First, MI)*	2. Organization Address:	3. Phone Number: (XXX) XXX-XXXX
4. Supervisor Name:*(Last, First, MI.)*	5. Phone Number: (XXX) XXX-XXXX	**6. Date of Report (DoR):**

SECTION II: EVENT DESCRIPTION: *(briefly explain the scenario that activated COOP and enforce essential records management protocols)*

Record Impacts: *(identify which organization had records impacted by the event and identify the type of record by selecting from the drop down menus)*

7a. JOINT STAFF:	**7b. JOINT DIRECTORATES:**	**7c. COMBATANT COMMANDS:**	**7d. DOD AGENCIES:**	**7e. OTHER :**	**7f. SUBMIT FILE PLAN**
▾	▾	▾	▾		File Plan
RECORD TYPE:	**RECORD TYPE:**	**RECORD TYPE:**	**RECORD TYPE:**	**RECORD TYPE:**	**ADD SUPPORTING DOCUMENTS** *(optional)*
▾	▾	▾	▾	▾	File Plan

8. Impacts explained: *(Briefly explain impacts to records and actions taken to minimize or resolve it)*

SECTION III: SURVEY

9a. Procedural Publications: During this event, were there noticeable gaps in procedural publications that impacted your response as a records manager? If so explain and provide recommendations for improvements.

9b. Organization Gaps: During this event, were there any organization activities occurring which hindered executing records manager responsibilities? If so, explain and provide recommendations for improvements.

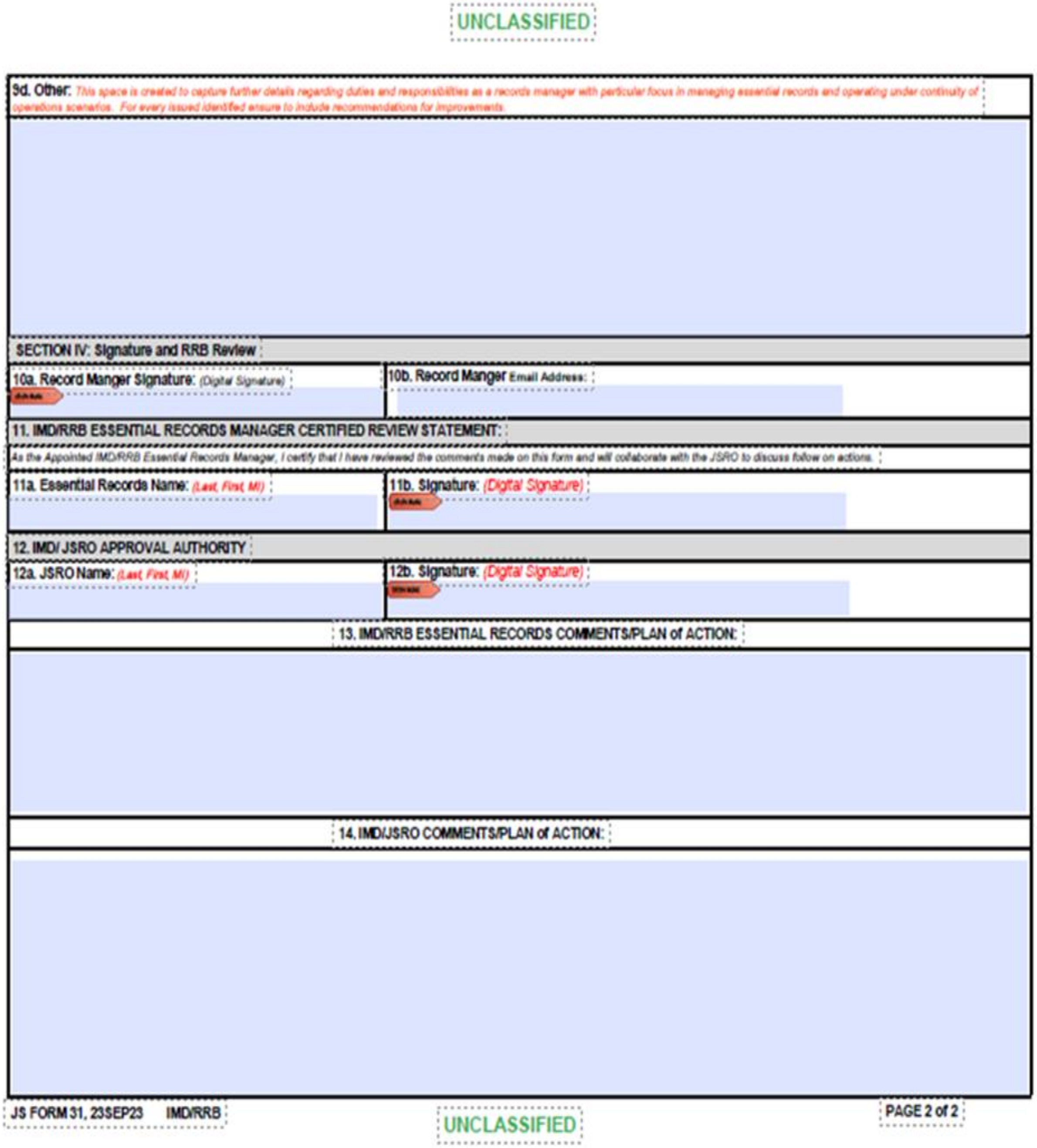
9c. Training: During this event, do you as a records manager, feel the training received, prepared you to respond appropriately and fulfill the responsibilities as a records manger with particular focus in managing essential records? Regardless of response, explain and if you felt as if more training is needed explain what you need more training on and provide recommendations for improvements.

JS FORM 31 23SEPT23 IMD/RRB

UNCLASSIFIED

PAGE 1 of 2

Figure 10. JS Form 31, "Records & Information Management-Essential Records-Continuity of Operations Program (COOP) Lessons Learned Survey"



UNCLASSIFIED

9d. Other: *This space is created to capture further details regarding duties and responsibilities as a records manager with particular focus in managing essential records and operating under continuity of operations scenarios. For every issued identified ensure to include recommendations for improvements.*

SECTION IV: Signature and RRB Review

10a. Record Manger Signature: *(Digital Signature)*

10b. Record Manger Email Address:

11. IMD/RRB ESSENTIAL RECORDS MANAGER CERTIFIED REVIEW STATEMENT:

As the Appointed IMD/RRB Essential Records Manager, I certify that I have reviewed the comments made on this form and will collaborate with the JSRO to discuss follow on actions.

11a. Essential Records Name: *(Last, First, MI)*

11b. Signature: *(Digital Signature)*

12. IMD/ JSRO APPROVAL AUTHORITY

12a. JSRO Name: *(Last, First, MI)*

12b. Signature: *(Digital Signature)*

13. IMD/RRB ESSENTIAL RECORDS COMMENTS/PLAN of ACTION:

14. IMD/JSRO COMMENTS/PLAN of ACTION:

JS FORM 31, 23SEP23 IMD/RRB

UNCLASSIFIED

PAGE 2 of 2

Figure 10 (con't).

(INTENTIONALLY BLANK)

ENCLOSURE D

ORGANIZATION MESSAGE SERVICE POLICY, CAPSTONE APPROACH, ELECTRONIC DISCOVERY, AND MANAGING TEXT MESSAGING

1. Organizational Messaging Service Policy

a. Organizational Messaging Service (OMS) policy establishes the guidelines to exchange organizational messages within and between the DoD, the U.S. Intelligence Community (IC), other U.S. Government (USG) agencies, and U.S. allies.

b. OMS is the DoD system of record for all organizational message traffic.

c. OMS provides a range of assured services to the customer community, which includes the Military Services, DoD Agencies, CCMDs, non-DoD USG activities, and the IC.

d. OMS supports the assured secure delivery of organizations' messages and includes the ability to exchange official information between military organization and to support interoperability between allied nations, non-DoD activities, and the IC.

e. Reference (ii) specifies the requirement for DoD electronic messaging services to operate in compliance with OMB Memorandum M-14-16.

2. Capstone Approach Introduction. The capstone approach was developed by NARA to assist federal agencies in complying with references (jj) and (ii), which have both been rescinded by current reference (e) and reinforced by reference (f). The original memorandums began an executive-wide effort to improve records management practices. Expectations set behind the capstone approach were to:

a. Improve records management accountability through enhanced documentation.

b. Increase identification of permanent records that held organization historical value which would ease efforts when transferring records to NARA.

c. Decrease costs of records management while increasing efficiency.

d. Optimize access to records responsive to eDiscovery or FOIA requests.

e. Leverage current technological capabilities.

3. Capstone Approach

a. The Capstone Approach is based on identifying e-mail accounts in accordance with the role/position of the person and the e-mails received. If the account owner receives and responds to e-mails that are critical or requires high level decisions, the account and the account owner will be identified as a capstone official and will be monitored by JSRO and CCMD CRMs. Executive Assistants (EAs), directorate directors and their EAs, program leads, heads of staff offices, and any other government official who may fall into this criterion will also be identified as capstone officials whose accounts also require monitoring.

b. The NA-1005 is a verification form used to verify capstone officials. The form assists in implementing GRS 6.1, Transmittal No 33 (2023), Email and other Electronic Messages Managed under a Capstone Approach.

c. Capstone E-mail Management

(1) RCs will work with RLs to manage capstone e-mail accounts by identifying accounts that contain records deemed permanent and require preservation.

(2) IAW reference (k), RCs will manage e-mail records disposition schedules.

(3) RCs will:

(1) Ensure e-mail records are scheduled.

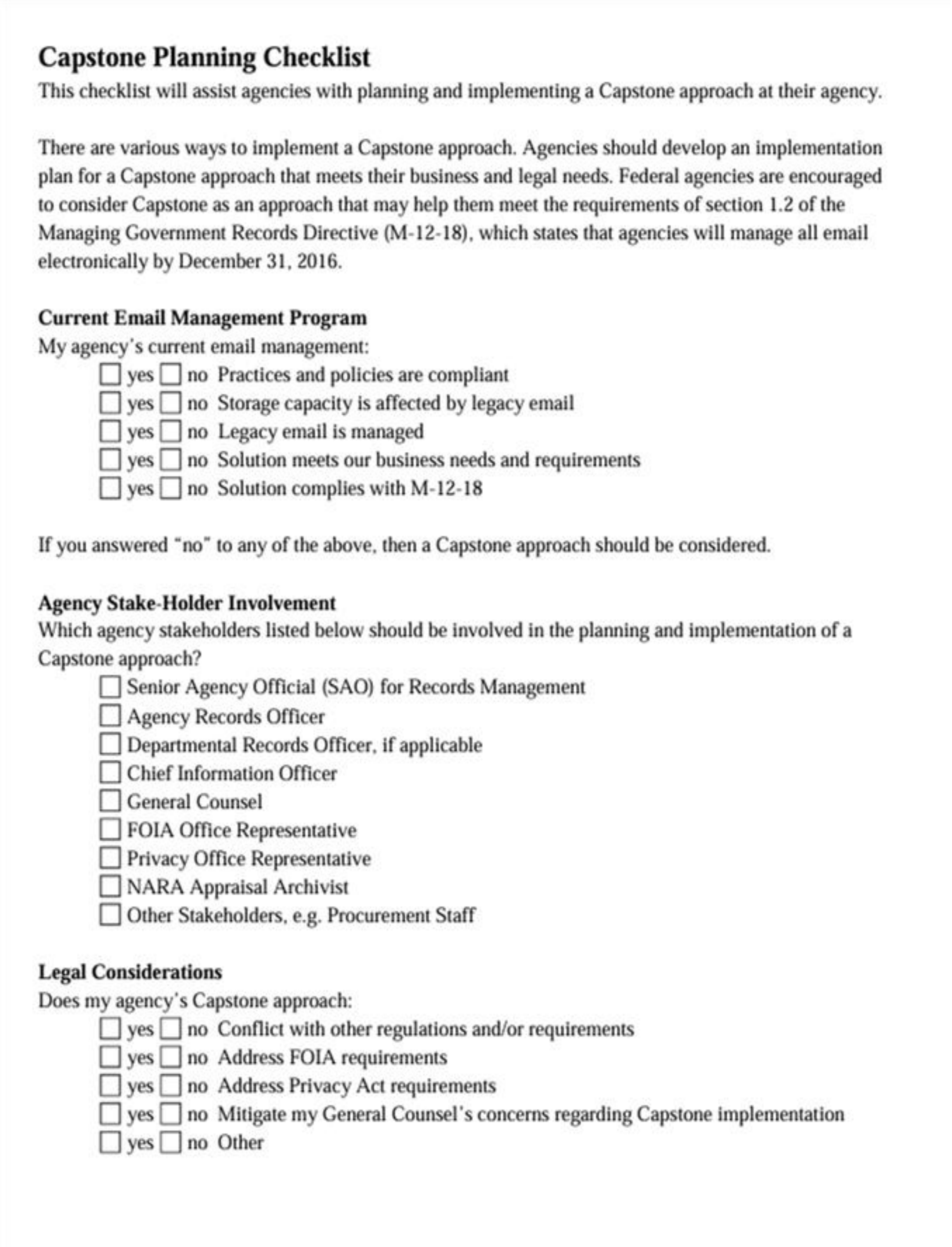
(2) Ensure e-mails are protected from unauthorized access, modification, or deletion of declared records.

(3) Ensure records in the repository are retrievable and usable.

(4) Ensure, IAW reference (b), 1236.22, Parts (1) and (3), e-mails capture and maintain required metadata.

(5) Decide if e-mail records and attachments can or should be associated with related records (follow directorate guidance).

d. To assist RCs prepare for planning and implementing a capstone e-mail management program, NARA provides the “Capstone Planning Checklist,” accessible at <https://www.archives.gov/files/records-mgmt/email-management/capstone-checklist.pdf>, that will lay the foundation for establishing the program. (See figure 11 below)



Capstone Planning Checklist

This checklist will assist agencies with planning and implementing a Capstone approach at their agency.

There are various ways to implement a Capstone approach. Agencies should develop an implementation plan for a Capstone approach that meets their business and legal needs. Federal agencies are encouraged to consider Capstone as an approach that may help them meet the requirements of section 1.2 of the Managing Government Records Directive (M-12-18), which states that agencies will manage all email electronically by December 31, 2016.

Current Email Management Program

My agency's current email management:

□ yes □ no Practices and policies are compliant
□ yes □ no Storage capacity is affected by legacy email
□ yes □ no Legacy email is managed
□ yes □ no Solution meets our business needs and requirements
□ yes □ no Solution complies with M-12-18

If you answered "no" to any of the above, then a Capstone approach should be considered.

Agency Stake-Holder Involvement

Which agency stakeholders listed below should be involved in the planning and implementation of a Capstone approach?

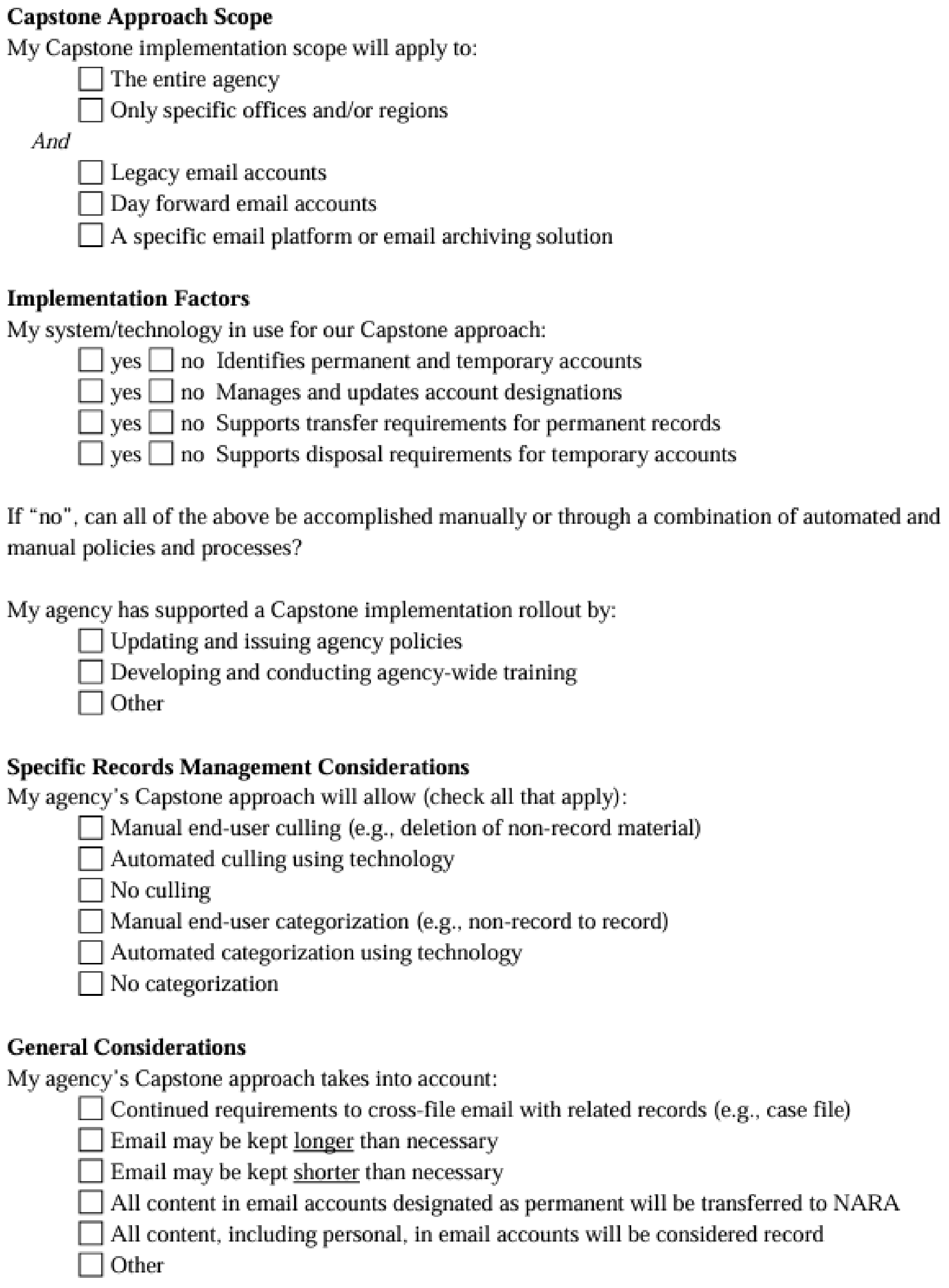
□ Senior Agency Official (SAO) for Records Management
□ Agency Records Officer
□ Departmental Records Officer, if applicable
□ Chief Information Officer
□ General Counsel
□ FOIA Office Representative
□ Privacy Office Representative
□ NARA Appraisal Archivist
□ Other Stakeholders, e.g. Procurement Staff

Legal Considerations

Does my agency's Capstone approach:

□ yes □ no Conflict with other regulations and/or requirements
□ yes □ no Address FOIA requirements
□ yes □ no Address Privacy Act requirements
□ yes □ no Mitigate my General Counsel's concerns regarding Capstone implementation
□ yes □ no Other

Figure 11. Capstone Planning Checklist



Capstone Approach Scope

My Capstone implementation scope will apply to:

□ The entire agency
□ Only specific offices and/or regions

And

□ Legacy email accounts
□ Day forward email accounts
□ A specific email platform or email archiving solution

Implementation Factors

My system/technology in use for our Capstone approach:

□ yes □ no Identifies permanent and temporary accounts
□ yes □ no Manages and updates account designations
□ yes □ no Supports transfer requirements for permanent records
□ yes □ no Supports disposal requirements for temporary accounts

If "no", can all of the above be accomplished manually or through a combination of automated and manual policies and processes?

My agency has supported a Capstone implementation rollout by:

□ Updating and issuing agency policies
□ Developing and conducting agency-wide training
□ Other

Specific Records Management Considerations

My agency's Capstone approach will allow (check all that apply):

□ Manual end-user culling (e.g., deletion of non-record material)
□ Automated culling using technology
□ No culling
□ Manual end-user categorization (e.g., non-record to record)
□ Automated categorization using technology
□ No categorization

General Considerations

My agency's Capstone approach takes into account:

□ Continued requirements to cross-file email with related records (e.g., case file)
□ Email may be kept longer than necessary
□ Email may be kept shorter than necessary
□ All content in email accounts designated as permanent will be transferred to NARA
□ All content, including personal, in email accounts will be considered record
□ Other

Figure 11 (con't)

4. Electronic Discovery (eDiscovery)

a. eDiscovery is a form of digital investigation that attempts to find evidence in e-mail or other forms of business communications that could be used as evidence for litigation purposes. It is governed by the regulations and laws listed in enclosure (i).

b. eDiscovery data includes:

(1) Data from online accounts.

(2) Internal applications.

(3) E-mail messages.

(4) Digital images.

(5) Social profiles.

(6) Web site content.

(7) Instant messages.

(8) Any information that supports litigation.

(9) Databases.

c. There are nine stages of eDiscovery.

(1) Information Governance. Information governance controls the policies for data collection.

(2) Identification. Identification dictates what and how the information will be reviewed and preserved managed during litigation.

(3) Preservation. ROs will receive formal instructions on how to preserve the data and they will communicate the procedures to RLs and RCs.

(4) Collection. Legal Counsel, Privacy, and ROs provide direct oversight on information preservation to ensure metadata (document creation dates, file size, and audit trails) are not altered in any way.

(5) Processing. When preparing for litigation, RCs will organize raw data to support the litigation.

(6) Review. RCs will conduct a review of information and separate pertinent information from non-pertinent information for preservation purposes.

(7) Analysis. RLs will conduct analysis with the RCs and identify "key" information that will support the litigation. After the information has been separated, based on the results from the analysis, RLs will work with ROs to prepare a litigation presentation and assist in designing the layout for court.

(8) Production. RCs will make all digital evidence into physical documents after all the key metadata have been captured.

(9) Preservation. Once all information is compiled and hard copies are made, the information will be turned over once again to the legal representatives for review and further processing.

d. Litigation holds will suspend any retention protocols and automatic deletions actions on records. ROs will need to work closely with RLs and RCs to ensure legal responsibilities are met.

4. Electronic Text Messaging

a. IAW reference (l), (m), and (mm), electronic messages (including chat or text) created or received for organizational purposes are records. A complete record of electronic message will include all messages, along with their attachments. The messages will also have required metadata and will be retrievable and usable and managed under GRS 6.1.

b. RCs and RLs will support ROs guidance by advocating to individual directorate staff members the responsibility everyone (including contractors) has in preserving e-mail, Teams Chat, or text messages that contain discussions regarding functions, policies, decisions, procedures, and essential transactions.

c. IAW reference (mm), RLs and RCs will work together and with organization service providers to ensure Microsoft Office 365 is configured properly to manage records created or received in Teams Chat, since Teams Chat is designated as the primary capability for managing messaging.

d. NARA provides a list of types of electronic messaging and examples. The list below can be found at <https://www.archives.gov/records-gmt/bulletins/2015/2015-02.html>.

Types of Electronic Messaging	**Examples**
Chat/Instant messaging	Google Chat, Skype for Business, IBM Sametime, Novell Groupwise Messenger, Facebook Messaging
Text messaging, also known as Multimedia Messaging Service (MMS) and Short Message Service (SMS)	iMessage, SMS, MMS on devices, such as Blackberry, Windows, Apple, or Android devices
Voicemail messaging • Can have voicemail sent to email as an attachment. • Messages can be sent or received from landline or mobile phones	Google Voice, voice to text conversion
Other messaging platforms or apps, such as social media or mobile device applications. These include text, media, and voice messages.	Twitter Direct Message, Slack, Snapchat, WhatsApp, Pigeon, Yammer, Jive, or other internal collaboration networks

Figure 12. Examples of Electronic Message Types

e. RCs and RLs will seek guidance from ROs to incorporate electronic messaging management into their SOPs and will follow guidance set in reference (l).

ENCLOSURE E

MANAGEMENT OF RECORDS AND INFORMATION

1. Introduction. Records provide a foundation for decision making mission planning and operations. The benefits of a good records management program are:

a. Organizing information for retrieval when needed.

b. Protecting records that are essential and critical to business operations.

c. Ensuring compliance which eliminates the cost of fines or other penalties.

2. Records Organization. Mission and business records should be located and arranged in a way that facilitates their use and disposition. RCs should consider the following when organizing records.

a. Access. Media-neutral records must be made easily accessible to users.

b. Security. Classified material must be maintained in security containers and on appropriate classified networks. Access to classified material must be restricted, monitored and free from unauthorized disclosure and are compliant with references (vv), (ww), and (xx).

c. Space. Records regardless of format, must be in spaces that meet current and anticipated needs.

d. Arrangement. Records will be positioned to provide accessibility and expediency to maximize their usage to JS and CCMD members.

3. Records File Plan. A records file plan documents the records and their use.

a. RCs will be responsible for managing the file plans and will identify each record by:

(1) Record Series Number.

(2) Record Series Title.

(3) Record Series Description.

(4) Disposition Instruction.

(5) Disposition Authority.

(6) Format (Paper or Electronic).

(7) Location.

(8) Additional information may include naming convention, records custodian name, and metadata.

b. RCs will annually review the file plan, records, and systems to ensure information is current, and accurate.

c. RCs will submit a copy of the file plan to RLs who review and provide recommendations (if required).

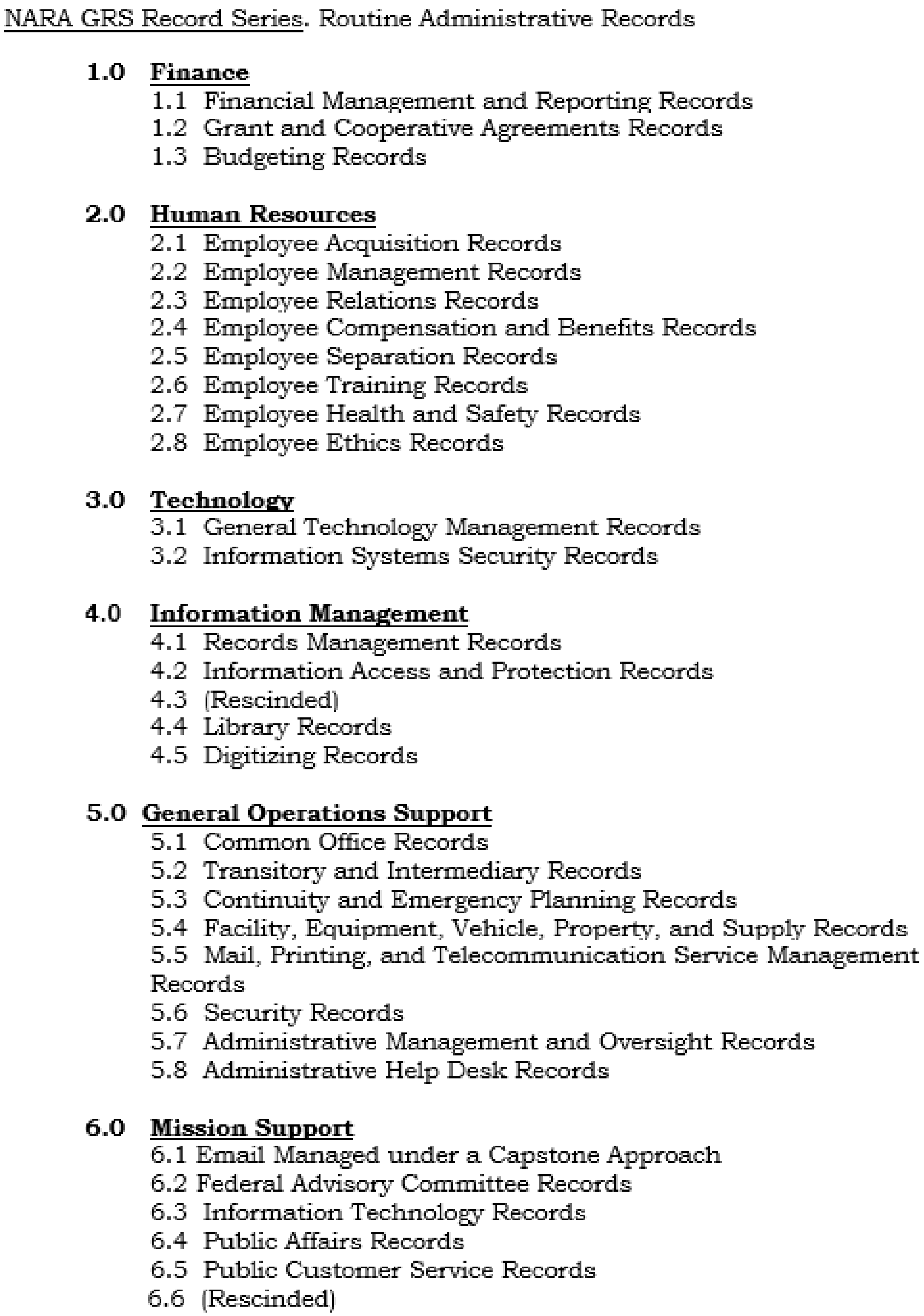
d. After modifications have been made, the RLs will send the file plan to the ROs, who will review and provide recommendations. Once finalized, the ROs will provide guidance on publication.

4. JS Mission Records and Business Records and Filing

a. IAW reference (j), business records document routine administrative activities, such as human resource, resource management IT, and legal activities. These record types are common records and can be found throughout the DoD. Business records are managed.

b. IAW reference (k), JS Mission Records (JSMRS) are records that capture the distinctive activities performed by the JS and are managed.

c. Below are the NARA GRS and the JSMRS list, which help RCs group records into filing categories. NARA GRS includes routine administrative records; the JMRS list includes records unique to the JS and CCMDs.



NARA GRS Record Series. Routine Administrative Records

1.0 Finance
- 1.1 Financial Management and Reporting Records
- 1.2 Grant and Cooperative Agreements Records
- 1.3 Budgeting Records

2.0 Human Resources
- 2.1 Employee Acquisition Records
- 2.2 Employee Management Records
- 2.3 Employee Relations Records
- 2.4 Employee Compensation and Benefits Records
- 2.5 Employee Separation Records
- 2.6 Employee Training Records
- 2.7 Employee Health and Safety Records
- 2.8 Employee Ethics Records

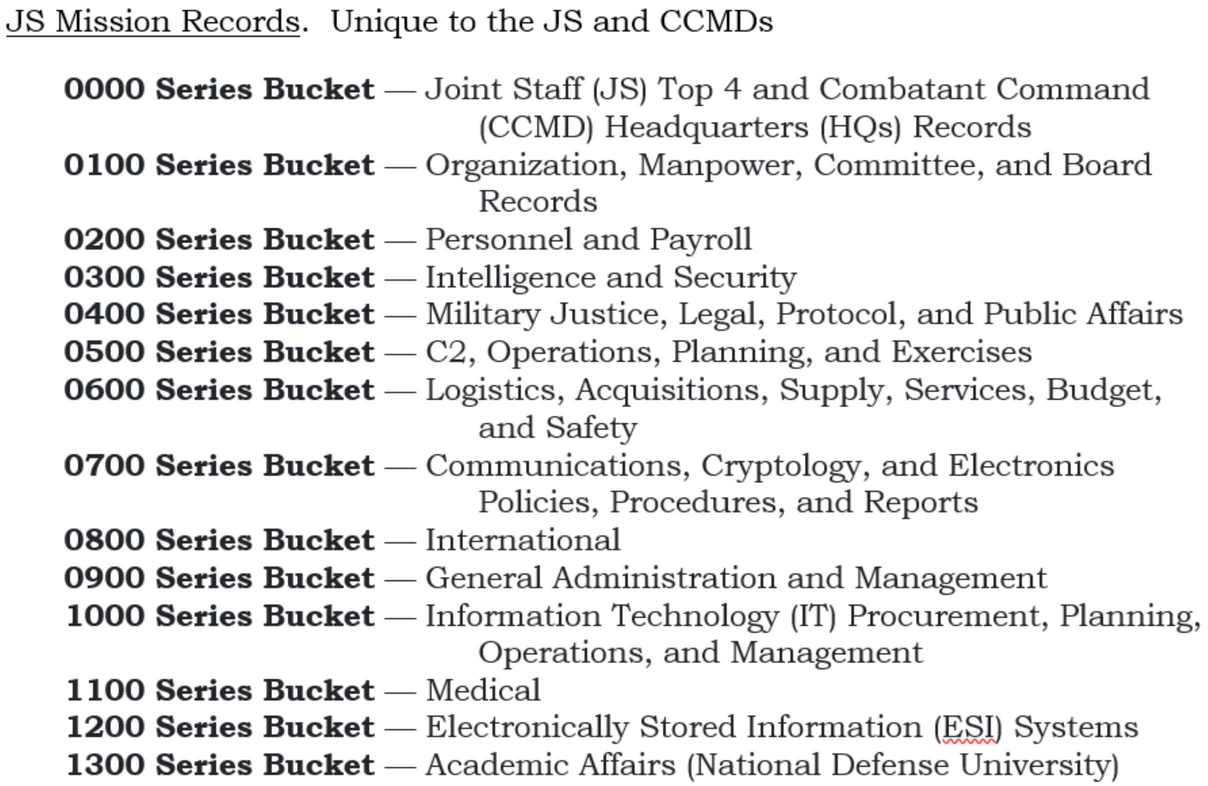
3.0 Technology
- 3.1 General Technology Management Records
- 3.2 Information Systems Security Records

4.0 Information Management
- 4.1 Records Management Records
- 4.2 Information Access and Protection Records
- 4.3 (Rescinded)
- 4.4 Library Records
- 4.5 Digitizing Records

5.0 General Operations Support
- 5.1 Common Office Records
- 5.2 Transitory and Intermediary Records
- 5.3 Continuity and Emergency Planning Records
- 5.4 Facility, Equipment, Vehicle, Property, and Supply Records
- 5.5 Mail, Printing, and Telecommunication Service Management Records
- 5.6 Security Records
- 5.7 Administrative Management and Oversight Records
- 5.8 Administrative Help Desk Records

6.0 Mission Support
- 6.1 Email Managed under a Capstone Approach
- 6.2 Federal Advisory Committee Records
- 6.3 Information Technology Records
- 6.4 Public Affairs Records
- 6.5 Public Customer Service Records
- 6.6 (Rescinded)

Figure 13. NARA GRS Record Series



JS Mission Records. Unique to the JS and CCMDs

0000 Series Bucket — Joint Staff (JS) Top 4 and Combatant Command (CCMD) Headquarters (HQs) Records
0100 Series Bucket — Organization, Manpower, Committee, and Board Records
0200 Series Bucket — Personnel and Payroll
0300 Series Bucket — Intelligence and Security
0400 Series Bucket — Military Justice, Legal, Protocol, and Public Affairs
0500 Series Bucket — C2, Operations, Planning, and Exercises
0600 Series Bucket — Logistics, Acquisitions, Supply, Services, Budget, and Safety
0700 Series Bucket — Communications, Cryptology, and Electronics Policies, Procedures, and Reports
0800 Series Bucket — International
0900 Series Bucket — General Administration and Management
1000 Series Bucket — Information Technology (IT) Procurement, Planning, Operations, and Management
1100 Series Bucket — Medical
1200 Series Bucket — Electronically Stored Information (ESI) Systems
1300 Series Bucket — Academic Affairs (National Defense University)

Figure 14. JS Mission Records

d. The NARA GRS and the JSMRS **only** apply to all media neutral records, which includes e-mails. It does not apply to non-record materials such as personal papers, blank forms, publications, etc.

e. RCs will group and arrange records based on their functions, use, and need for accessibility, and file them:

(1) Numerically. Files are identified and retrieved by a number (e.g., SSN, purchase order).

(2) Chronologically. Files are identified and retrieved by a date.

(3) Alphabetically. Files are identified and retrieved by a name or location.

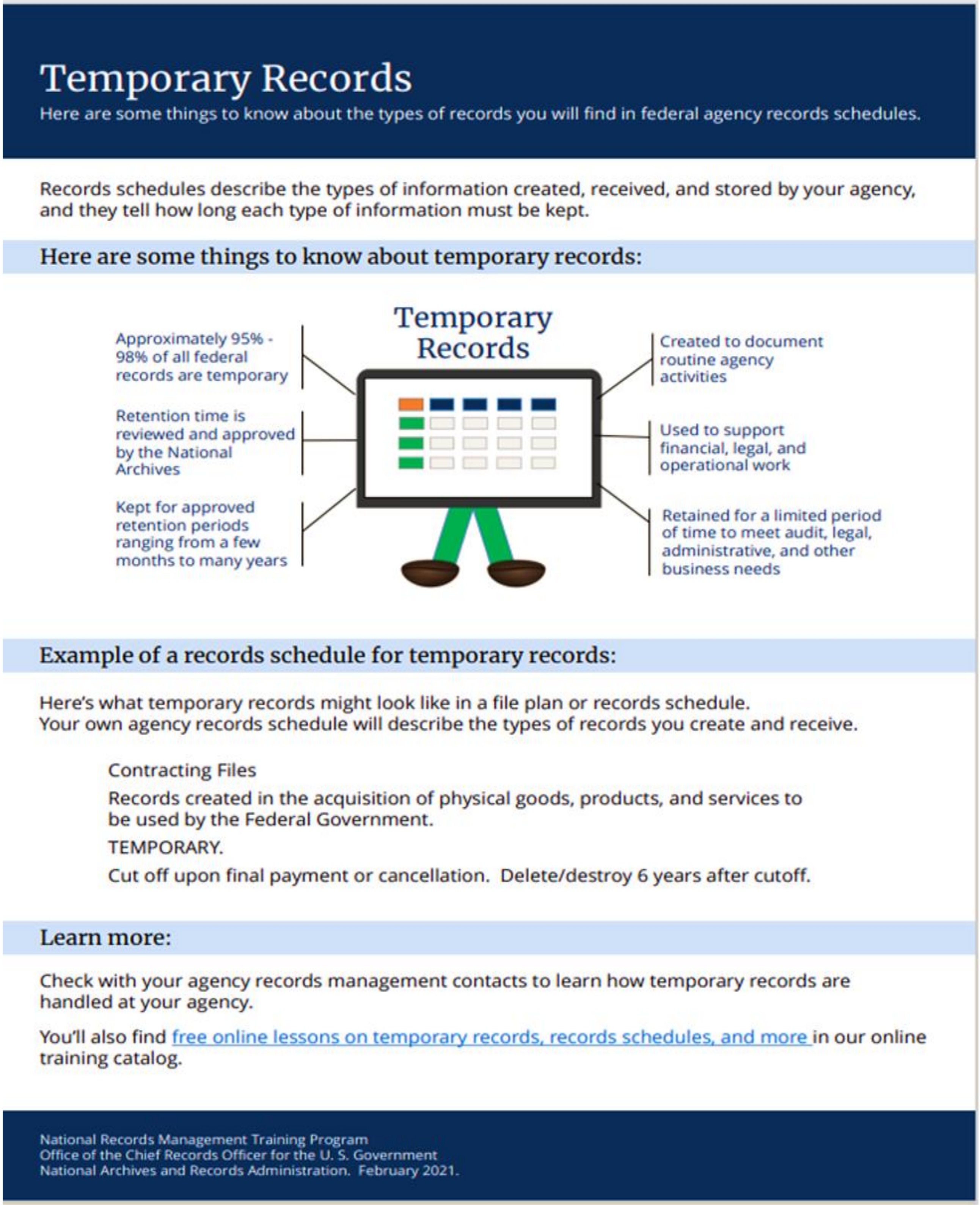
(4) Subject. Files are identified and retrieved by their content

(5) Alpha Numeric. Files are identified and retrieved by a combination of letters and numbers.

f. RCs will work with RLs and RO to apply appropriate file numbers and disposition instructions.

g. Once the disposition is set to a file, there will be a “Cut-Off” timeline where the file will be considered no longer needed for day-to-day activities. RCs will be responsible for physically or electronically moving the record to “inactive” status by placing the file in another location which will prevent filing errors.

h. To further assist in determining records, the following five pages display CIO’s “TIP SHEETs” (2021) that contains information regarding managing permanent and temporary records/schedules and managing non-records and personal file material. **They can be found on: Tip Sheets: Temporary Records, Permanent Records, Non-records, and Personal Files (archives.gov)**.



Temporary Records

Here are some things to know about the types of records you will find in federal agency records schedules.

Records schedules describe the types of information created, received, and stored by your agency, and they tell how long each type of information must be kept.

Here are some things to know about temporary records:

Temporary Records

Approximately 95% - 98% of all federal records are temporary

Retention time is reviewed and approved by the National Archives

Kept for approved retention periods ranging from a few months to many years

Created to document routine agency activities

Used to support financial, legal, and operational work

Retained for a limited period of time to meet audit, legal, administrative, and other business needs

Example of a records schedule for temporary records:

Here's what temporary records might look like in a file plan or records schedule.
Your own agency records schedule will describe the types of records you create and receive.

Contracting Files

Records created in the acquisition of physical goods, products, and services to be used by the Federal Government.

TEMPORARY.

Cut off upon final payment or cancellation. Delete/destroy 6 years after cutoff.

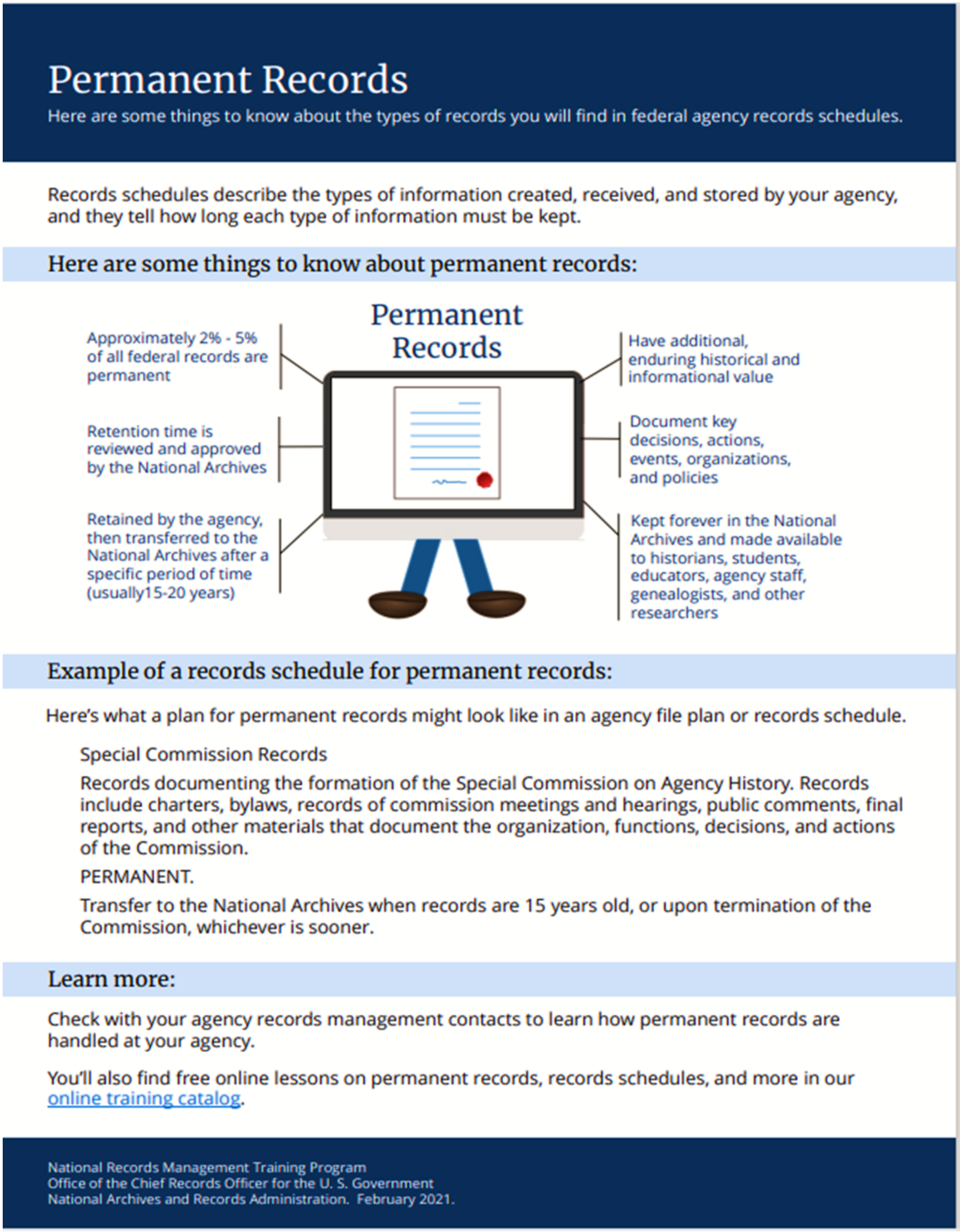
Learn more:

Check with your agency records management contacts to learn how temporary records are handled at your agency.

You'll also find free online lessons on temporary records, records schedules, and more in our online training catalog.

National Records Management Training Program
Office of the Chief Records Officer for the U. S. Government
National Archives and Records Administration. February 2021.

Figure 15. Temporary Records Tip Sheet



Permanent Records

Here are some things to know about the types of records you will find in federal agency records schedules.

Records schedules describe the types of information created, received, and stored by your agency, and they tell how long each type of information must be kept.

Here are some things to know about permanent records:

Permanent Records

Approximately 2% - 5% of all federal records are permanent

Retention time is reviewed and approved by the National Archives

Retained by the agency, then transferred to the National Archives after a specific period of time (usually15-20 years)

Have additional, enduring historical and informational value

Document key decisions, actions, events, organizations, and policies

Kept forever in the National Archives and made available to historians, students, educators, agency staff, genealogists, and other researchers

Example of a records schedule for permanent records:

Here's what a plan for permanent records might look like in an agency file plan or records schedule.

Special Commission Records

Records documenting the formation of the Special Commission on Agency History. Records include charters, bylaws, records of commission meetings and hearings, public comments, final reports, and other materials that document the organization, functions, decisions, and actions of the Commission.

PERMANENT.

Transfer to the National Archives when records are 15 years old, or upon termination of the Commission, whichever is sooner.

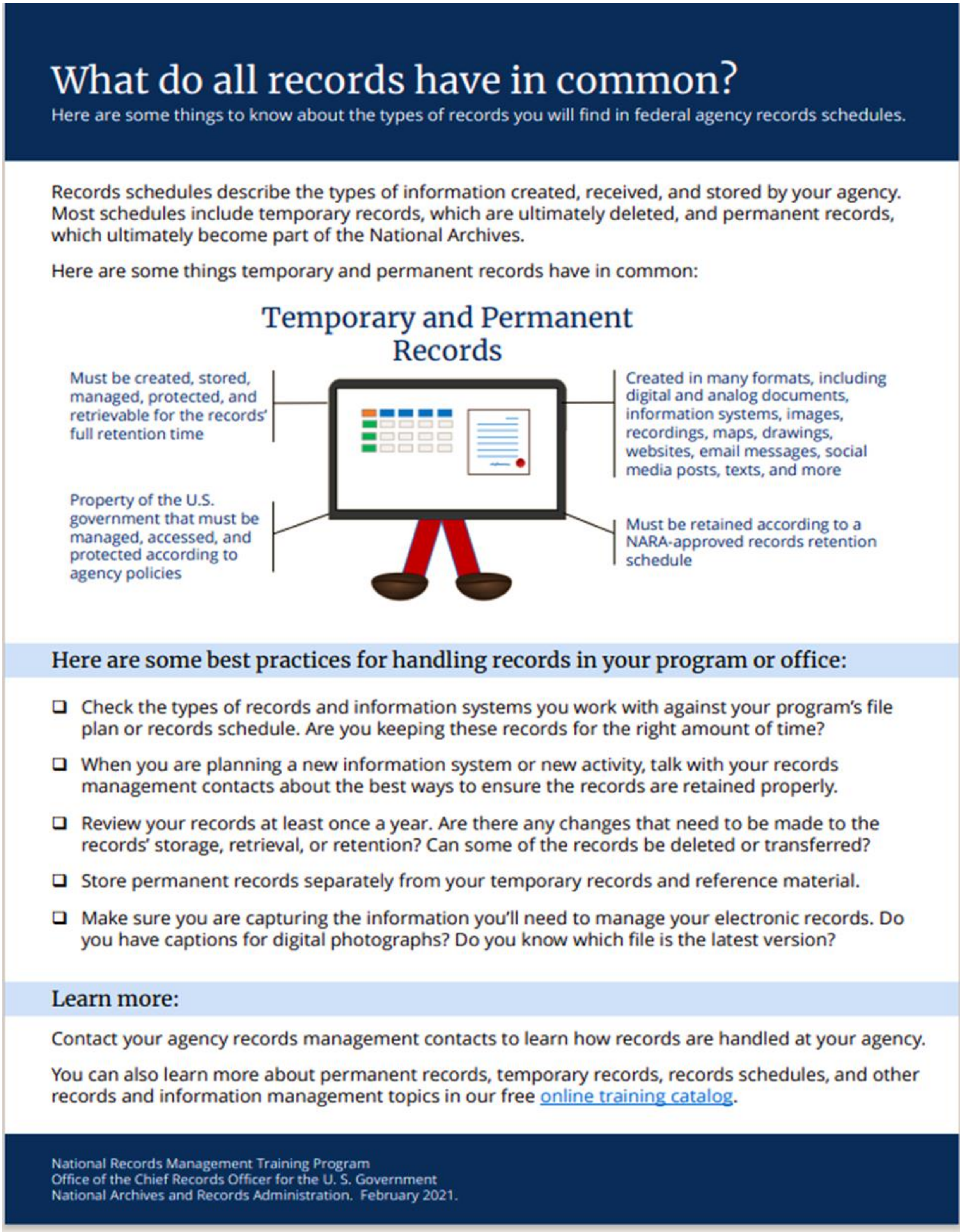
Learn more:

Check with your agency records management contacts to learn how permanent records are handled at your agency.

You'll also find free online lessons on permanent records, records schedules, and more in our online training catalog.

National Records Management Training Program
Office of the Chief Records Officer for the U. S. Government
National Archives and Records Administration. February 2021.

Figure 16. Permanent Records Tip Sheet



What do all records have in common?

Here are some things to know about the types of records you will find in federal agency records schedules.

Records schedules describe the types of information created, received, and stored by your agency. Most schedules include temporary records, which are ultimately deleted, and permanent records, which ultimately become part of the National Archives.

Here are some things temporary and permanent records have in common:

Temporary and Permanent Records

Must be created, stored, managed, protected, and retrievable for the records' full retention time

Property of the U.S. government that must be managed, accessed, and protected according to agency policies

Created in many formats, including digital and analog documents, information systems, images, recordings, maps, drawings, websites, email messages, social media posts, texts, and more

Must be retained according to a NARA-approved records retention schedule

Here are some best practices for handling records in your program or office:

- □ Check the types of records and information systems you work with against your program's file plan or records schedule. Are you keeping these records for the right amount of time?
- □ When you are planning a new information system or new activity, talk with your records management contacts about the best ways to ensure the records are retained properly.
- □ Review your records at least once a year. Are there any changes that need to be made to the records' storage, retrieval, or retention? Can some of the records be deleted or transferred?
- □ Store permanent records separately from your temporary records and reference material.
- □ Make sure you are capturing the information you'll need to manage your electronic records. Do you have captions for digital photographs? Do you know which file is the latest version?

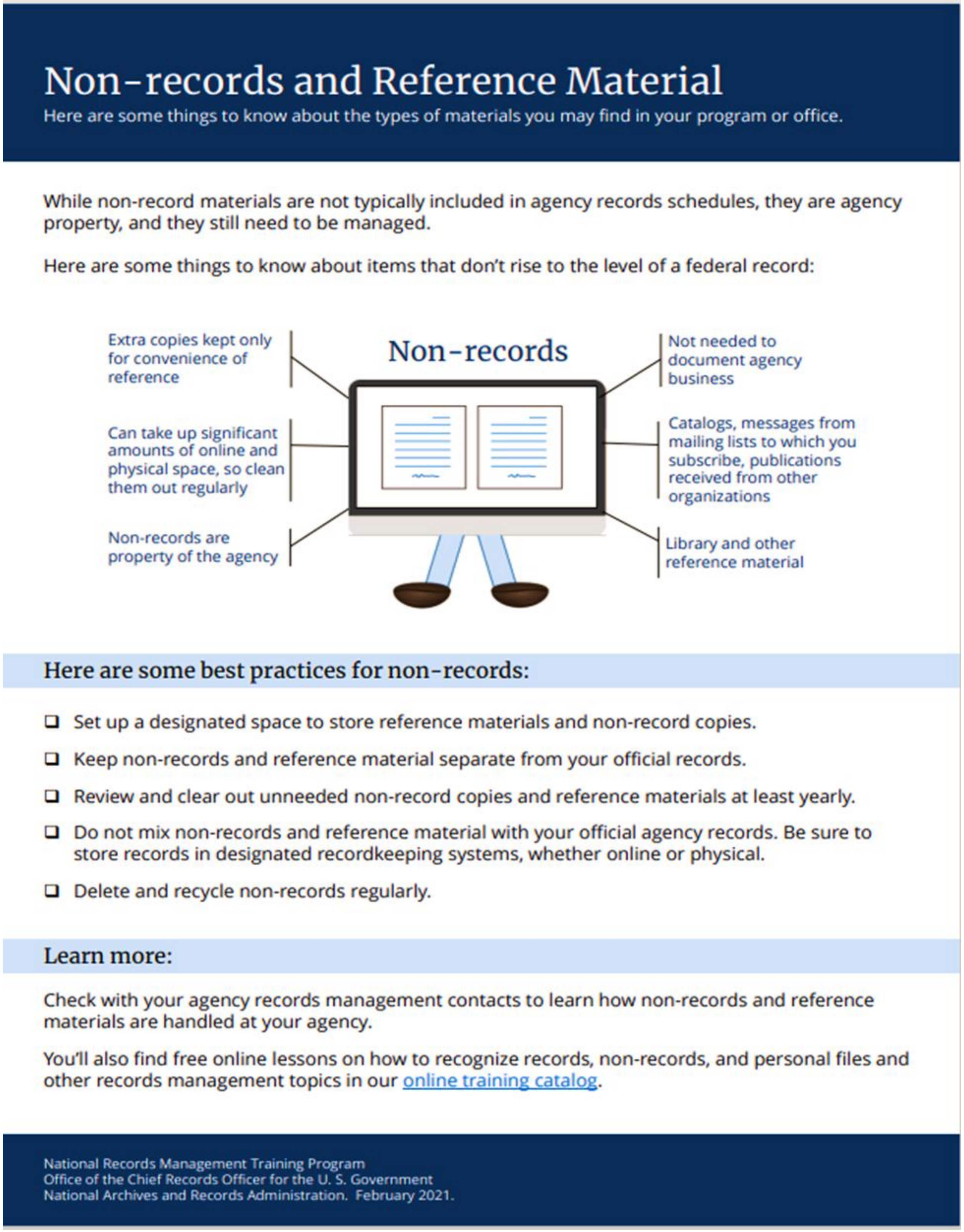
Learn more:

Contact your agency records management contacts to learn how records are handled at your agency.

You can also learn more about permanent records, temporary records, records schedules, and other records and information management topics in our free online training catalog.

National Records Management Training Program
Office of the Chief Records Officer for the U. S. Government
National Archives and Records Administration. February 2021.

Figure 17. What Do All Records Have in Common Tip Sheet



Non-records and Reference Material

Here are some things to know about the types of materials you may find in your program or office.

While non-record materials are not typically included in agency records schedules, they are agency property, and they still need to be managed.

Here are some things to know about items that don't rise to the level of a federal record:

Non-records

Extra copies kept only for convenience of reference

Can take up significant amounts of online and physical space, so clean them out regularly

Non-records are property of the agency

Not needed to document agency business

Catalogs, messages from mailing lists to which you subscribe, publications received from other organizations

Library and other reference material

Here are some best practices for non-records:

- ❑ Set up a designated space to store reference materials and non-record copies.
- ❑ Keep non-records and reference material separate from your official records.
- ❑ Review and clear out unneeded non-record copies and reference materials at least yearly.
- ❑ Do not mix non-records and reference material with your official agency records. Be sure to store records in designated recordkeeping systems, whether online or physical.
- ❑ Delete and recycle non-records regularly.

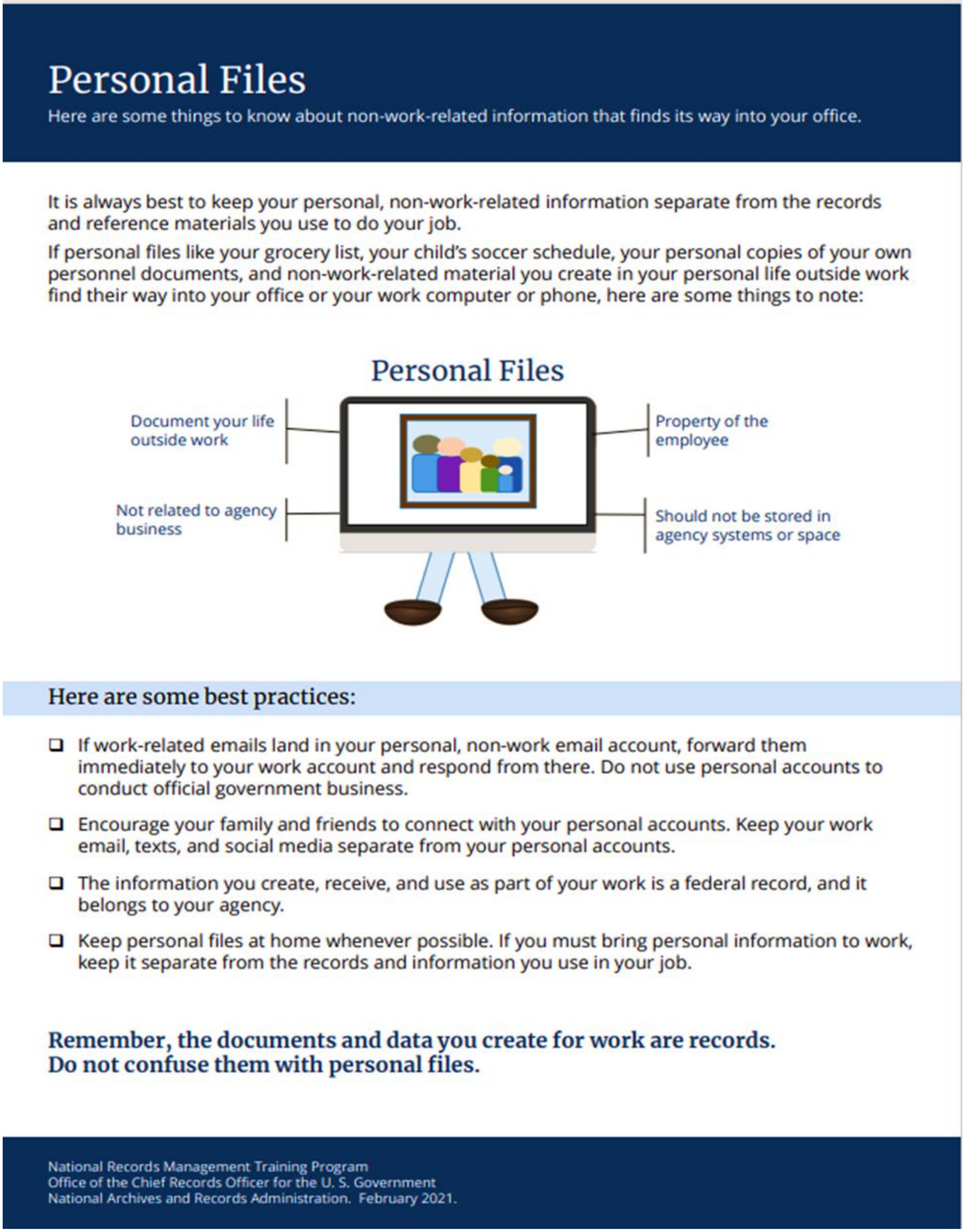
Learn more:

Check with your agency records management contacts to learn how non-records and reference materials are handled at your agency.

You'll also find free online lessons on how to recognize records, non-records, and personal files and other records management topics in our online training catalog.

National Records Management Training Program
Office of the Chief Records Officer for the U. S. Government
National Archives and Records Administration. February 2021.

Figure 18. Non-Records and Reference Material Tip Sheet



Personal Files

Here are some things to know about non-work-related information that finds its way into your office.

It is always best to keep your personal, non-work-related information separate from the records and reference materials you use to do your job.

If personal files like your grocery list, your child's soccer schedule, your personal copies of your own personnel documents, and non-work-related material you create in your personal life outside work find their way into your office or your work computer or phone, here are some things to note:

Personal Files

Document your life outside work

Not related to agency business

Property of the employee

Should not be stored in agency systems or space

Here are some best practices:

- ❑ If work-related emails land in your personal, non-work email account, forward them immediately to your work account and respond from there. Do not use personal accounts to conduct official government business.
- ❑ Encourage your family and friends to connect with your personal accounts. Keep your work email, texts, and social media separate from your personal accounts.
- ❑ The information you create, receive, and use as part of your work is a federal record, and it belongs to your agency.
- ❑ Keep personal files at home whenever possible. If you must bring personal information to work, keep it separate from the records and information you use in your job.

Remember, the documents and data you create for work are records.
Do not confuse them with personal files.

National Records Management Training Program
Office of the Chief Records Officer for the U. S. Government
National Archives and Records Administration. February 2021.

Figure 19. Personal Files Tip Sheet

ENCLOSURE F

ELECTRONIC RECORDS MANAGEMENT

1. Purpose. This enclosure provides guidance on integrating electronic records management and preservation considerations into the design, development, enhancement, and implementation of electronic information systems.

a. Control requirements. Record managers must ensure within their organizations that the following controls are integrated into electronic information systems. RMs will need to work with their designated IT and KM assets to ensure these control requirements are incorporated into organization electronic records management designs.

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

b. Protection of Electronic Records

(1) RCs and RLs will work alongside IT assets to ensure records retain protection regardless of classification. There is zero tolerance for mishandling of records. As such, to fully protect records, RCs and RLs must:

(a) Work with ROs to ensure all records meet current GRS standards, and ensure the EIS will support the records throughout the records lifecycle.

(b) Work with IT and KM assets to identify and integrate innovative tools, hardware, and software upgrades successfully to retain the functionality and integrity of records.

(c) When RCs are assisting organizations with organizing records and conducting inventories, ensure:

1. Records are properly declared by ensuring all records have been assigned individual identifiers.

2. Records are captured properly and made retrievable.

3. Records are organized IAW reference (k).

4. Records are protected from unauthorized access, modification, or deletion and audit trails are in place to track the use of the record.

5. Records have in place appropriate access for users.

6. Records in EIS are usable and retrievable for as long they are needed to support organization functions and meet NARA-approved disposition.

NOTE: RCs will use JS Form 30v3 (2023) to report all findings and will retain internally until an annual SAV or audit is scheduled.

(d) Digitization of Temporary Records. IAW 1236 Subpart D of reference (tt), digitizing temporary records must:

1. Capture of all information contained in the original source records.

2. Include all pages or parts from the original source records.

3. Ensure the digitized document can be used for all purposes throughout the organizations.

4. Be digitized IAW rules and regulations to fully ensure protection.

5. Ensure users within the organization can locate, access, and use the digitized versions for the record's entire retention period.

6. Ensure records are backed up regular and backups do not impede the usability or integrity of the records.

(e) Digitizing Permanent Records

1. IAW reference (uu), digitizing permanent records ensures organizations can use the digital versions for the same purposes as its original source record.

a. IAW part 1236.42, Subpart E of reference (b) and reference (vv), ROs will advise digitization of permanent records by using reference (vv).

b. RCs and RLs will advise directorates on the relationships tied to source records and retain these relationships when digitized by:

(1) Capturing metadata requirements.

(2) Organizing the folder structure of the file system.

(3) Using file formats that allow for multi-page files, such as PDF or TIFF.

(4) Through a combination of all these approaches.

NOTE: 1236 does not require optical character recognition (OCR) to be performed during digitization. However, it is a JS requirement to OCR any digitized document to ensure its searchability and rapid retrievability as it benefits the needs of the organization.

c. Web-based Records Management Applications. A records management application (RMA) collects, organizes, and categorizes electronic records in their original file form and in a NARA-acceptable transfer format; it also manages the metadata regarding scanned hard copy records.

(1) SharePoint will provide users within the JS and CCMDs the ability to manage records via lists and/or libraries; with document repositories that allow the creation or receipt of records and information along with the capability to distribute, use, and store records that support current business and mission practices.

(2) To meet reference (i) requirement, RCs will work with RLs, who will work with the ROs and provide guidance and assistance to all users in creating electronic filing systems on SharePoint sites and transfer all record materials from share drives onto the designated areas within those sites.

NOTE: Personal files will not be stored on any SharePoint site.

(3) For sites or portions of a site or web records requiring dispositioning, ROs will contact NARA for guidance and work with RLs in developing procedures for preservation.

d. Management of Social Media and Social Media Platforms

(1) The integration of social media is an integral element of DoD strategies as it pertains to electronic information management. Therefore, it is imperative to properly manage social media IAW the rules and regulations that are current.

(2) The JS and CCMDs will use and manage social media and social media platforms IAW references (i), (j), (bbb), (ccc), (ddd), and (eee). For further information, visit <https://www.defense.gov/social-media-policy/>.

e. Transferring Permanent Electronic Records to NARA. IAW part 1232 of reference (b), Chapters 31 and 33 of reference (c), and reference (k):

(1) Permanent electronic records will be transferred to NARA in an acceptable medium. Prior to transfer, permanent electronic records must be dispositioned. Each directorate will be responsible for maintaining the integrity of their records while in transition.

(2) Temporary Retention of Copy. Each directorate will retain a copy of any permanent electronic records and will destroy the copy once a formal notification from NARA is received stating that legal responsibility has been assumed. Part 1235 of reference (b) provides the requirements governing the selection of electronic records storage. Media types approved for transfer are:

(a) CD-ROM.

(b) DVD.

(c) Reel magnetic tape.

(d) Removable hard drives.

(3) Formats. The following list provides information regarding approved formats.

(a) Components may not transfer to NARA electronic records that are in a format dependent on specific hardware or software.

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

(c) Some of the formats currently acceptable to NARA are: data files and databases; e-mail; plain American Standard Code for Information Interchange files, with or without Standard Generalized Markup Language tags; tagged image file format; .pdf; digital spatial data files; digital photos; and web records (hypertext markup language or extensible markup language).

(INTENTIONALLY BLANK)

ENCLOSURE G

RECORDS MAINTENANCE AND DISPOSITION

1. Purpose. This enclosure provides procedures for ensuring records are readily available for business purposes, are protected, and properly maintained during their retention period, and are destroyed or transferred to NARA according to the Records Schedule in Volume II of this manual.

2. File Labeling. Proper labeling is essential for accurate filing and for retrieval, retention, and disposition of records regardless of the form or format of the record or the container in which it is kept.

a. All Records. Upon approval, FCs will place approved file plan under 0900-02-H "Records Management."

b. Audiovisual Records. Labels will also identify:

(1) For still photographs, the date, location, names of people, and even the photograph documents. To avoid damage, the label will be attached to the container not to the photo.

(2) For motion picture films, videotapes, and audiotapes, the date and subject of the record and any other pertinent identification not contained within the record itself when viewed or listened to.

c. Electronic Records

(1) External Electronic Labels. Labels on electronic record containers will also identify:

(a) The hardware and software that will read the record.

(b) The originating office symbol.

(c) The subject of the record.

(d) The begin and end dates of the information contained therein.

(2) Internal Electronic Labels

(a) Labels within electronic records, commonly known as "file names" (or folder or directory names), are those labels within CD-ROMs, internal hard drives, local networks, and other electronic records/EIS that can only be entered and read by machine.

(b) Internal electronic labeling does not lend itself to the same level of detail as external labeling. However, file labeling/naming conventions, at a minimum, will be standardized within each office of record in a way that is readily understandable throughout that office. Subdirectory labels might contain the major functional series numbers and names that characterize the activities of the office. Folder labels might identify the names and numbers of sub-functional groups. Subordinate folder labels and electronic file labels should be sufficiently descriptive of the information within them that they need not be opened to determine the nature of the contents.

3. Files Cutoff, Retention, and Disposition. JS and CCMD files will be filtered by the record's modified by date, or the date the record was created. Disposed of records is IAW current approved records retention and disposition schedules.

a. Cutoff. Files cutoff is the process of closing out files at regular intervals, placing them in inactive status, and establishing the start of the retention period. Files cutoff is essential to controlling the accumulation of records and assuring their proper retention and disposition.

(1) Where the instructions in Volume II do not specify, JS and CCMD files will be cutoff at the end of the calendar year (CY).

(2) Files maintained on a CY basis will be cutoff on 31 December of each year and placed in the inactive CY files area, and new CY files established.

(3) If the CCMDs have an ERM, filter records by the modified by date or by the date the records were created, and disposed of them on IAW reference (k).

(4) Files cutoff on the occurrence of an event will be cutoff upon occurrence of that event. For purposes of establishing the retention period, the cutoff date, and date of relocation to the inactive files area, will be the end of the CY or FY, as applicable.

(5) Files with a retention period of less than 1 year will be cutoff on a daily, weekly, or monthly basis to facilitate timely disposal. For example, large accumulations of records that are to be destroyed after 6 months could be cutoff at the end of each month, a new file started, and the cutoff file disposed of after 6 months.

(6) Files having no retention period are scheduled to be disposed of when no longer needed, when superseded or obsolete, or on occurrence of an event. For these types of files, the Records Schedule may read: “Destroy when superseded or rescinded” or “Destroy on receipt of next inspection report.” These types of files, along with all reference material, will be reviewed on an annual basis, and all files, records, and materials that are not current or are no longer needed will be destroyed.

(INTENTIONALLY BLANK)

ENCLOSURE H

RECORDS RETIREMENT, TRANSFER, AND RECALL

1. Retirement and Transfer

a. Documentation

(1) All Records

(a) SF 135. Records to be retired or transferred will be identified on SF 135. The SF 135 serves as a packing list, as a means of controlling the location and disposition of files, and as a receipt for the transaction. To meet SF 135 requirements, please follow component guidelines.

(b) SF 258. Permanent records will be transferred to NARA on SF 258, "Agreement to Transfer Records to the National Archives of the United States," with the records listed on attached SF 135s.

(c) Digitization of records no longer requires ISFs, and NARA requires all paper copies to be digitized by CY 2024. Should agencies be required to have an ISF, then third party solutions must be explored and an ISF must be created and managed to manage records. It is recommended before seeking ISF support to reach out to the JSRO for JS inquiries and CCMD CRMs for CCMD inquiries.

(2) Electronic Records and EIS

(a) NARA no longer requires additional documentation for the transfer of electronic records and EIS, unless the information provided when the records were appraised is insufficient for NARA purposes. In this case, NARA will contact the controlling JS or CCMD RM to obtain the additional information, and may require completion of NA Forms 14097 or 14028.

(b) NARA provides current information on acceptable transfer format and media in reference (fff).

b. Shipping. Records will be shipped in standard-sized record containers, each holding one cubic-foot. These are currently available only from the General Services Administration (GSA) Federal Supply Service at <www.gsaadvantage.gov>. Special containers for oversized materials may also be obtained from GSA. Prior written approval from the receiving agency is required for shipments in any other type of container.

2. Recall and Return

a. Only the controlling JSRO or CCMD CRMs, and those individuals designated by their respective RLs and RCs as set forth in subparagraph 2.b., are authorized to recall records. Requests will be made using Optional Form 11, "Reference Request – Federal Records Centers." A separate form will be completed for each record requested using the information provided on the returned SF 135 for the requested record.

b. Requests for reference services on records that have been transferred to NARA will be accomplished only through the controlling JS or CC RM.

ENCLOSURE I

REFERENCES

a. CJCSI 5760.01B, 23 April 2023, “Records and Information Management Policy

b. Title 36, CFR, CH XII, Sub-Chapter B, Amended 29 December 2023, “Parks, Forest, and Public Property”, “National Archives and Records Administration”, “Records Management”,

PRT 1222, “Creation and Maintenance of Federal Records”
PRT 1223, “Managing Vital Records”
PRT 1230, “Unlawful or Accidental Removal, Defacing, Alteration or Destruction of Records”
PRT 1232, “Transfer of Records to Records Storage Facilities”
PRT 1235, “Transfer of Records to the National Archives of the United States
PRT 1236, “Electronic Records Management”

c. Title 44, U.S. Code, amended 2 January 2024,

Chapter 21, 26 November 2014, “National Archives and Records Administration”
Chapter 29, 01 January 202, “Records Management by the Archivist of the United States and by the Administrator of General Services”
Chapter 31, 21 October 1976, “Records Management by Federal Agencies”
Chapter 33, 26 November 2014, “Disposal of Records”
Chapter 36, 23 December 2022, “Management and Promotion of Electronic Government Services”

d. CJCSI 5721.01G, 01 July 2022, “Organizational Messaging Service”

e. NARA M-19-21, 28 June 2019, “Transition to Electronic Records”

f. NARA M-23-07, 23 December 2022, “Update to Transition to Electronic Records”

g. OMB Circular A-130, 28 July 2016, “Managing Information as a Strategic Resource”

h. DoDM 8180.01, 4 August 2023, “Information Technology Planning for Electronic Records Management”

i. DoDI 8170.01CH1, 24 August 2021, “Online Information Management and Electronic Messaging”

j. “DoD Records Strategy,” 23 May 2023

k. CJCSM 5760.01A, 13 July 2012, “Joint Staff and Combatant Command Records and Information Management Manual VOL II-Disposition Schedule”

l. DoD memo, 27 September 2023, “Use of Text Messaging on Mobile Devices & Records Management of Electronic Messages”

m. Department of Interior (DoI), 8 September 2022, “Managing Electronic Email” (brochure)

n. NARA Bulletin 2013-02, 5 January 2023, “Expanding Role-Base Approach (Capstone) for Electronic Messages”

o. NARA M-12-18, 24 August 2012, “Managing Email Records in Compliance with Managing Government Records Directive”

p. NARA Bulleting 2023-04, 23 October 2023, “Managing Records Created on Collaboration Platforms”

q. NARA Bulleting 2014-02, October 2013, “Managing Social Media Records”

r. “NARA Essential Records Guide,” August 2016

s. NARA’s Records Management Key Terms and Acronyms List

t. CJCSM 3105.01A, 12 October 2021, “Joint Risk Analysis”

u. JSI 7100.01G, 28 February 2022, “Joint Staff Risk Management and Internal Control Program”

v. “DoD Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs,” 9 January 2017

w. Title 18, U.S. Code, Part 1 Chapter 31 Section 641, 3 January 2012 “Public Money, Property or Records,”

x. Title 46, CFR, amended 1 January 2024, Chapter IV, Sub-Chapter A, PRT 503, Subpart G, Section 503.59, “Safeguarding Classified Information”

y. DoDM 5200.01 VOL I, 28 July 2022, “Information Security Program: Overview, Classification and Declassification”

z. CJCSI 3231.01C, 15 December 202, “Safeguarding Nuclear Command and Control Extremely Sensitive Information.”

aa. DoDM 5200.01 VOL III, 28 July 2020, “DoD Information Security Program-Protection of Classified Information”

bb. NATO Instruction 1-27, 18 August 2022, “Control of NATO Classified Documents”

cc. DoDI 5015.02, 17 August 2017, “DoD Records Management Program” CHG1

dd. ISOO 2023-002, 23 June 2023, “Handling National (NATO) Information Identified During Automatic Declassification Processing”

ee. Title 32, CFR, amended 4 January 2024, Subtitle A, Chapter I, Sub-Chapter D, PRT 117, Section 117.19, “International Security Requirement”

ff. DoD Administrative Instruction (AI) 15 CH2, 17 November 2020, “OSD Records and Information Management Program”

gg. CJCSI 5714, 18 April 2012, “Policy for the Release of Joint Information”

hh. NARA M-12-18, 24 August 2012, “Managing Government Records”

ii. NARA M-14-16, 15 September 2014, “Guide to Managing Email”

jj. NARA Bulletin 2013-02, 29 August 2013 “Capstone Approach”

ll. Presidential Policy Directive (PPD) 40, 15 July 2016, “National Continuity Policy”

mm. DoD CIO memo, 10 August 2022, “Use of Non-Government Owned Mobile Devices”

nn. International Organization for Standardization (ISO) 15489:1:2016, “Information and Documentation for Records Management”

oo. ISO/TS 16175 2:2020, “Information and Documentation-Processes and functional requirements for software” pp. NARA, January 2005, “Guidance on Managing Web Records”

qq. OMB M 23-10, 8 February 2023, “The Registration and Use of .gov Domains in the Federal Government”

rr. DoDD 8000.01 CH1, 27 July 2017 “Management of the Department of Defense Information Enterprise (DoD IE)”

ss. DoDD 5144.02 CH2, 30 November 2022, “DoD Chief Information Officer (DoD CIO)”

tt. Title 36, CFR, CH XII Subchapter D, amended 3 April 2024, “Digitizing temporary Records.”

uu. Federal Register VOL 88 No. 28410, 5 June 2023, “Digitizing Permanent Records”

vv. Federal Agencies Digital Guidelines Initiative (FADGI), 10 May 2022

ww. NARA Bulleting 2015-04 Appendix B, 15 September 2015, “Metadata Guidance for the Transfer of Permanent Electronic Records”

xx. Title 5, U.S. Code, 8 December 2023, “Government Organizations and Employees”

yy. DoD 5230.30M, 8 February 2022, “DoD Mandatory Declassification Review (MDR) Program”

zz. E.O. 13526, 29 December 2009, “*Classified National Security*”

aaa. NARA Bulletin 2014-04, 31 January 2014, “NARA Format Guidance for the Transfer of Permanent Records”

bbb. DoDI 5230.09, 25 January 2019, “Clearance of DoD Information for Public Release”

ccc. DoDI 5230.29 CH2, 8 February 2022, “Security and Policy Review of DoD Information for Public Release.”

ddd. DoDI 5400.17 CH1, 24 January 2023, “Official Use of Social Media for Public Affairs Purposes” eee. Hatch Act Guidance on Social Media, February 2018

fff. “Electronic Records Management Guidance” <http://www. archives.gov/ records-mgmt/initiatives/ erm-guidance.html>

(INTENTIONALLY BLANK)

GLOSSARY

PART I – ABBREVIATIONS AND ACRONYMS

Items marked with an asterisk (*) *have definitions in PART II*

CCMD	Combatant Command
CIO	Chief Information Officer
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJCSM	Chairman of the Joint Chiefs of Staff Manual
COO	Continuity of Operations
COOP	Continuity of Operation Program
CRM	Command Record Manager
CUI	Controlled Unclassified Information
DISA	Defense Information Systems Agency
DoD	Department of Defense
EIS	Enterprise Information System
ESI	Extremely Sensitive Information
eRecord	electronic record
ERM	Electronic Records Management
FADGI	Federal Agencies Digital Guidelines Initiative
GRS	General Records Schedule
IAW	in accordance with
IMD	Information Management Division
ISF	Inactive Storage Facility
JS	Joint Staff
JSCRO	Joint Staff Chief Records Officer
JSMRS	Joint Staff Mission Records Schedule
JRAM	Joint Risk Analysis Methodologies
MFR	memorandum for record
NARA	National Archives and Records Administration
NC2	Nuclear Command and Control
NC2-ESI	Nuclear Command and Control-Extremely Sensitive Information
OSD	Office of the Secretary of Defense

PPD	Presidential Policy Directive
RC	Record Custodian
RL	Record Liaison
RO	Record Officer
RoIO	Release of Information Officer
RRB	Records and Research Branch
MIL STD	Military Standard

PART II – DEFINITIONS

Active records – Records that continue to be used with sufficient frequency to justify keeping them in the office of creation, current records.

Continuity of Operations Program – An effort within individual agencies to ensure they can continue to perform their Mission Essential Functions and Primary Mission Essential Functions during a wide range of emergencies, including localized acts of nature, accidents, and technological or attack related emergencies. Also called COOP.

Continuity of Operations Plan – A documented plan that details how individual agencies can continue to perform its Mission Essential Functions, Primary Mission Essential Functions, and any National Essential Functions during emergencies, including acts of nature, accidents, technological and attack-related emergencies during a wide range of events that impact normal operations. Covers devolution and reconstitution with appropriate delegations of authority for leadership and staff to increase survivability and perform the essential functions. Required by Presidential Policy Directive 40. Other plans with names like Emergency Plan, Disaster Plan, Emergency Response Plan, Disaster Preparedness Plan, Contingency Plan, etc., are generally supportive plans and do not replace the COOP Plan.

drivers of risk – Factors that act either to increase or decrease the probability or consequence of risks arising from various sources.

electronic records (e-Records) – e-Records are records that are stored in a form that only a computer can process.

Essential Records – Records an agency needs to meet operational responsibilities under national security emergencies or other emergency conditions (emergency operating records) or to protect the legal and financial rights of the Government and those affected by Government activities (legal and financial rights records).

Essential Records Inventory – A list which identifies the records that have been designated as essential. It includes other identifying information such as where the records are located, who is responsible for them, when they are cycled, format, and similar information useful for the agency to effectively manage the records.

Essential Records Management – Essential records management is the protection and the ready availability of the essential records, information systems, data management software, and supported equipment needed support mission essential functions.

File Plan – A plan designating the physical location(s) at which an agency's files are to be maintained, the specific types of files to be maintained there, and the organizational element(s) having custodial responsibility. Also: A document containing the identifying number, title or description, and disposition authority of files held in an office.

Filing System – A set of policies and procedures for organizing and identifying files or documents to speed their retrieval, use, and disposition.

Frozen Records – Temporary records held for litigation, investigation, or audit purposes. Frozen records can be destroyed only after completion of litigation, audit, or investigation and notification from the appropriate authority.

General Records Schedules – General Records Schedules (GRS) are issued by the Archivist of the United States under the authority of title 44, U.S. Code, section 3303a (d) to provide disposition authority for records common to several or all Federal agencies. The GRS cover records documenting administrative functions rather than program functions. Agencies must apply the GRS to the greatest extent possible.

hazard – Security, environmental, demographic, political, technical, or social conditions with potential to cause harm.

inactive records – Records that are no longer used in the day-to-day course of business, but that may be preserved and occasionally used for legal, historical, or operational purposes.

information system – An organized set of procedures and techniques designed to store, retrieve, manipulate, analyze, and display information. If automated, information system also includes hardware and software.

inventory – A survey of agency records and non-record materials conducted primarily to develop records schedules and to identify various records (permanent, temporary, essential, official records or non-record materials).

Joint Risk Analysis Methodology – A risk framework providing a consistent, standardized way to appraise, manage, and communicate risk. Also called JRAM.

Joint Staff Mission Record Schedule – Joint Staff Mission Record Schedule provides mandatory disposition instructions to maintain JS operational records as well as provides management steps when they are no longer needed for current business. Also called JSMRS.

lifecycle – The management concept that records pass through three stages: creation, maintenance and use, and disposition.

non-record materials – Non-record materials are materials excluded from the legal definition of records. Non-record materials include unofficial copies of documents kept only for convenience or reference.

Presidential Policy Directive 40, National Continuity Policy – Directs the Federal Emergency Management Agency (FEMA) to coordinate the implementation, execution, and assessment of continuity activities among executive departments and agencies. Signed by the President on 15 July 2016, replaced NSPD-51/HSPD-20 and the NCPIP. PPD 40 created an Inter-agency Reconstitution Working Group, which includes the Department of Homeland Security/FEMA, Office of Personnel Management, General Services Administration, and National Archives and Records Administration. Parts of PPD 40 are classified.

permanent records – Permanent records are records that are appraised as having sufficient historical value to warrant preservation.

personal data – information (typically held electronically) about a particular person, especially sensitive information regarding their finances, medical history, etc.

risk – Risk is the probability and consequence of an event causing harm to something valued, classified within one of four risk levels (low, moderate, significant, or high).

permanent record – Record appraised by the National Archives and Records Administration as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time it is needed for administrative, legal, or fiscal purposes.

record – Record Includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the U.S. Government or because of the informational value of data in them.

record series – A group of records arranged according to a filing system or kept together because they relate to a particular subject or function, result from the same activity, document a specific type of transaction, exist in the same media format, or have some other type of relationship.

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

regulation – Rules and guidelines that are created and enforced by government agencies or other regulatory bodies. These regulations are designed to ensure compliance with statutory laws.

Risk Acceptability/Tolerance Matrix – Represents your agency's tolerance level for acceptable and unacceptable risks.

Risk Appraisal – A component of the Joint Risk Analysis Methodologies, during which knowledge and understanding is generated.

Risk Assessment – Second pillar in the Joint Risk Analysis Methodologies, during which sources of harm are linked with likely consequences and expected probability.

Risk Communication – A component of the Joint Risk Analysis Methodologies encompassing the exchange of risk perspectives across processes and among leadership.

Risk Evaluation – Sub-set of Risk Judgment, during which a decision maker determines the acceptability of a risk.

Risk Management – Risk management is the process of identifying (through risk assessments) and evaluating (through risk analysis) risks to records and the development of strategies to manage the risk. Risk management is a component of the Joint Risk Analysis Methodologies within its four pillars (accept, avoid, mitigate transfer) in managing risks and making risk decisions.

Scheduled Records – Records whose final disposition has been approved by NARA.

scheduling – The process of determining and recording in records schedule the appropriate retention period and ultimate disposition of a series. The records thus provided for are called scheduled records.

statute – Laws or regulations that are created and enacted by legislative bodies. They are binding to all individuals and organizations within the jurisdiction of the legislative body that created them. Failure to comply with statutory requirements can result in legal penalties.

temporary record – Record approved by the National Archives and Records Administration for disposal after a specified retention period.

training materials – written documents, manuals or handbooks, video presentations and online training courses.

transfer – The process of moving records from one location to another, especially from office space to off-site storage facilities, from one agency to another, or from an agency office to a Federal Records Center or to National Archives and Records Administration.

unauthorized disposal – The improper removal of records without National Archives and Records Administration (NARA) approval or the willful or accidental destruction of records without regard to a NARA approved records schedule. Unauthorized disposition of Federal records is against the law and punishable by up to $250,000 in fines and imprisonment.

(INTENTIONALLY BLANK)

(INTENTIONALLY BLANK)
Inner Back Cover

INTENTIONALLY BLANK
(BACK COVER)