



DoD 5015.02-STD

**ELECTRONIC RECORDS
MANAGEMENT
SOFTWARE APPLICATIONS
DESIGN CRITERIA
STANDARD**

April 25, 2007

**ASSISTANT SECRETARY OF DEFENSE FOR
NETWORKS AND INFORMATION INTEGRATION/
DEPARTMENT OF DEFENSE CHIEF INFORMATION OFFICER**

FOREWORD

This Standard is reissued under the authority of DoD Directive 5015.2, "Department of Defense Records Management Program," March 6, 2000, (Reference (a)) which provides implementing and procedural guidance on the management of records in the Department of Defense. It sets forth mandatory baseline functional requirements for Records Management Application (RMA) software used by the DoD Components in implementing their records management programs; defines required system interfaces and search criteria that RMAs shall support; and describes the minimum records management requirements that must be met based on current National Archives and Records Administration (NARA) regulations.

DoD 5015.2-STD, "Design Criteria Standards for Electronic Records Management Software Applications," June 19, 2002, (Reference (b)) is hereby canceled.

This Standard applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the Department of Defense (hereafter referred to collectively as the "DoD Components").

The standard is effective immediately for all new electronic records management information systems development efforts. Commercial products applying for testing after the standard date will be held compliant to this standard. Commercial products listed as compliant to version 2 of this standard on the product register are grandfathered until their version 2 compliance expires, which is two years after their last test date. The Heads of the DoD Components may issue supplementary instructions only when necessary to provide for unique requirements within their organizations, provided those instructions do not adversely affect interoperability and compatibility with DoD Automated Information Systems (AIS) across the Global Information Grid (GIG) architecture.

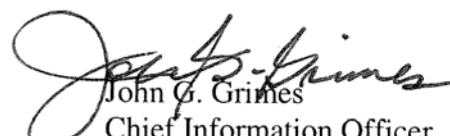
Send recommended changes to this Standard to:

Office of the Deputy Assistant Secretary of Defense/
Deputy Chief Information Officer,
Information Policy Directorate
1851 South Bell Street
Suite 600
Arlington, VA 22202

Voice: 703-602-1007
FAX: 703-602-0830
DSN: 324-1007
Email: ronald.kelly@osd.mil

DoD 5015.02-STD, April 25, 2007

This Standard is approved for public release; distribution is unlimited. The DoD Components, other Federal Agencies, and the public may obtain copies of this Standard via the Internet at: <http://www.dtic.mil/whs/directives>.



John G. Grimes
Chief Information Officer
Department of Defense

TABLE OF CONTENTS

	<u>Page</u>
FOREWORD	1
TABLE OF CONTENTS.....	3
TABLES	4
REFERENCES	7
DEFINITIONS.....	11
ABBREVIATIONS AND ACRONYMS.....	28
C1. CHAPTER 1 - GENERAL INFORMATION	30
C1.1. PURPOSE	30
C1.2. LIMITATIONS	31
C2. CHAPTER 2 - MANDATORY REQUIREMENTS.....	32
C2.1. GENERAL REQUIREMENTS	32
C2.2. DETAILED REQUIREMENTS	33
C3. CHAPTER 3 - MANAGEMENT OF CLASSIFIED RECORDS	58
C3.1. MANAGEMENT OF CLASSIFIED RECORDS.....	58
C3.2. OPTIONAL SECURITY FEATURES	64
C4. CHAPTER 4 – MANAGING RECORDS FOR THE PRIVACY ACT AND THE FREEDOM OF INFORMATION ACT	66
C4.1. MANAGEMENT OF PRIVACY ACT RECORDS.....	66
C4.2. MANAGEMENT OF FREEDOM OF INFORMATION ACT RECORDS.....	79
C4.3. ACCESS CONTROL FOR PRIVACY ACT AND FREEDOM OF INFORMATION ACT RECORDS	86
C5. CHAPTER 5 - TRANSFERS.....	92
C5.1. TRANSFER RMA TO RMA INTEROPERABILITY.....	92
C5.2. SUPPORT OF SECURITY INTEROPERABILITY ELEMENTS	105
C5.3. OPTIONAL TRANSFER ELEMENTS	106

C5.4.	TRANSFER ACCESS CONTROL.....	110
C6.	CHAPTER 6 - NON-MANDATORY FEATURES	112
C6.1.	REQUIREMENTS DEFINED BY THE ACQUIRING OR USING ACTIVITY	112
C6.2.	OTHER USEFUL RMA FEATURES.....	113
C6.3.	SEARCH AND DISCOVERY INTEROPERABILITY	116
C6.4.	NON-MANDATORY ACCESS CONTROL.....	116

TABLES

C2.T1.	FILE PLAN COMPONENTS.....	33
C2.T2.	RECORD FOLDER COMPONENTS.....	34
C2.T3.	RECORD METADATA COMPONENTS.....	37
C2.T4.	TRANSMISSION AND RECEIPT DATA.....	41
C2.T5.	RECORD METADATA COMPONENTS.....	42
C2.T6.	MANDATORY AUTHORIZED INDIVIDUAL REQUIREMENTS	49
C3.T1.	CLASSIFIED RECORD COMPONENTS	58
C3.T2.	CLASSIFIED RECORD AUTHORIZED INDIVIDUAL REQUIREMENTS	63
C4.T1.	SYSTEM OF RECORD COMPONENTS	66
C4.T2.	PRIVACY ACT FILE COMPONENTS	69
C4.T3.	INDIVIDUAL ACCESS REQUEST COMPONENTS.....	70
C4.T4.	ACCESS RECORD COMPONENTS	71
C4.T5.	DENIAL COMPONENTS.....	72
C4.T6.	APPEAL COMPONENTS	72
C4.T7.	AMENDMENT COMPONENTS	73
C4.T8.	DISPUTE COMPONENTS	74
C4.T9.	DISCLOSURE REQUEST COMPONENTS.....	75
C4.T10.	DISCLOSURE METADATA COMPONENTS	75
C4.T11.	ACCOUNTING RECORD COMPONENTS.....	77
C4.T12.	EXEMPTION COMPONENTS	78
C4.T13.	MATCHING PROGRAM COMPONENTS	78
C4.T14.	ACCESS RULES COMPONENTS.....	79
C4.T15.	FOIA REQUEST COMPONENTS	80
C4.T16.	FOIA DISCLOSURE REQUEST COMPONENTS	81
C4.T17.	FOIA DISCLOSURE COMPONENTS	81
C4.T18.	FOIA EXEMPTION COMPONENTS	83
C4.T19.	FOIA APPEAL COMPONENTS	84
C4.T20.	FOIA REPORTS METADATA DISCLOSURE COMPONENTS	85
C4.T21.	AUTHORIZED INDIVIDUAL REQUIREMENTS FOR PRIVACY ACT AND FOIA RECORDS.....	86
C5.T1.	RECORD LEVEL CORE (DEFINED MANDATORY)	94
C5.T2.	RECORD LEVEL E-MAIL (DEFINED MANDATORY).....	95
C5.T3.	RECORD LEVEL SCANNED (DEFINED MANDATORY).....	95

C5.T4.	RECORD LEVEL PDF (DEFINED MANDATORY).....	96
C5.T5.	RECORD LEVEL DIGITAL PHOTOGRAPH (DEFINED MANDATORY).....	96
C5.T6.	RECORD LEVEL WEB RECORDS (DEFINED MANDATORY).....	97
C5.T7.	RECORD LEVEL SCANNED (DEFINED OPTIONAL).....	98
C5.T8.	RECORD LEVEL PDF (DEFINED OPTIONAL).....	98
C5.T9.	RECORD LEVEL DIGITAL PHOTOGRAPH (DEFINED OPTIONAL).....	98
C5.T10.	RECORD LEVEL WEB RECORD (DEFINED OPTIONAL).....	99
C5.T11.	RECORD (TRANSFER MANDATORY).....	99
C5.T12.	RECORD (TRANSFER DEFINED OPTIONAL).....	100
C5.T13.	RECORD (TRANSFER ORGANIZATION-DEFINED).....	100
C5.T14.	RECORD LEVEL LIFECYCLE (TRANSFER MANDATORY).....	101
C5.T15.	RECORD LEVEL LIFECYCLE (TRANSFER ORGANIZATION-DEFINED).....	101
C5.T16.	FOLDER LEVEL (DEFINED TRANSFER LIFECYCLE MANDATORY).....	102
C5.T17.	FOLDER LEVEL LIFECYCLE (TRANSFER LIFECYCLE ORGANIZATION- DEFINED).....	102
C5.T18.	FOLDER LEVEL (TRANSFER MANDATORY).....	102
C5.T19.	FOLDER LEVEL (TRANSFER DEFINED OPTIONAL).....	103
C5.T20.	FOLDER LEVEL (TRANSFER ORGANIZATION-DEFINED).....	103
C5.T21.	COMPUTER FILE CORE (DEFINED MANDATORY).....	104
C5.T22.	SECURITY MARKING METADATA.....	105
C5.T23.	DOWNGRADING AND DECLASSIFICATION METADATA.....	105
C5.T24.	RECORD CATEGORY (DEFINED TRANSFER MANDATORY).....	106
C5.T25.	EVENTS (DEFINED TRANSFER MANDATORY).....	107
C5.T26.	EVENTS (TRANSFER ORGANIZATION-DEFINED).....	107
C5.T27.	TRIGGER (DEFINED TRANSFER MANDATORY).....	107
C5.T28.	TRIGGER (TRANSFER ORGANIZATION-DEFINED).....	108
C5.T29.	VITAL RECORD REVIEW (DEFINED TRANSFER MANDATORY).....	108
C5.T30.	VITAL RECORD REVIEW (TRANSFER ORGANIZATION-DEFINED).....	109
C5.T31.	LIFECYCLE PHASE (DEFINED TRANSFER MANDATORY).....	110
C5.T32.	LIFECYCLE PHASE (TRANSFER ORGANIZATION-DEFINED).....	110
C5.T33.	AUTHORIZED INDIVIDUAL REQUIREMENTS FOR TRANSFER ACCESS CONTROL.....	110
C6.T1.	AUTHORIZED INDIVIDUAL REQUIREMENTS (DEFINED OPTIONAL).....	117

REFERENCES

- (a) DoD Directive 5015.2, "Department of Defense Records Management Program," March 6, 2000
- (b) DoD 5015.2-STD, "Design Criteria Standards for Electronic Records Management Software Applications," June 19, 2002 (hereby canceled)
- (c) Director of Central Intelligence Directive 6/3, "Protecting Sensitive Compartmented Information within Information Systems," May 24, 2000
- (d) Deputy Assistant Secretary of Defense for Networks and Information Integration Specification, "Department of Defense Discovery Metadata Specification (DDMS), Version 1.3," July 29, 2005¹
- (e) Executive Order 12958, "Classified National Security Information," as amended by Executive Order 13292, "Further Amendments to Executive Order 12958," March 28, 2003
- (f) National Archives and Records Administration, "Disposition of Federal Records – A Records Management Handbook," 1997²
- (g) Title 36, Code of Federal Regulations, Parts 1194.21, 1194.22, 1194.31, 1220.14, 1222.10, 1222.32, 1222.50, 1228.24, 1228.270, 1228.54, 1228.58, 1228.60, 1234.2, 1234.22, 1234.24, 1234.28, 1234.30, 1234.32, 1234.34, 1236.14, and 1236.20
- (h) International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 11179-1, "Information technologies – Metadata Registries," September 15, 2004³
- (i) Section 3301 of title 44, United States Code, "Definition of Records"
- (j) Section 3511 of title 44, United States Code, "Establishment and Operation of Government Information Locator Service"
- (k) Federal Information Processing Standard Publication 192, "Application Profile for the Government Information Locator Service," December 7, 1994⁴
- (l) DoD Instruction 8520.2, "Public Key Infrastructure and Public Key Enabling", April 1, 2004⁵
- (m) Section 2901 of title 44, United States Code, "Definitions"
- (n) Organization for the Advancement of Structured Information Standards Reference Model for Service Oriented Architecture 1.0, August 2, 2006⁶
- (o) ISO 23081-1, "Information and Documentation — Records Management Processes- Metadata Records," January 15, 2006⁷

¹ http://www.afei.org/news/documents/DDMS-v1_2.pdf

² <http://www.archives.gov/records-mgmt/publications/disposition-of-federal-records/>

³ [http://standards.iso.org/ittf/PubliclyAvailableStandards/c035343_ISO_IEC_11179-2004\(E\).zip](http://standards.iso.org/ittf/PubliclyAvailableStandards/c035343_ISO_IEC_11179-2004(E).zip)

⁴ <http://www.itl.nist.gov/fipspubs/fip192.htm>

⁵ http://www.dtic.mil/whs/directives/corres/pdf/i85202_040104/i85202p.pdf

⁶ <http://www.oasis-open.org/committees/download.php/19679/soa-rm-cs.pdf>

⁷ https://committees.standards.org.au/COMMITTEES/IT-021/N0001/ISO_23081-1_2006.pdf

- (p) DoD Directive 5400.07, “DoD Freedom of Information Act (FOIA) Program”, October 28, 2005
- (q) Section 2902 of title 44, United States Code, “Objectives of Records Management”
- (r) DoD Chief Information Officer Memorandum, “DoD Net-Centric Data Strategy,” May 9, 2003
- (s) DoD Directive 8320.2, “Data Sharing in a Net-Centric Department of Defense,” December 2, 2004
- (t) NARA Guidance, “Electronic Records Management Guidance on Methodology for Determining Agency-unique Requirements,” August 23, 2004⁸
- (u) Section 3103 of title 44, United States Code, “Transfer of Records to Records Centers”
- (v) ISO 8601, “Data elements and interchange formats – Information interchange – Representation of dates and times,” December 3, 2004⁹
- (w) Section 794d of title 29, United States Code, “Electronic and Information Technology”
- (x) Section 3303 of title 44, United States Code, “Lists and Schedules of Records”
- (y) Records Management Task Force Guidance, “Functional Baseline Requirements and Data Elements for Records Management Application Software,” August 28, 1995¹⁰
- (z) Director of Central Intelligence Directive (DCID) 6/6, “Security Control on the Dissemination of Intelligence Information,” July 11, 2001
- (aa) DoD Directive 5210.83, “Department of Defense Unclassified Controlled Nuclear Information (DoD UNCI),” November 15, 1991
- (ab) DoD 5400.7-R, “DoD Freedom of Information Act Program Regulation,” September 1998
- (ac) DoD Directive 5230.24, “Distribution Statements on Technical Documents,” March 18, 1987
- (ad) DoD 5200.1-R, “Information Security Program Regulation,” January 14, 1997
- (ae) Section 3105 of title 44, United States Code, “Safeguards”
- (af) Section 2909 of title 44, United States Code, “Retention of Records”
- (ag) Executive Order 12968, “Access to Classified Information,” August 4, 1995
- (ah) Title 32, Code of Federal Regulations, Part 2001, “Classified National Security Information,” current edition
- (ai) Controlled Access Program Coordination Office (CAPCO), “The Authorized Classification & Controlled Markings Register”¹¹
- (aj) Section 552a of title 5, United States Code
- (ak) DoD 5400.11-R, “Department of Defense Privacy Program,” August 1983
- (al) Organization for the Advancement of Structured Information Standards (OASIS) Specification, “Universal Description, Discovery and Integration v3.0.2 (UDDI),” February 2005¹²

⁸ <http://www.archives.gov/records-mgmt/policy/requirements-guidance.html>

⁹ <http://www.iso.org/iso/en/prods-services/popstds/datesandtime.html>

¹⁰ http://jitic.fhu.disa.mil/recmgmt/func_req.doc

¹¹ <http://www.cms.ic.gov/capco> or <http://www.cms.cia.sgov/capco>

¹² <http://www.uddi.org/specification.html>

DoD 5015.02-STD, April 25, 2007

- (am) Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Plan, “DoD Information Management (IM) Strategic Plan, Version 2.0,” October 1, 1999¹³
- (an) DoD Chief Information Officer Architecture, “Global Information Grid Architecture, Version 2.0,” December 9, 2003¹⁴
- (ao) Joint Requirements Oversight Council Memorandum, “Global Information Grid Capstone Requirements Document, JROCM 134-01,” August 30, 2001
- (ap) DoD Directive 4630.5, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” May 4, 2004

¹³ <http://www.dod.mil/nii/org/cio/ciolinks/references/itmstpln/itmstpln-memo.html>

¹⁴ <https://standmgt.disa.mil/restricted/ncow.html>

DEFINITIONS

DL1.1. Access. The ability or opportunity to gain knowledge of stored information.

DL1.2. Access Control. The term “access control” has the following meanings:

DL1.2.1. A service feature or technique used to permit or deny use of the components of a communication system.

DL1.2.2. A technique used to define or restrict the rights of individuals or application programs to obtain data from, or place data onto, a storage device.

DL1.2.3. The definition or restriction of the rights of individuals or application programs to obtain data from, or place data into, a storage device. Types of access control methods include Mandatory Access Control and Discretionary Access Control (Reference (c)).

DL1.2.4. The process of limiting access to the resources of an AIS to authorized users, programs, processes, or other systems. (DL1.15)

DL1.2.5. The function performed by the resource controller that allocates system resources to satisfy user requests.

DL1.3. Accession. The act of transferring physical custody of documentary material to an archival institution.

DL1.4. Addressee. The name of the organization or individual to whom a record is addressed.

DL1.5. Application. The system or problem to which a computer is applied. Reference is often made to an application as being either of the computational type (arithmetic computations predominate) or of the data processing type (data handling operations predominate).

DL1.6. Application Administrators. The individuals who are responsible for setting up the RMA infrastructure write the configuration plan and periodic changes for Network System Administrator implementation.

DL1.7. Attachment. A record, object, or document associated with another document or record and filed in the RMA or transmitted as part of the other document or record.

DL1.8. Attribute. The term “attribute” is defined in Deputy Assistant Secretary of Defense for Networks and Information Integration Specification (Reference (d)).

DL1.9. Audit Trail. An electronic means of tracking interactions with records within an electronic system so that any access to the record within the electronic system can be

documented as it occurs or afterward. An audit trail may identify unauthorized actions in relation to the records, e.g., modification, deletion, or addition.

DL1.10. Authenticity. A condition that proves that a record is genuine based on its mode (i.e., a method by which a record is communicated over space or time), form (i.e., the format or media that a record has upon receipt), state of transmission (i.e., the primitiveness, completeness, and effectiveness of a record when it is initially set aside after being made or received), and manner of preservation and custody.

DL1.11. Authorized Individual. A Records Manager or other person specifically designated by the Records Manager as responsible for managing various aspects of an organization's records.

DL1.12. Author, Originator, or Creator. The person, office, or designated position responsible for creation or issuance of a document. The author, originator, or creator is usually indicated on the letterhead or by signature. For RMA purposes, the author, originator, or creator may be designated as a person, official title, office symbol, or code.

DL1.13. Auto-Filing. The ability of an RMA to automatically file records without user intervention.

DL1.14. Backward Compatible. The ability of a software program or piece of hardware to read files in previous versions of the software or hardware.

DL1.15. Biometrics. The measurable physical characteristics or personal behavioral traits used to recognize the identity or verify the claimed identity of an individual. (DL1.2)

DL1.16. Boolean Operators. The operators of Boolean algebra. Boolean operators may be represented in various ways. Often they are simply written as "AND," "OR," and "NOT". While any number of logical "ANDs" (or any number of logical "ORs") may be chained together without ambiguity, the combination of "ANDs" and "ORs" and "NOTs" can lead to ambiguity. In such cases, parentheses may be used to clarify the order of operations. As always, the operations within the innermost set of parentheses is performed first, followed by the next set out, etc., until all operations within parentheses have been completed. Then any operations outside the parentheses are performed.

DL1.17. Bulk Load. An automatic data import.

DL1.18. Business Rules. The descriptions of operations, definitions and constraints that apply to an organization in achieving its goals. For example, a business rule might state that no credit check is to be performed on return customers. Other rules might define a tenant in terms of solvency or list preferred suppliers and supply schedules. These rules would then be used to help

the organization to better achieve goals, communicate among principals and agents, communicate with interested third parties, demonstrate fulfillment of legal obligations, operate more efficiently, automate operations, and perform analysis on current practices.

DL1.19. Cascading Style Sheets (CSS). A stylesheet language used to describe the presentation of a document written in a markup language. Its most common application is to style web pages written in Hypertext Markup Language (HTML) and Extensible Hypertext Markup Language (XHTML), but the language can be applied to any application of Extensible Markup Language (XML), including Scalable Vector Graphics (SVG) and Extensible User Interface Language (XUL). The CSS specifications are maintained by the World Wide Web Consortium (W3C).

DL1.20. Classification Guide. A documentary form of classification guidance issued by an original classification authority that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element. (Reference (e)).

DL1.21. Classified Information. The information that has been determined pursuant to Executive Order (EO) 12958, as amended by EO 13292 (Reference (e)) or any predecessor order, to require protection against unauthorized disclosure, and that is marked to indicate its classified status when in documentary form.

DL1.22. Classification Markings. The identifications or markings that leave no doubt about the classified status of the information, the level of protection required, and the duration of the classification. Such markings include: Overall Markings, Portion Markings, Classified by line, Reason line, Derived from line, and Declassify on line (Reference (e)).

DL1.23. Common Access Cards (CAC). The cards that feature bar-coding, a magnetic strip, and an embedded integrated circuit chip used for access to buildings, to computer systems, etc.

DL1.24. Compression. A process, which using special software, reduces the file size of a given electronic file.

DL1.25. Copy. In electronic records, the action or result of reading data from a source (the RMA's repository), leaving the source data unchanged, and writing the same data elsewhere on a medium that may differ from the source (a user workspace or other device) (NARA Handbook, Reference (f)).

DL1.26. Create. In electronic records, the action or result of filing a new record and its associated metadata.

DL1.27. Creator. (DL1.12.)

DL1.28. Cutoff. To cut off records in a file means to break, or end, the record at regular intervals to permit disposal or transfer in complete blocks and, for correspondence files, to permit the establishment of new files. Cutoffs are needed before disposition instructions can be applied because retention periods usually begin with the cutoff, not with the creation or receipt, of the records. In other words, the retention period normally does not start until the records have been cut off. Cutoffs involve ending input to old files and starting input to new ones at regular intervals (Reference (f)). Cutoff is sometimes abbreviated as COFF and is also called file cutoff or file break.

DL1.28.1. For records with retention periods of less than 1 year, the cutoff is at an interval equal to the retention period. For example, if a record series has a 1-month retention period, cut the file off at the end of each month and then apply the retention period (that is, hold the file 1 more month before destroying it).

DL1.28.2. For records with retention periods of 1 year or more, the cutoff is at the end of each fiscal (or calendar) year. For example, if the disposition instruction for a correspondence file is "Destroy after 3 years," then destroy it 3 years after the annual cutoff date has been reached.

DL1.28.3. For records with retention periods based on an event or action, cutoff on the date the event occurs or when the action is completed, and then apply the retention period. For example, if the disposition for case working papers is "Destroy when related case file is closed," then cut off and destroy the working papers when closing the related file.

DL1.28.4. For records with retention periods based on a specified time period after an event or action occurs, apply the retention period after the placement in an inactive file on the date the event occurs or when the action is completed and the inactive file is cutoff at the end of each fiscal (or calendar) year. For example, if the disposition for a case file is "Destroy 6 years after case is closed," then destroy 6 years after the annual cutoff along with all other case files closed during that year.

DL1.29. Cycle. The periodic replacement of obsolete copies of vital records with copies of current vital records. This may occur daily, weekly, quarterly, annually, or at other designated intervals as specified by regulation or by the Records Manager (part 1236.14 of title 36 Code of Federal Regulations (CFR), (Reference (g))).

DL1.30. DoD Discovery Metadata Specification (DDMS). The Department of Defense Discovery Metadata Specification defines discovery metadata elements for resources posted to community and organizational shared spaces. The DDMS specifies a set of information fields used to describe any data or service asset that is made known to the Enterprise.

DL1.31. Database. In electronic records, a set of data elements, consisting of at least 1 file or of a group of integrated files, made available to several users (part 1234.2 of Reference (g)).

DL1.32. Database Management System (DBMS). A software system used to access and retrieve data stored in a database (part 1234.2 of Reference (g)).

DL1.33. Data Element. Unit of data for which definition, identification, representation and permissible values are specified by means of a set of attributes (ISO Standard, Reference (h)).

DL1.34. Date Filed. The date and time that an electronic document was filed in the RMA and declared a record. This date and time shall be assigned by the computer at the time the record is filed in the RMA.

DL1.35. Declassification. The authorized change in the status of information from classified information to unclassified information (Reference (e)).

DL1.36. Declassification Guide. The written instructions issued by a declassification authority that describes the elements of information regarding a specific subject that may be declassified and the elements that must remain classified (Reference (e)).

DL1.37. Defense Message System (DMS). A secure and accountable writer-to-reader messaging service accessible from world-wide DoD locations to tactically deployed users and other designated Federal users, with interfaces to Allied users and Defense contractors.

DL1.38. Denial Authority. The name, title, position, and signature or electronic signature of individual designated with permission to deny access to records requested under the Privacy Act, or FOIA.

DL1.39. Derivative Classification. The incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification (Reference (e)).

DL1.40. Destruction. In records management, the primary type of disposal action. Methods of destroying records include selling or salvaging the record medium and burning, pulping, shredding, macerating, or discarding it with other waste materials (part 1228.58 of Reference (g)).

DL1.41. Disposition. Those actions taken regarding Federal records after they are no longer required to conduct current Agency business (Reference (f)). These actions include:

DL1.41.1. The transfer of records to Agency storage facilities or Federal Record Centers (FRCs).

DL1.41.2. The transfer of records from one Federal Agency to another.

DL1.41.3. The transfer of permanent records to NARA.

DL1.41.4. The disposal of temporary records no longer needed to conduct agency business, usually by destruction or, occasionally, by donation of temporary records to an eligible person or organization after the authorized retention period has expired and after NARA has approved the donation (part 1228.60 of Reference (g)).

DL1.42. Disposition Action. The action to be taken when a disposition date occurs (e.g., interim transfer, accession, or destroy).

DL1.43. Disposition Action Date. The fixed date on which the records in a file become due for final disposition.

DL1.44. Disposition Authority. The legal authority that empowers an Agency to transfer permanent records to NARA or to carry out the disposal of temporary records. Must be obtained from NARA and also, for certain records proposed as temporary, from the GAO (Reference (f)).

DL1.45. Disposition Instruction. The directions for cutting off records and carrying out their disposition (transfer, retirement, or destruction) in compliance with NARA's regulations and the General Records Schedule. Disposition instructions in an RMA include retention-related fields such as authority, transfer location, active or dormant chronological retention periods, and conditional retention periods (Reference (f)).

DL1.46. Disposition Instruction Type. One of three ways of scheduling a disposition instruction: time, event, or a combination of both time and event. (DL1.57, DL1.129, DL1.130, and Reference (f)).

DL1.47. Document. The information set down in any physical form or characteristic. A document may or may not meet the definition of a record.

DL1.48. Document Type Definition (DTD). A Document Type Definition is a set of declarations that conform to a particular markup syntax and that describe a class, or "type", of SGML or XML documents, in terms of constraints on the structure of those documents. A DTD

specifies, in effect, the syntax of an “application” of SGML or XML, such as the derivative language HTML or XHTML. This syntax is usually a less general form of the syntax of SGML or XML.

DL1.49. Downgrade. A determination by a declassification authority that information classified and safeguarded at a specified level shall be classified and safeguarded at a lower level (Reference (e)).

DL1.50. Drop-Down Lists. A predefined set of data used to populate certain record metadata fields.

DL1.51. Dublin Core. The Dublin Core is a metadata element set which is a standard for cross-domain information resource description. It includes all Dublin Core Metadata Initiative terms (that is, refinements, encoding schemes, and controlled vocabulary terms) intended to facilitate discovery of resources. The Dublin Core has been in development since 1995 through a series of focused invitational workshops that gather experts from the library world, the networking and digital library research communities, and a variety of content specialties.

DL1.52. Edit. A function that allows the user to change an existing record's metadata.

DL1.53. Electronic Mail Message. A document created or received via an electronic mail system, including brief notes, formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message (part 1234.2 of Reference (g)).

DL1.54. Electronic Mail System. A computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or data bases on either personal computers or mainframe computers, and word processing documents not transmitted on an e-mail system. (Part 1234.2 of Reference (g)).

DL1.55. Electronic Record. The information recorded in a form that requires a computer or other machine to process it and that satisfies the legal definition of a record according to section 3301 of title 44 of United States Code (USC) (Reference (i)).

DL1.56. Embedded Fonts. The technology that allows fonts used in the creation of a document to travel with that document, ensuring that a user sees documents exactly as the designer intended them to be seen.

DL1.57. Event Disposition. A disposition instruction in which a record is eligible for the specified disposition (transfer or destroy) upon or immediately after the specified event occurs. No retention period is applied and there is no fixed waiting period as with “timed” or combination “timed-event” dispositions. Example: “Destroy upon completion of Government Accountability Office Audit” (Reference (f)).

DL1.58. Exchangeable Image File Format (EXIF) Information. The exchangeable image file format is a specification for the image file format used by digital cameras.

DL1.59. Exemption Categories. A list of specific reasons, as specified in EO 12958, as amended, that agency heads use to exempt classified material from automatic declassification.

DL1.60. Extensibility. A system design principle where the implementation takes into consideration future growth. It is a systemic measure of the ability to extend a system and the level of effort required to implement the extension. Extensions can be through the addition of new functionality or through modification of existing functionality. The central theme is to provide for change while minimizing impact to existing system functions.

DL1.61. File. An arrangement of records.

DL1.61.1. When used as a noun, this term is used to denote papers, photographs, photocopies, maps, machine-readable information, or other recorded information, regardless of physical form or characteristic. Files are accumulated or maintained on shelves, in filing equipment, boxes, or machine-readable media, and they occupy office or storage space (part 1220.14 of Reference (g)).

DL1.61.2. When used as a verb, this term is used to define the act of assigning and storing records in accordance with the file plan (Reference (f)).

DL1.62. File Plan. A document containing the identifying number, title, description, and disposition authority of files held or used in an office (Reference (f)).

DL1.63. Format. For electronic records, this term refers to the computer file format described by a formal or vendor standard or specification, such as ISO/IEC 8632-1 [Information Technology - Computer Graphics - Metafile for the Storage and Transfer of Picture Description Information (CGM)]; ISO/IEC 10918 [Joint Photographic Experts Group (JPEG)]; WordPerfect for Windows; or Microsoft Word for Windows. For non-electronic records, the format refers to its physical form: e.g., paper, microfilm, and video.

DL1.64. Freeze. The suspension or extension of the disposition of temporary records that cannot be destroyed on schedule because of special circumstances, such as a court order or an

investigation. A freeze requires a temporary extension of the approved retention period (Reference (f)).

DL1.65. Global Information Grid (GIG). The globally interconnected, end-to-end set of information capabilities, associated processes and personnel for collecting, processing, storing, disseminating, and managing information on demand to Warfighters, policy makers, and support personnel. The GIG includes all owned and leased communications and computing systems and services, software (including applications), data, security services, and other associated services necessary to achieve information superiority.

DL1.66. Government Information Locator Service (GILS). A Federal Government service to help the general public locate and access information throughout the Federal Government according to section 3511 of title 44 USC (Reference (j)). GILS describes the information available in those resources and provides assistance in obtaining that information. GILS uses network technology and international standards for information search and retrieval. These standards are described in the Federal Information Processing Standard (FIPS) Publication 192, "Application Profile for the Government Information Locator Service" (Reference (k)).

DL1.67. International Color Consortium/Image Color Management (ICC/ICM) Profile. The profile describing exactly how the primary colors map to device independent color.

DL1.68. Imaging Tools. The software and hardware that works together to capture, store, and recreate images.

DL1.69. Information. Facts, data, or instructions in any medium or form.

DL1.70. Ingest. The ability of an RMA to bring in exported records and record metadata.

DL1.71. Inheritance. The field inherits data from the same field in the parent object.

DL1.72. Intelligent Name. An intelligent name is a clear, uncoded identification of the individual.

DL1.73. Interdependent Fields. The values placed in one field have an affect on what related fields are mandatory or what data can be entered into those fields.

DL1.74. Interoperability. The ability of systems, units, or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together.

DL1.75. Keyboard Shortcut. A keyboard shortcut (also known as an accelerator key, shortcut key, or hotkey) is one or a set of keyboard keys that, when pressed simultaneously, perform a predefined task. Such a task could be done with the computer's pointing device, but would require the user to take his or her hands off of the keyboard, and then place them on said device. Hence, they are a shortcut in that they save the user time.

DL1.76. Life Cycle. The records life cycle is the life span of a record from its creation or receipt to its final disposition. It is usually described in three stages: creation, maintenance and use, and final disposition.

DL1.77. Lifecycle Phase. A specific phase of a record's existence from creation through final disposition.

DL1.78. Linking. The action of referencing or associating records with one another.

DL1.79. Location of Record. A pointer to a record's location. Examples: an operating system path and filename, the location cited within a file plan, or the location of a magnetic tape rack.

DL1.80. Marginalia. The general term for notes, scribbles, doodles and editorial comments made in the margin of a book. Marginalia can add or detract from the value of a book, depending on the book and the author of the marginalia

DL1.81. Media Type. The material or environment on which information is inscribed (e.g., microform, electronic, paper).

DL1.82. Move. The function that allows the user to relocate records and metadata.

DL1.83. Multiple Sources. The information classified based on two or more source documents, classification guides or combination of both (Reference (e)).

DL1.84. Namespace. An XML namespace is a W3C standard for providing uniquely named elements and attributes in an XML instance. An XML instance may contain element or attribute names from more than one XML vocabulary. If each vocabulary is given a namespace then the ambiguity between identically named elements or attributes can be resolved. All element names within a namespace must be unique.

DL1.85. Office Applications. The software packages that perform a variety of office support functions, such as word processing, desktop publishing, spreadsheet calculations, electronic mail, facsimile transmission and receipt, document imaging, optical character recognition (OCR), workflow, and data management. These applications are generally used to generate, convert, transmit, or receive business documents.

DL1.86. Optical Character Recognition (OCR). The recognition of printed or written text characters by a computer. This involves analysis of the scanned-in image and then translation of the character image into character codes, such as American Standard Code for Information Interchange (ASCII). OCR is being applied by libraries, businesses, and government agencies to create text-searchable files for digital collections. OCR is also used to help process checks and credit card slips and sort the mail.

DL1.87. Original Classification. An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure (Reference (e)).

DL1.88. Originating Organization. The official name or code identifying the office responsible for the creation of a document.

DL1.89. Permanent Record. A record appraised by NARA as having sufficient historical or other value to warrant continued preservation by the Federal Government beyond the time it is normally needed for a particular Agency's administrative, legal, or fiscal purposes (Reference (f)).

DL1.90. Public Key-Enabled. The incorporation of the use of certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation (DoD Instruction, Reference (I)).

DL1.91. Portal. A single point of access for all repositories and databases storing electronic records and record metadata.

DL1.92. Producing Applications. The software that feeds records into the RMA.

DL1.93. Product Combinations. The result of integrating two or more distinct products, where typically, one product primarily creates records and another product performs the records' retention schedule tracking.

DL1.94. Privileged Users. The individuals who are given special permission to perform functions beyond those of typical users.

DL1.95. Publication Date. The date and time that the author or originator completed the development of or signed the document. For electronic documents, this date and time should be established either by the author or from the time attribute assigned to the document by the application used to create the document. This is not necessarily the date or time that the document was filed in the RMA.

DL1.96. Public Key Infrastructure (PKI). An arrangement that provides for third party vetting of, and vouching for, user identities. It also allows binding of public keys to users. This is usually carried out by software at a central location together with other coordinated software at distributed locations. The public keys are typically in certificates.

DL1.97. Rebuild. Reconstructing the records management environment after a disaster.

DL1.98. Receipt Data. The information in electronic mail systems regarding dates and times of receipt of a message, or acknowledging receipt or access by specific addressee(s). It is not the date and time of delivery to the Agency. If receipt data are provided by the computer system, they are a required part of documents or records received through electronic mail (part 1234.2 of Reference (g)).

DL1.99. Record. The information, regardless of medium, that details business transactions. Records include all books, papers, maps, photographs, machine-readable materials, and other documentary materials, regardless of physical form or characteristics. Records are made or received by an Agency of the United States Government under Federal law or in connection with the transaction of public business. Records are 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 Government or because of the value of data in the record (Reference (i)).

DL1.100. Record Category. A description of a particular set of records within a file plan. Each category has retention and disposition data associated with it, applied to all record folders and records within the category.

DL1.101. Record Category Identifier. An Agency's alphanumeric or numeric identifier indicating a unique record category.

DL1.102. Record Element. A logical data structure comprised of embedded record elements and record attributes.

DL1.103. Record Folder. A record folder is an extension to the file plan either as a static structure or an aggregate gathering of records. It is used to manage case records and to break other records into periods supporting retention and disposition.

DL1.104. Record Identifier. An element of metadata, a record identifier is a data element whose value is system-generated and that uniquely identifies a particular record.

DL1.105. Records Management. The planning, controlling, directing, organizing, training, promoting, and other managerial activities involving the life cycle of information, including

creation, maintenance (use, storage, retrieval), and disposal, regardless of media. Record management procedures are used to achieve adequate and proper documentation of Federal policies and transactions and effective and economical management of Agency and organizational operations as stated in Section 2901 of Title 44 of USC (Reference (m)).

DL1.106. Records Management Application. The software used by an organization to manage its records. An RMA's primary management functions are categorizing and locating records and identifying records that are due for disposition. RMA software also stores, retrieves, and disposes of the electronic records that are stored in its repository.

DL1.107. Records Managers. The individuals who are responsible for records management administration.

DL1.108. Record Metadata. The information describing data; that is, information describing the structure (data elements), interrelationships, and other characteristics of records (ISO Standard (Reference (o))).

DL1.109. Recovery/Rollback Capability. The ability to re-establish the system following any system failure.

DL1.110. Redaction. The separation of disclosable from non-disclosable information by removing or permanently blocking out individual words, sentences or paragraphs, or the removal of whole pages prior to the release of the document.

DL1.111. Referential Integrity. The capability of ensuring that all references are updated or deleted as necessary when a key reference is changed in a database environment.

DL1.112. Regrade. A determination by a classification or declassification authority that information classified and safeguarded at a specified level requires a different level of classification and safeguarding.

DL1.113. Relational Integrity. The capability of ensuring that "children" in a database or hierarchical structure are updated or deleted appropriately as actions are taken on the "parent." Maintaining relational integrity prevents "orphans."

DL1.114. Rendering Aid. The capability to properly render and present metadata content and context.

DL1.115. Rendition. The replication that provides the same content but differs from the reference because of storage format, or storage medium.

DL1.116. Repository for Electronic Records. A direct access device on which the electronic records and associated metadata are stored.

DL1.117. Retention Period. The length of time that a record must be kept before it can be destroyed. Records not authorized for destruction are designated for permanent retention. Retention periods for temporary records may be expressed in two ways (Reference (f)).

DL1.117.1. A fixed period from the time records in the series or system is created. Normally, a fixed period that follows their regular cutoff dates. For example, the phrase “destroy after 2 years” provides continuing authority to destroy records in a given series 2 years after their creation (normally 2 years after their regular cutoff date).

DL1.117.2. A fixed period after a predictable event. Normally, a fixed period following the systematic cutoff applied after completion of an event. The wording in this case depends on the kind of action involved. Note the following examples:

DL1.117.2.1. “After completion” (as of a study, project, audit).

DL1.117.2.2. “After sale or transfer” (as of personal or real property).

DL1.117.2.3. “After publication” (as of monthly reports).

DL1.117.2.4. “After superseded” (as of an administrative directive).

DL1.117.2.5. “After revision or cancellation” (as of a form).

DL1.117.2.6. “After acceptance or rejection” (as of an application).

DL1.118. Retention Schedule. A plan for the management of records listing types of records and how long they should be kept; the purpose is to provide continuing authority to dispose of, transfer, or archive records.

DL1.119. Roles. The grouping of resource permissions defined for an application.

DL1.120. Scheduled Records. The records whose final disposition has been approved by NARA.

DL1.121. Screening. The aggregation and review of records for management and disposition purposes.

DL1.122. Service-oriented Architecture (SOA). A paradigm for organizing and using distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with, and use capabilities to produce desired effects that are consistent with measurable preconditions and expectations (Reference (n)).

DL1.123. Source Document. An existing document that contains information that is incorporated, paraphrased, restated, or generated in new form into a new document (Reference (e)).

DL1.124. Standardized Data Element. The data elements as defined by particular stakeholder groups or communities of interest including but not limited to type, size, label, definition and value domain.

DL1.125. Storage. The space for non-active records, which can be digital, optical, or physical.

DL1.126. Subject. The principal topic addressed in a record.

DL1.127. Supplemental Markings. The document markings not necessarily related to classification markings, but which elaborate on or clarify document handling, e.g., “ORCON (Originator Controlled);” Special Access Programs; “RD (Restricted Data).”

DL1.128. System of Records. A group of records under the control of any agency from which information is retrieved by the name of the individual or by an individual identifier.

DL1.129. Time Disposition. A disposition instruction specifying when a record shall be cut off and when a fixed retention period is applied. The retention period does not begin until after the records have been cut off. Example: “Destroy after 2 years — cut off at the end of the calendar (or fiscal) year; hold for 2 years; then destroy” (Reference (f)).

DL1.130. Time-Event Disposition. A disposition instruction specifying that a record shall be disposed of at a fixed period of time after a predictable or specified event. Once the specified event has occurred, then the retention period is applied. Example: “Destroy 3 years after close of case.” The record does not start its retention period until after the case is closed — at that time its folder is cutoff and the retention period (destroy after 3 years) is applied (Reference (f)).

DL1.131. Transfer. The act or process of moving records from one location to another, especially from the office space in which the record is used, to Agency storage facilities or FRCs, from one Federal Agency to another, or from office or storage space to NARA for permanent preservation. Transfer does not relieve the owning organization of legal and management responsibilities for non-permanent records. Transferring permanent records to NARA does not transfer legal ownership and responsibility for the records to NARA until an SF

258, Agreement To Transfer Records To The National Archives Of The United States is generated by NARA and approved by the transferring Agency. (Reference (f)).

DL1.132. Transmission Data. The information in electronic mail systems regarding the date and time messages were sent or forwarded by the author or originator. If this data is provided by the electronic mail system, it is required as part of the record for documents that are transmitted and received via electronic mail (part 1234.2 of Reference (g)).

DL1.133. Trigger. The procedures that are stored in a database and executed or “fired” when a table is modified. Triggers are very powerful tools that can be used to perform many tasks such as restricting access to specific data, perform logging, or auditing of data sets.

DL1.134. Unscheduled Records. The records that do not have a NARA-approved final disposition.

DL1.135. Upgrade. A determination that certain information requires, in the interest of national security, a higher degree of protection against unauthorized disclosure than currently provided, together with a changing of the classification designation to reflect such higher degree. The determination to reclassify information pursuant to EO 12958 as amended by EO 13292 (Reference (e)) is a form of classification upgrade for the purposes of this Standard.

DL1.136. User-Definable Fields. The fields defined during application configuration by authorized individuals to support organization-specific information management and access requirements.

DL1.137. Version. Changes in version imply substantive changes in content rather than differences in format,

DL1.138. View. The function that allows the user to look at the metadata and content of a record in a viewer or other application.

DL1.139. Vital Records. The essential Agency records needed to meet operational responsibilities under national security emergencies or other emergency or disaster 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). They are subject to periodic review and update. Emergency operating records are the type of vital records essential to the continued functioning or reconstitution of an organization during and after an emergency. Included are emergency plans and directive(s), orders of succession, delegations of authority, staffing assignments, selected program records needed to continue the most critical Agency operations, and related policy or procedural records assisting Agency staff in conducting operations under emergency conditions and for resuming normal operations after an emergency.

Legal and financial rights records are those essential to protecting the legal and financial rights of the Government and of the individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as “rights-and-interests” records (part 1236.14 of Reference (g)).

DL1.140. Web Services. A standardized way of integrating web-based applications using open standards over an Internet Protocol backbone. Web services allow applications developed in various programming languages and running on various platforms to exchange data without intimate knowledge of each application’s underlying IT systems (Reference (s)).

DL1.141. Workflow. The tasks, procedural steps, organizations or people, required input and output information, and tools needed for each step in a business process. A workflow approach to analyzing and managing a business process can be combined with an object-oriented programming approach, which tends to focus on documents, data, and databases.

DL1.142. EXtensible Stylesheet Language Transformations (XSLT). The styling of an XML document by describing how one XML document is transformed into another XML document.

DL1.143. XML Schema. An XML schema is a description of a type of XML document, typically expressed in terms of constraints on the structure and content of documents of that type, above and beyond the basic syntax constraints imposed by XML itself. An XML schema provides a view of the document type at a relatively high level of abstraction.

ABBREVIATIONS AND ACRONYMS

AIS	Automated Information System
ASCII	American Standard Code for Information Interchange
BIFF	Binary Interchange File Format
C4ISR	Command, Control, Communications, Computers and Intelligence Surveillance and Reconnaissance
CAC	Common Access Card
CFR	Code of Federal Regulations
CGM	Computer Graphics Metafile
COFF	Cutoff
COTS	Commercial-Off-The-Shelf
CSS	Cascading Style Sheets
DBMS	Database Management System
DCID	Director of Central Intelligence Directive
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry
DDMS	DoD Discovery Metadata Specification
DMS	Defense Message System
DoDD	Department of Defense Directive
DTD	Document Type Definition
EO	Executive Order

E-mail	Electronic mail
EXIF	Exchangeable Image File Format
FIPS	Federal Information Processing Standard
FOIA	Freedom of Information Act
FRC	Federal Records Center
GAO	Government Accountability Office
GIF	Graphic Image Format
GIG	Global Information Grid
GILS	Government Information Locator Service
GOTS	Government Off-the-Shelf
HTML	Hyper Text Markup Language
IAR	Individual Access Request
ICC/ICM	International Color Consortium/Image Color Management
IC ISM	Intelligence Community Metadata Standard for Information Security Markings
IEC	International Electrotechnical Commission
IM	Information Management
ISO	International Organization for Standardization
IT	Information Technology
JITC	Joint Interoperability Test Command
JPEG	Joint Photographic Experts Group

JTA	Joint Technical Architecture
LAN	Local Area Network
NARA	National Archives and Records Administration
NOS	Network Operating System
NSS	National Security Systems
OCR	Optical Character Recognition
OLE	Object Linking and Embedding
ORCON	Originator Controlled
OSD	Office of the Secretary of Defense
PDF	Portable Document Format
PKI	Public Key Infrastructure
PNG	Portable Network Graphics
RD	Restricted Data
RMA	Records Management Application
RMTF	Records Management Task Force
SGML	Standard Generalized Markup Language
SMTP	Simple Mail Transfer Protocol
sRGB	Standard Red Green Blue
SOA	Service Oriented Architecture

SOR	System of Records
SORN	System of Records Notice
STD	Standard
SVG	Scalable Vector Graphics
TCP/IP	Transmission Control Protocol/Internet Protocol
TIFF	Tagged Image Interchange Format
UCNI	Unclassified Controlled Nuclear Information
UDDI	Universal Description Discovery and Integration
URL	Uniform Resource Locator
USC	United States Code
UUID	Universally Unique Identifier
WAN	Wide Area Network
W3C	World Wide Web Consortium
XHTML	eXtensible Hypertext Markup Language
XML	eXtensible Markup Language
XSLT	eXtensible Stylesheet Language Transformations
XUL	XML User-interface Language

C1. CHAPTER 1

GENERAL INFORMATION

C1.1. PURPOSE

C1.1.1. This Standard sets forth mandatory baseline functional requirements and requirements for classified marking, access control, and other processes, and identifies non-mandatory features deemed desirable for Records Management Application (RMA) software. This revised version of the Standard incorporates requirements for managing Freedom of Information Act and Privacy Act records (Reference (p)). This version also incorporates baseline requirements for RMA to RMA interoperability and archival transfer to the NARA.

C1.1.2. This Standard describes the minimum records management requirements that must be met in accordance with section 2902 of title 44 United States Code (USC) Reference (q) and guidance and implementing regulations promulgated by NARA. The word “shall” identifies mandatory system standards and the word “should” identifies design objectives that are desirable but not mandatory.

C1.1.3. This version also expects the development of RMA software to adhere to DoD net-centric information sharing principles and is intended to provide guidance to vendors (References (r) and (s)). The DoD Components shall use this Standard in the implementation of their records management programs to include certification testing by Joint Interoperability Test Command (JITC). DoD Chief Information Officer Memorandum (Reference (r)) and DoD Directive (Reference (s)) detail the DoD information sharing principles, identifying the need to make data holdings visible, accessible, understandable, and trusted. The DoD records are an important part of the DoD information assets, and as such should be included in efforts to improve information sharing. New requirements found in this Standard are intended to ensure that for the Department of Defense, RMA software shall facilitate DoD Component, Service, and Agency efforts to share information. The goal of this Standard relative to the DoD records is to make records:

C1.1.3.1. Visible by developing and registering standardized metadata.

C1.1.3.2. Accessible through web services with usable, standardized interfaces.

C1.1.3.3. Understandable through the availability and use of rich metadata describing the records and their context.

C1.1.4. As part of the DoD movement towards net-centric information sharing, RMA software should migrate towards providing standards-compliant services for the Department of Defense. These services would provide the capability to announce an RMA's holdings and request records, making records both visible and accessible. The services would be paired with service connection instructions, making the service itself understandable. DoD users of RMA software would then incorporate these services into a larger service-oriented architecture to achieve broader information sharing.

C1.2. LIMITATIONS

This Standard addresses a minimum set of baseline functional requirements applicable to all RMAs used within the Department of Defense. For the Defense Information Systems Agency's (DISA) Joint Interoperability Test Command (JITC) to certify that an RMA is compliant with this Standard, these minimum requirements must be met, regardless of organizational and site-specific needs. Using organizations may identify additional requirements to satisfy their site-specific needs, but these functions shall not be tested nor certified as compliant by JITC. Examples of site-specific needs are the capability to capture and manage DMS records, and the capability to adopt features described as optional in Chapter C6 of this Standard. Site-specific requirements shall be addressed in detail in a later version of this Standard. Please refer to NARA Guidance, "Electronic Records Management Guidance on Methodology for Determining Agency-unique Requirements" (Reference (t)).

C2. CHAPTER 2

MANDATORY REQUIREMENTS

C2.1. GENERAL REQUIREMENTS

C2.1.1. Managing Records. RMAs shall manage records in accordance with this Standard, regardless of storage media or other characteristics (section 1222.10 of Reference (g) and section 3103 of Reference (u)).

C2.1.2. Accommodating Dates and Date Logic. RMAs shall correctly accommodate and process information that contains dates in current, previous, and future centuries (ISO Standard (Reference (v))). A recommended format is provided in Table C5.T6 of DoD Standard Reference (d), e.g. YYYY-MM-DD. RMA shall provide date translation from other date formats. The capability shall include, but not be limited to, century recognition, calculation, and logic that accommodate same-century and multi-century formulas and date values, and date interface values that reflect the century. RMAs shall store years in a 4-digit format. Leap year calculations shall be accommodated (e.g., 1900 is not a leap year; 2000 is a leap year).

C2.1.3. Meta -Tagging Organizational Data. RMAs shall allow for the implementation of discovery meta-tagging. Current guidance for meta-tagging DoD data can be found in the Department of Defense Discovery Metadata Specification (Reference (d)). When selecting commercial-off-the-shelf (COTS) products to support RMA requirements, selection criteria should include the feasibility and capability of the COTS products to implement and maintain DoD discovery metadata requirements. This requirement implies the capability for adding Organization-Defined metadata fields, modifying existing field labels, and mapping data fields to standard transfer format fields.

C2.1.4. Backward Compatibility. RMAs shall provide the capability to access information from their superseded repositories and databases. This capability shall support at least 1 previously verified version of backward compatibility.

C2.1.5. Accessibility. The available documentation for RMAs shall include product information that describes features that address parts 1194.21 and 1194.31 of Reference (g). For web-based applications, part 1194.22 of Reference (g) shall also apply (section 794d of title 29 USC (Reference (w))).

C.2.1.6. Extensibility. RMAs shall include the capability to provide open standards interfaces in order to integrate into an organization's information technology enterprise. This capability shall include the capability to accept and file records from producing applications and provide support to the organization's workflow.

C2.1.7. Security Compliance. RMAs shall support applicable security standards including Security Technical Implementation Guides.

C2.2. DETAILED REQUIREMENTS

C2.2.1. Implementing File Plans. RMAs shall provide the capability to:

C2.2.1.1. Allow only authorized individuals to create, edit, and delete file plan components and their identifiers. Each component identifier shall be linked to its associated component and to its higher-level component identifier(s) (part 1222.50 of Reference (g) and section 3303 of title 44 USC (Reference (x))). Table C2.T.1. identifies mandatory file plan components. The Mandatory Data Collection section indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not in the Mandatory Data Collection section, the RMA shall behave in a predictable manner as a result of queries or other operations when the fields are not populated. The Mandatory Data Structure section indicates that the field must be present and available to the user either as read/write or as read only depending upon the kind of data being stored. The Mandatory Support section indicates that the RMA shall support capability without requiring knowledge of the underlying source code, data structure, or other implementation details. The file plan components should be organized into logical sets that, when populated, shall provide all the file plan references necessary to properly annotate (file) a record.

Table C2.T1. File Plan Components

Requirement	File Plan Component	Reference/ Comment
Mandatory Data Collection		
C2.T1.1.	Record Category Name	Records Management Task Force (RMTF) Guidance (Reference (y))
C2.T1.2.	Record Category Identifier	RMTF (Reference (y)); RMAs shall ensure unique.
C2.T1.3.	Record Category Description	RMTF (Reference (y))
C2.T1.4.	Disposition Instructions	part 1228.24 of Reference (g)
C2.T1.5.	Disposition Authority	RMTF (Reference (y))
C2.T1.6.	Transfer or Accession to NARA Indicator	
C2.T1.7.	Vital Record Indicator	part 1236.20 of Reference (g)
Mandatory Data Structure		
C2.T1.8.	Vital Record Review and Update Cycle Period	part 1236.20 of Reference (g); Mandatory if vital record indicator is true.

Requirement	File Plan Component	Reference/ Comment
Mandatory Support		
C2.T1.9.	Organizational Definable Fields	Multiple organizational defined fields shall be supported.

C2.2.1.2. Allow only authorized individuals to designate the metadata fields to be constrained to selection lists. RMAs shall provide the capability for authorized individuals to create and maintain selection lists for all supported data types (e.g., drop-down lists) for metadata items that are constrained to a pre-defined set of data.

C2.2.1.3. Allow only authorized individuals to create, edit, and delete file plan metadata elements or attributes, and their associated selection lists.

C2.2.1.4. Allow only authorized individuals to select where data collection for optional metadata fields is mandatory for a given organization.

C2.2.1.5. Allow only authorized individuals to create, edit, and delete record folder components and their non-system generated identifiers. Each component identifier shall be linked to its associated component and to its higher-level file plan component identifier(s) (parts 1194.21 and 1222.50 of Reference (g)). Table C2.T2 identifies mandatory record folder components. The Mandatory Data Collection indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not in the Mandatory Data Collection column, the RMA shall behave in a predictable manner as a result of queries or other operations when the fields are not populated. The Mandatory Inheritance Support column indicates that the field must inherit data from the same field in the parent object and may be locally overwritten. The Mandatory Data Structure column indicates that the field must be present and available to the user either as read/write or as read only depending upon the kind of data being stored. The Mandatory Support column indicates that the RMA shall support capability without requiring knowledge of the underlying source code, data structure, or other implementation details. If the RMA requires the use of folders for all categories, it must be able to accommodate record-level retention schedules without requiring the user to create a folder for each record.

Table C2.T2. Record Folder Components

Requirement	File Plan Component	Reference/ Comment
Mandatory Data Collection		
C2.T2.1.	Folder Name	
C2.T2.2.	Folder Identifier	RMAs shall ensure unique.
C2.T2.3.	Location	RMTF (Reference (y)); Mandatory if the record is not in the RMA repository.
C2.T2.4.	Vital Record Indicator	part 1236.20 of Reference (g)

Requirement	File Plan Component	Reference/ Comment
Mandatory Data Structure		
C2.T2.5.	Vital Record Review and Update Cycle Period	part 1236.20 of Reference (g); Mandatory if Vital Record Indicator is true. Inheritance may be overwritten by user.
C2.T2.6.	Supplemental Marking List	Multiple supplemental marking entry selections shall be supported.
Mandatory Support		
C2.T2.7.	Organization Definable Fields	Multiple organization definable fields shall be supported.

C2.2.1.6. Allow only authorized individuals to create, edit, and delete folder metadata elements or attributes, and their associated selection lists.

C2.2.1.7. Ensure that identifiers (e.g., folder identifiers, record category identifiers) are unique so that ambiguous assignments, links, or associations cannot occur.

C2.2.1.8. Associate the attributes of file plan components to record folders and records where the records are not associated with folders.

C2.2.1.9. Provide a scripting capability to allow only authorized individuals to attach simple process actions such as alerts and notifications to any or all metadata fields or to restrict record access based on the content of fields. This scripting capability shall allow for evaluation of the contents of 2 or more fields on the same record, as well as of fields in objects linked to that record.

C2.2.1.10. Sort by a single field or multiple fields, and to view, save, and print user-selected portions of the file plan, including record folders (Reference (y)).

C2.2.2. Scheduling Records. RMAs shall provide the capability to:

C2.2.2.1. Allow only authorized individuals to create, edit, and delete retention schedule components of record categories.

C2.2.2.2. Define an unconstrained number of multiple phases (e.g., transfer to inactive on-site storage, transfer to off-site storage) within a retention schedule.

C2.2.2.3. Define parallel and interdependent phases within a retention schedule, including the capability to assign phase precedence or weight.

C2.2.2.4. Allow an authorized individual to select cutoff as the trigger to begin final disposition calculations.

C2.2.2.5. Calculate interim phases and final disposition from the trigger date selected by an authorized individual.

C2.2.2.6. Allow only authorized individuals to define the cutoff criteria and, for each life cycle phase, define the following disposition components for a record category:

C2.2.2.6.1. Retention period (e.g., fiscal year or calendar year).

C2.2.2.6.2. Disposition action (interim transfer, accession, or destroy).

C2.2.2.6.3. Location of interim transfer or accession location (if applicable).

C2.2.2.7. Schedule and reschedule records and/or record folders. Mandatory disposition types include:

C2.2.2.7.1. Time Dispositions. A cyclical process where records are eligible to enter their disposition lifecycle immediately after the conclusion of a fixed period of time following organization-defined cutoff (e.g., days, months, years).

C2.2.2.7.2. Event Dispositions. A unique event(s) process where records are eligible for disposition immediately after a specified event takes place (i.e., the event acts as cutoff and there is no retention period).

C2.2.2.7.3. Time-Event Dispositions. A unique event(s) process where the timed retention periods are triggered after a specified event takes place (i.e., the event makes the record folder eligible for closing and/or cutoff and there is a retention period).

C2.2.2.8. Allow authorized individuals to define and name disposition events. Multiple events per disposition instruction shall be supported, with 1 or more being necessary to trigger cutoff, retention and/or interim transfer actions as required by the organization. RMAs shall support recurring events.

C2.2.2.9. Automatically calculate the complete life cycle, including intermediate phases, of record folders and records not in folders (Reference (f)). RMAs shall allow an authorized individual to enter an "as-of" reference date for this calculation.

C2.2.2.10. Reschedule dispositions of record folders and/or records not in folders during any phase of their life cycle if an authorized individual changes the disposition instructions. This

requirement includes the capability to change the cutoff criteria of disposition instructions and to change the retention period(s) associated with a disposition.

C2.2.2.11. Recalculate the record life cycle based on changes to any life-cycle date and set the filing status of the folder (i.e., open, closed) according to the business rules associated with date change(s).

C2.2.3. Declaring and Filing Records

C2.2.3.1. RMAs shall provide the capability to associate the attributes of a record folder to a record. If the capability is already implemented, for categories to be managed at the record level, provide the capability to associate a record category to a record (part 1222.50 of Reference (g)).

C2.2.3.2. Table C2.T3 identifies mandatory record metadata components. The Mandatory Structure section indicates that the field shall be present and available to the user either as read/write or as read only depending upon the kind of data being stored. The Mandatory Data Collection section indicates that an RMA shall ensure population of the associated data structure with non-null values. The Mandatory Support section indicates that an RMA shall provide a capability to support creating and managing the metadata. Where data collection is not mandatory, an RMA shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.

Table C2.T3. Record Metadata Components

Requirement	Record Metadata Component	Reference/Comment
Mandatory Data Collection		
	Record Identifiers, Markings, and Indicators	
C2.T3.1.	Unique Record Identifier	RMA shall ensure unique.
	Record Descriptors	
C2.T3.2.	Subject or Title	part 1234.22 of Reference (g)
	Record Dates	
C2.T3.3.	Date Filed	RMTF (Reference (y)); System Date, not editable.
C2.T3.4.	Publication Date	part 1234.22 of Reference (g)
	Record People and Organizations	
C2.T3.5.	Author or Originator	part 1234.22 of Reference (g)
C2.T3.6.	Originating Organization	part 1234.22 of Reference (g)

Requirement	Record Metadata Component	Reference/Comment
Mandatory Data Structure		
	Record Identifiers, Markings, and Indicators	
C2.T3.7.	Supplemental Marking List	Multiple Supplemental Markings entry selections shall be supported (Director of Central Intelligence Directive (DCID) (Reference (z)), DoD Directive (Reference (aa)), DoD Regulation (Reference (ab)), DoD Directive (Reference (ac)), and DoD Regulation (Reference (ad))).
	Record Descriptors	
C2.T3.8.	Media Type	RMTF (Reference (y))
C2.T3.9.	Format	RMTF (Reference (y))
	Record Dates	
C2.T3.10.	Date Received	
	Record People and Organizations	
C2.T3.11.	Addressee(s)	Mandatory for correspondence.
C2.T3.12.	Other Addressee(s)	Mandatory for correspondence (Reference (e), part 1234.22 of Reference (g), and Reference (ad)).
	Additional Metadata	
C2.T3.13.	Location	RMTF (Reference (y))
Mandatory Support		
C2.T3.14.	Organization-Defined Fields	Multiple Organization-Defined Fields shall be supported.

C2.2.3.3. RMAs shall provide the capability for only authorized individuals to create, edit, and delete record metadata elements or attributes, and their associated pick lists. RMAs shall provide a capability for only authorized individuals to indicate whether the field is constrained to a pick list and whether users can select more than 1 item from the list.

C2.2.3.4. RMAs shall provide the capability for authorized individuals to select where data collection for optional metadata fields is mandatory for a given organization.

C2.2.3.5. RMAs shall assign a unique computer-generated record identifier for each record they manage regardless of where that record is stored (Reference (y)).

C2.2.3.6. RMAs shall provide the capability to create, view, save, and print the complete record metadata, or user-specified portions thereof, sorted and/or grouped by user preference (Reference (y)).

C2.2.3.7. RMAs shall prevent subsequent changes to electronic records stored in their supported repositories. The contents of the records, once filed, shall be preserved (part 1222.50 of Reference (g) and Reference (y)).

C2.2.3.8. RMAs shall not permit modification of the metadata fields indicated by this Standard as not editable.

C2.2.3.9. RMAs shall capture, populate, and/or provide the user with the capability to populate the metadata elements before filing the record. RMAs shall ensure that fields designated mandatory for data collection are non-null before filing the record (parts 1222.50 and 1234.22 of Reference (g)).

C2.2.3.10. For records that are being filed via the user interface, RMAs shall provide the user with the capability to edit the record metadata prior to filing the record, except for data specifically identified in this Standard as not editable. For auto-filing, RMAs shall provide the user the option of editing the record metadata prior to filing.

C2.2.3.11. Dates captured electronically shall be valid dates as defined in paragraph C2.1.2. Where data entry/capture errors are detected, RMAs shall prompt the user to correct the errors. These prompts shall provide guidance to the user in making corrective actions (e.g., "Date format incorrect - use YYYY/MM/DD.")

C2.2.3.12. RMAs shall provide the capability for only authorized individuals to define and add organization-defined metadata fields (e.g., project number, budget line) for site-specific requirements (part 1234.22 of Reference (g)).

C2.2.3.13. RMAs shall provide the capability to view, save, or print metadata, including file plan and folder metadata, associated with a specified record or set of records or user-specified portions thereof, sorted and/or grouped by user preference.

C2.2.3.14. RMAs shall provide the capability for only authorized individuals to limit the record folders and record categories presented to a user or workgroup. Based on these limits, RMAs shall present to users only those record categories or folders available to the user or workgroup for filing.

C2.2.3.15. RMAs shall provide the capability for only authorized individuals to limit the selection or pick list items presented to a user or workgroup. Based on these limits, RMAs shall present to users only selection or pick list items available to the user or workgroup for filing.

C2.2.3.16. RMAs shall provide the capability for only authorized individuals to change a record folder or record category associated with a record.

C2.2.3.17. RMAs shall provide a capability for referencing or linking and associating supporting and related records and related information, such as notes, marginalia, attachments,

and electronic mail-return receipts to a specified record. RMAs shall allow only authorized individuals to change or delete links and associations that affect disposition (Reference (y)).

C2.2.3.18. RMAs shall provide a capability for links to be labeled to indicate the type and direction of the relationship between the records. For example in a supersedes/superseded relationship, a later record supersedes an earlier one, and the earlier one was superseded by the later one, e.g. the label of the link from the later record to the earlier one should be “supersedes”, while the label of the link from the earlier record to the later one should be “superseded by”.

C2.2.3.19. RMAs shall provide a capability for linking and unlinking records both during and after the process of filing a record. RMAs shall allow only authorized individuals to remove links that affect disposition.

C2.2.3.20. RMAs shall provide a capability for authorized individuals to define, update, and assign permissions for use of organization-defined link types (Reference (y)).

C2.2.3.21. RMAs shall provide the capability to support multiple copies of a record. These shall be associated and linked. Each rendition shall be associated with its own set of metadata.

C2.2.3.22. RMAs shall provide the capability to increment versions of records when filing. RMAs shall associate and link the versions. Each version shall be associated with its own set of metadata.

C2.2.3.23. RMAs shall link the record metadata to the record so that it can be accessed for display, export, etc. (part 1234.32 of Reference (g)).

C2.2.3.24. RMAs shall provide the capability for only authorized individuals to modify the metadata of stored records. However, RMAs shall not allow the editing of metadata fields that have been specifically identified in this Standard as not editable.

C2.2.3.25. RMAs shall enforce data integrity, referential integrity, and relational integrity of the record metadata.

C2.2.3.26. RMAs shall provide the capability to automatically synchronize multiple databases and repositories.

C2.2.4. Filing Electronic Mail Messages (E-Mail). RMAs shall:

C2.2.4.1. Treat e-mail messages the same as any other record, i.e., e-mail shall be subject to all requirements of this Standard (sections 1222.32 and 1234.24 of Reference (g)).

C2.2.4.2. Capture and automatically store the transmission and receipt data identified in Table C2.T4. if available from the e-mail system, as part of the record metadata when an e-mail message is filed as a record (part 1234.24 of Reference (g)). Unless specifically overwritten by the organization, RMAs shall not allow editing of the subject, date, or time sent or received of the original e-mail record. RMAs shall provide the capability for editing all other metadata fields prior to filing. RMAs may map email transmission and receipt data to record metadata elements as described. Elements that are copied shall also be maintained separately to facilitate search, retrieval, transfer, and archival.

Table C2.T4. Transmission and Receipt Data

Transmission and Receipt Data	E-mail Record Metadata Field Name
The intelligent name, the clear, uncoded, identifications of the sender.	E-mail Sender, may be mapped to Author or Originator.
The intelligent name of all primary addressees (or distribution lists).	E-mail Addressee, may be mapped to Addressee(s).
The intelligent name of all other addressees (or distribution lists).	E-mail Other Addressee, may be mapped to Other Addressee(s).
The date and time the message was sent.	E-mail Date Sent, may be copied as Publication Date.
For messages received, the date and time the message was received (if available).	E-mail Date Received, may be mapped to Date Received.
The subject of the message.	E-mail Subject may be mapped to Subject, and optionally as Title.

C2.2.4.3. Provide user-selectable options of filing e-mail and e-mail attachments as a single record, filing selected e-mail items as individual records, or doing both. When the attachments are filed as individual records, the user shall be provided the capability to enter the metadata required in Table C2.T3. (part 1234.24 of Reference (g)).

C2.2.4.4. Not allow separate filing of Object Linking and Embedding (OLE) objects embedded in the body of the e-mail message.

C2.2.4.5. Not require users to save attachments to a hard drive or other media prior to filing them separately from the e-mail message.

C2.2.4.6. Automatically link e-mail records to their attachments when both are filed separately (part 1234.24 of Reference (g)).

C2.2.4.7. Provide graphical user interface capabilities that allow an authorized individual to map additional standard-compliant (e.g. DMS) e-mail application header fields to record metadata fields.

C2.2.5. Filing Records to be Later Transferred or Accessioned to NARA

C2.2.5.1. Table C2.T5 identifies additional metadata for records to be transferred or accessioned to NARA that are additional to previously defined metadata and are mandatory for collection.

Table C2.T5. Record Metadata Components

Requirement	Record Metadata Component	Reference/Comment
Mandatory Data Collection		
Scanned Records		
C2.T5.1.	Scanned Image Format and Version	NARA allows one of the following only; check with NARA (http://www.archives.gov/records-mgmt/initiatives/erm-products.html) for changes: Tagged Image Interchange Format (TIFF) 4.0 TIFF 5.0 TIFF 6.0 Joint Photographic Experts Group (JPEG) (all versions) Graphic Image Format (GIF) 87a GIF 89a Binary Image Interchange Format (BIIF) Portable Network Graphics (PNG) 1.0.
C2.T5.2.	Image Resolution	Image resolution relative to image encoding standard.
Portable Document Format (PDF) Records		
C2.T5.3.	Producing Application	Application used to render content to PDF.
C2.T5.4.	Producing Application Version	
C2.T5.5	PDF Version	NARA allows versions 1.0 through 1.4 only; check with NARA for changes.
Digital Photographs		
C2.T5.6	Caption	Narrative text describing each individual image in order to understand and retrieve it. Standard caption information typically includes the “who, what, when, where, why” about the photograph.
Web Records		
C2.T5.7	File Name	The file name of each web site file shall not exceed 99 ASCII characters, and with the path the name shall not exceed 254 ASCII characters.
C2.T5.8	Web Platform	Include the specific software applications and where available intended browser applications and versions.
C2.T5.9	Web Site Name	Title of the website from the main entry page.

DoD 5015.02-STD, April 25, 2007

Requirement	Record Metadata Component	Reference/Comment
C2.T5.10	Web Site Uniform Resource Locator (URL)	Include the filename of the starting page of the transferred content.
C2.T5.11	Capture Method	Include name and description of harvester used. If PDF, include the software and version used to capture the PDF. If more than 1 clearly identify which content was captured by which method.
C2.T5.12	Capture Date	Date record was captured.
C2.T5.13	Contact	Point of Contact information for person responsible for capturing the web record.
Mandatory Support		
	Scanned Records	
C2.T5.14	Image Bit Depth	Bit Depth relative to the image encoding standard.
	PDF Records	
C2.T5.15	Creating Application	Application used to create initial record content, includes version.
C2.T5.16	Document Security Settings	Additional Security added during PDF rendering.
	Digital Photographs	
C2.T5.17.	Photographer	Identify the full name (and rank, if military) and organization (agency, if Federal) of the photographer credited with the photograph, if available.
C2.T5.18.	Copyright	Indicate for each image whether there is a restriction on the use of that image because of a copyright or other intellectual property rights. Agencies must provide, if applicable, the owner of the copyright and any conditions on the use of the photograph(s), such as starting and ending dates of the restriction.
C2.T5.19.	Bit Depth	Identify the bit depth of the transferred files.
C2.T5.20.	Image Size	Specify the image height and width of each image in pixels.
C2.T5.21.	Image Source	Identify the original medium used to capture the images.
C2.T5.22.	Compression	Identify the file compression method used (if applicable) and the compression level (e.g., medium, high) selected for the image(s).
C2.T5.23.	International Color Consortium/Image Color Management (ICC/ICM) profile	Provide custom or generic color profiles, if available, for the digital camera or scanner used [e.g., standard Red Green Blue (sRGB)].
C2.T5.24.	Exchangeable Image File Format (EXIF) Information	If available, preserve and transfer to NARA the EXIF information embedded in the header of image files (as TIFF tags or JPEG markers) by certain digital cameras (e.g., make and model of the digital camera).
	Web Records	
C2.T5.25	Content Management System	Application used to manage files on the web.

C2.2.5.2. RMAs shall provide an alert or warning that all PDF records to be transferred or accessioned to NARA must include embedded fonts, which shall be verified with NARA for applicability.

C2.2.6. Storing Records. RMAs shall:

C2.2.6.1. Provide at least 1 portal that provides access to all associated repositories and databases storing electronic records and their metadata. RMAs shall, through such a portal service or through an alternate service, provide metadata compliant with the DDMS (Reference (d)).

C2.2.6.2. Prevent unauthorized access to record repositories (part 1222.50 of Reference (g) and section 3105 of title 44 USC (Reference (ae))).

C2.2.6.3. Manage and preserve any record in any supported repository, regardless of its format, structure, or naming convention, so that, when retrieved, it can be reproduced, viewed, and manipulated in the same manner as the original. RMAs shall not require file extensions or associations to desktop applications as a condition of filing records (parts 1222.50 and 1234.22 of Reference (g), and Reference (y)).

C2.2.6.4. Allow only authorized individuals to move or delete records from a repository (parts 1222.50 and 1234.28 of Reference (g)).

C2.2.6.5. Raise an alert or notification if records have been removed from a repository outside of the RMA interface (parts 1222.50 and 1234.28 of Reference (g)).

C2.2.7. Retention and Vital Records Management

C2.2.7.1. Screening Records. RMAs shall:

C2.2.7.1.1. Provide for sorting, viewing, saving, printing, identification, search, retrieval, display and archiving of record folder metadata and/or record metadata regardless of media based on any combination of record category, disposition, folder and/or record metadata including organization-defined metadata and system generated metadata.

C2.2.7.1.2. Provide for sorting, viewing, saving, and printing life cycle information, eligibility dates, and events of user-selected record folders and records.

C2.2.7.1.3. Allow the user to select and order the columns presented in screening result lists.

C2.2.7.1.4. For records and record folders with event- and time-event-driven dispositions, allow authorized individuals to indicate when the specified event has occurred.

C2.2.7.1.5. Provide for sorting, viewing, saving, and printing lists and partial lists of unscheduled record folders and/or records. Unscheduled items have no approved final disposition but may be cut off and subject to interim transfer.

C2.2.7.1.6. Allow authorized individuals the capability to enter a reference “as-of” date to support screening of future lifecycle actions.

C2.2.7.2. Closing Record Folders. RMAs shall:

C2.2.7.2.1. Allow authorized individuals to close record folders to further filing after the specified event occurs.

C2.2.7.2.2. Allow only authorized individuals to add records to a previously closed record folder and to reopen a previously closed record folder for additional public filing.

C2.2.7.3. Cutting Off Record Folders. RMAs shall provide the capability to:

C2.2.7.3.1. Implement cutoff instructions for scheduled and unscheduled record folders. RMAs shall identify record folders eligible for cutoff and present them only to the authorized individual for cutoff approval. Cutoff shall start the first disposition phase of a record or folder life cycle as controlled by the disposition instruction attached to the file plan record category or records schedule (Reference (y)).

C2.2.7.3.2. Allow only authorized individuals to add records or make other alterations to record folders that have been cut off.

C2.2.7.4. Freezing/Unfreezing Records. RMAs shall:

C2.2.7.4.1. Provide the capability for only authorized individuals to extend or suspend (freeze) the retention period of record folders or records beyond their scheduled disposition (part 1228.54 of Reference (g) and Section 2909 of title 44 USC (Reference (af))).

C2.2.7.4.2. Provide a metadata element for authorized individuals to enter the reasons for freezing a record or record folder. Freeze codes entered here should match the freeze codes used by NARA and the Federal Record Centers.

C2.2.7.4.3. Identify record folders and/or records that have been frozen and provide authorized individuals the capability to unfreeze them. Unless the records have been rescheduled

in conjunction with the freeze, RMAs shall restore unfrozen records and/or record folders to the calculated phase of their lifecycle as if they were never frozen.

C2.2.7.4.4. Allow authorized individuals to search, update, and view the reasons for freezing a record or record folder.

C2.2.7.5. Transferring Records. RMAs shall:

C2.2.7.5.1. Identify and present those record folders and records eligible for interim transfer and/or accession (References (u) and (y)).

C2.2.7.5.2. For records approved for interim transfer or accession and that are stored in the RMA's supported repositories, copy the pertinent records and associated metadata of the records and their folders to a filename, path, or device specified by a user with permissions to facilitate the transfer. For permanent records to be accessioned to NARA, the accessioning file(s) shall be made to conform to one of the formats and media specified in part 1228.270 of Reference (g) (part 1234.32 of Reference (g) and Reference (y)). (Requirement C2.2.10.5.)

C2.2.7.5.3. For records approved for accession and that are not stored in an RMA supported repository, copy the associated metadata for the records and their folders to a filename, path, or device specified by a user with permissions to facilitate the transfer. For permanent records to be accessioned to NARA, the metadata shall conform to one of the formats and media specified in part 1228.270 of Reference (g).

C2.2.7.5.4. For records approved for interim transfer or accession, allow only authorized individuals to delete the records and/or related metadata after successful transfer has been confirmed (part 1228.54 of Reference (g) and Reference (ae)). RMAs shall provide the capability to allow the organization to retain the metadata for records that were transferred or accessioned.

C2.2.7.5.5. Provide documentation of transfer activities in an electronic format that can be saved as a record.

C2.2.7.5.6. Provide the capability for bulk updating of record and folder metadata as a result of transfer actions.

C2.2.7.6. Destroying Records. RMAs shall:

C2.2.7.6.1. Identify and present to the records manager the record folders and records, including record metadata, that have met the retention period. Records assigned more than 1 disposition must be retained and linked to the record folder (category) with the longest

retention period. Links to record folders (categories) with shorter retention periods should be removed as they become due (parts 1228.58 and 1234.32 of Reference (g) and Reference (y)).

C2.2.7.6.2. Present a second confirmation requiring authorized individuals to confirm the delete command before the destruction operation is executed for records approved for destruction (References (y) and (ae)).

C2.2.7.6.3. Delete electronic records approved for destruction in a manner that prevents their physical reconstruction using commonly available file restoration utilities (part 1234.34 of Reference (g)).

C2.2.7.6.4. Provide an option allowing the organization to select whether to retain or delete the metadata of destroyed records.

C2.2.7.6.5. Restrict the records destruction commands to authorized individuals (part 1222.50 of Reference (g) and Reference (ae)).

C2.2.7.6.6. Provide documentation of destruction activities. This documentation shall be stored as records.

C2.2.7.7. Cycling Vital Records. RMAs shall provide:

C2.2.7.7.1. The capability for authorized individuals to enter the Vital Records Review and Update Cycle Period when creating or updating the file plan.

C2.2.7.7.2. The capability for authorized individuals to enter the date when the records associated with a vital records folder have been reviewed and updated.

C2.2.7.7.3. A means for identifying and aggregating vital records due for cycling.

C2.2.7.7.4. A means for identifying and aggregating vital records by previous cycle dates.

C2.2.7.7.5. A capability to allow an authorized individual to enter a reference “as-of” date to plan for future review cycles.

C2.2.7.8. Searching For and Retrieving Records. RMAs shall:

C2.2.7.8.1. Allow users to browse the records stored in the file plan based on their user access permissions.

C2.2.7.8.2. Allow searches using any combination of the record category, record and/or folder metadata elements (Reference (d) and (y)), including organization-defined and system-generated metadata.

C2.2.7.8.3. Allow the user to specify partial matches and shall allow designation of “wild card” fields or characters.

C2.2.7.8.4. Allow searches using combinations of Boolean and relational operators: “and,” “and not,” “or,” “greater than” (>), “less than” (<), “equal to” (=), “not equal to” (<>), is blank, is null, not blank, and not null and shall provide a mechanism to override the default (standard) order of precedence.

C2.2.7.8.5. Present the user a list of records and/or folders meeting the retrieval criteria, or notify the user if there are no records and/or folders meeting the retrieval criteria. RMAs shall allow the user to select and group results, and to order the columns presented in the search results list for viewing, transmitting, printing, etc. (Reference (y)).

C2.2.7.8.6. Provide to the user's workspace (filename, location, or path name specified by the user) copies of electronic records, selected from the list of records meeting the retrieval criteria, in the filing format in which they were provided to the RMA for filing (Reference (y)). RMAs shall not require that applications necessary to manipulate the records be installed on the retrieving workstation.

C2.2.7.8.7. Provide the capability for filed e-mail records to be retrieved back into a compatible e-mail application for viewing, forwarding, replying, and any other action within the capability of the e-mail application.

C2.2.7.8.8. Provide authorized users a choice of retrieving filed records to their workspace or into a compatible application for viewing, editing, and any other action within the capability of the application.

C2.2.7.8.9. When the user selects a record for retrieval, present a list of available versions. The list shall default to the latest version of the record for retrieval but allow the user to select and retrieve any version.

C2.2.7.8.10. Allow users to select any number of records, and their metadata, for retrieval from the search results list.

C2.2.7.8.11. Allow the user to abort a search.

C2.2.8. Access Controls

Table C2.T6. summarizes requirements that refer to “authorized individuals” and offers additional information regarding example user-type roles and responsibilities. In general, Application Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users. RMAs shall provide the capability to allow organizations to define roles and responsibilities to fit their records management operating procedures.

Table C2.T6. Mandatory Authorized Individual Requirements

Requirement	Application Administrator	Records Manager	Privileged User
C2.T6.1. (C2.2.1.1.) Create, edit, and delete file plan components and their identifiers.	Ensures that data structures are correctly installed and database links are in place.	Enters file plan data.	None
C2.T6.2. (C2.2.1.2) Designate the metadata fields that are to be constrained to selection lists. Create and maintain selection lists for all supported data types for metadata items that are constrained to a pre-defined set of data..	Ensure database is correctly set up and installed.	Define lists.	None
C2.T6.3. (C2.2.1.3.) Create, edit, and delete file plan metadata elements or attributes, and their associated selection lists..	Ensures that data structures are correctly installed and database links are in place.	Enters file plan data.	None
C2.T6.4. (C2.2.1.4.) Select where data collection for optional metadata fields is mandatory for a given organization.	Creates structures.	Creates and edits fields.	None
C2.T6.5. (C2.2.1.5.) Create, edit, and delete record folder components and their non-system generated identifiers.	Ensures that data structures are correctly installed and database links are in place.	Enters file plan data.	None
C2.T6.6. (C2.2.1.6.) Create, edit, and delete folder metadata elements or attributes, and their associated selection lists.	Ensures that data structures are correctly installed and database links are in place.	As necessary.	None
C2.T6.7. (C2.2.1.10) Allow attachment of simple process actions to any or all metadata fields or to restrict record access based on the content of fields.	Creates rules and connects them to fields.	Manually execute rules if necessary.	None
C2.T6.8. (C2.2.2.1) Create, edit, and delete retention schedule components of record categories.	Ensures that data structures are correctly installed and database links are in place.	Enters disposition data, enters event data, and closes folders.	Enters event data and closes folders.

Requirement	Application Administrator	Records Manager	Privileged User
C2.T6.9. (C2.2.2.4) Select cutoff as the trigger to begin final disposition calculations.	Ensures that data structure is correctly installed and database links are in place.	Enters criteria and phase information.	None
C2.T6.10. (C2.2.2.5.) Select trigger date for interim phases and final disposition calculation	None	Selects trigger date and sets up rules.	None
C2.T6.11. (C2.2.2.6.) Define the cutoff criteria and, for each life cycle phase, the following disposition components for a record category . . .	Ensures that data structure is correctly installed and database links are in place.	Enters criteria and phase information.	None
C2.T6.12. (C2.2.2.8) Defining and naming disposition events.	As necessary.	As necessary.	As necessary.
C2.T6.13. (C2.2.2.9.) Enter an “as-of” reference date for lifecycle phase calculation.	As necessary.	As necessary.	None
C2.T6.14. (C2.2.2.10) Change the disposition instructions.	None	Edits disposition information and manually executes rules necessary to reschedule.	None
C2.T6.15. (C2.2.3.3.) Create, edit, and delete record metadata elements or attributes, and their associated pick lists.	Ensures that data structure is correctly installed and database links are in place.	Creates selection lists.	Enters data (all users).
C2.T6.16. (C2.2.3.4.) Select where data collection for optional metadata fields is mandatory for a given organization.	During setup.	Advising.	None
C2.T6.17. (C2.2.3.12.) Define and add organization-defined metadata fields (e.g., project number, budget line) for site-specific requirements.	During setup.	Advising.	None
C2.T6.18. (C2.2.3.14.) Limit the record folders and record categories presented to a user or workgroup.	Record categories during setup.	Record folders.	Record folders.
C2.T6.19. (C2.2.3.15.) Limit the selection or pick list items presented to a user or workgroup.	During setup.	As necessary.	None
C2.T6.20. (C2.2.3.16) Change a record folder or record category associated with a record.	As necessary.	As necessary.	None
C2.T6.21. (C2.2.3.17.) Change or delete links and associations.	Database is correctly installed and configured.	Change links as necessary.	None
C2.T6.22. (C2.2.3.19.) Remove links that affect disposition.	As necessary.	As necessary.	As necessary.
C2.T6.23. (C2.2.3.20.) Define, update, and assign permissions for use of organization-defined link types	During setup.	As necessary.	None
C2.T6.24. (C2.2.3.24.) Modify the metadata of stored records.	As necessary.	Change data as necessary.	Change data as necessary.

Requirement	Application Administrator	Records Manager	Privileged User
C2.T6.25. (C2.2.4.7.) Map additional standard-compliant (e.g. Defense Messaging Service (DMS)) e-mail application header fields to record metadata fields.	During setup.	As necessary.	None
C2.T6.26. (C2.2.6.4.) Move or delete records from the repository.	As necessary.	As necessary.	None
C2.T6.27. (C2.2.7.1.4.) Indicate when the specified event has occurred for records and record folders with event and time-event driven dispositions.	Database setup.	Link dispositions to record categories.	Enter event information.
C2.T6.28. (C2.2.7.1.6.) Enter a reference “as-of” date to support screening of future lifecycle actions.	As necessary.	As necessary.	None
C2.T6.29. (C2.2.7.2.1.) Close record folders to further filing after the specified event occurs.	As necessary.	As necessary.	As necessary.
C2.T6.30. (C2.2.7.2.2.) Add records to a previously closed record folder or to reopen a previously closed record folder for additional public filing.	As necessary.	As necessary.	As necessary.
C2.T6.31. (C2.2.7.3.1.) Approve cutoff.	As necessary.	Routine work.	None
C2.T6.32. (C2.2.7.3.2.) Add records or make other alterations to record folders that have been cut off.	Database support.	Enters limits.	None
C2.T6.33. (C2.2.7.4.1.) Extend or suspend (freeze) the retention period of record folders or records beyond their scheduled disposition.	Database and business rules.	Freezing/unfreezing.	None
C2.T6.34. (C2.2.7.4.2.) Enter the reasons for freezing a record or record folder.	Database and business rules.	Freezing/unfreezing.	None
C2.T6.35. (C2.2.7.4.3.) Unfreeze capability.	Database and business rules.	Freezing/unfreezing.	None
C2.T6.36. (C2.2.7.4.4.) Search, update, and view the reasons for freezing a record or record folder.	Database and business rules.	Freezing/unfreezing.	None
C2.T6.37. (C2.2.7.5.4.) Delete the records and/or related metadata after successful transfer has been confirmed.	As necessary.	As necessary.	None
C2.T6.38. (C2.2.7.6.2) Confirm the delete command, before the destruction operation is executed.	As necessary.	As necessary.	None
C2.T6.39. (C2.2.7.6.5.) Access to records destruction commands.	As necessary.	As necessary.	None
C2.T6.40. (C2.2.7.7.1) Enter the Vital Records Review and Update Cycle Period when creating or updating the file plan.	Ensure database structure is adequate and correctly installed.	Enters cycling data.	None

Requirement	Application Administrator	Records Manager	Privileged User
C2.T6.41. (C2.2.7.7.2.) RMAs shall provide the capability for authorized individuals to enter the date when the records associated with a vital records folder have been reviewed and updated.	Ensure database structure is adequate and correctly installed.	Enters cycling data.	Cycles and updates records.
C2.T6.42. (C2.2.7.7.5.) Enter a reference “as-of” date to plan for future review cycles.	As necessary.	As necessary.	As necessary.
C2.T6.43. (C2.2.8.1.) Edit the roles defined in this Standard and to create and maintain user-defined roles.	As necessary.	As necessary.	None
C2.T6.44. (C2.2.8.3.) Allow access to the RMA.	As necessary.	As necessary.	None
C2.T6.45. (C2.2.8.3.2.) Define the minimum length of the Password field.	Define minimum length.	None	None
C2.T6.46. (C2.2.9.2.) Determine which of the objects and specified actions listed in subparagraph C2.2.9.1. are audited.	Manage audits.	None	None
C2.T6.47. (C2.2.9.3.1) Set up specialized reports to determine what level of access a user has and to track a user’s actions over a specified time period.	Create reports.	None	None
C2.T6.48. (C2.2.9.3.2.) Set up specialized reports to facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service.	Create reports.	None	Create reports, if security officer.
C2.T6.49. (C2.2.9.5) Export and/or backup and remove audit files from the system.	Export and/or backup and remove audit files.	File audit logs as records.	None
C2.T6.50. (C2.2.10.3.) Map producing system standard and organization-defined metadata to RMA standard or organization-defined metadata fields.	Database setup.	During export/import.	None
C2.T6.51. Authorize transfer of records to NARA.	As necessary.	As necessary.	As necessary.

C2.2.8.1. RMAs shall provide a graphical user interface capability to authorized individuals to edit the roles defined in this Standard and to create and maintain organization-defined roles.

C2.2.8.2. Upon installation, RMAs shall require that the default password for the super user or Application Administrator be changed from the default.

C2.2.8.3. RMAs, in conjunction with their operating environment, shall use identification and authentication measures that allow only authorized individuals access to the RMA. At a minimum, an RMA shall implement identification and authentication measures that require the following (References (e) and Executive Order (Reference (ag))).

C2.2.8.3.1. User ID.

C2.2.8.3.2. Password. RMAs shall provide the capability for authorized individuals to define the minimum length of the password field.

C2.2.8.3.3. Alternative Methods. Other methods of access control (e.g., Biometrics, CAC, or PKI) in lieu of or in conjunction with the above are acceptable. If used in lieu of, the alternative must provide at least as much security.

C2.2.8.4. RMAs shall provide the capability for only individuals with Application Administrator access to authorize access capabilities to any combination of the items identified in Table C2.T5. to individuals and to groups.

C2.2.8.5. RMAs shall provide the capability to define different groups of users with different access privileges. RMAs shall control access to file plan components, record folders, and records based on group membership as well as user account information. At a minimum, access shall be restricted to appropriate portions of the file plan for purposes of filing and/or searching/retrieving (part 1234.28 of Reference (g) and Reference (y)).

C2.2.8.6. RMAs shall provide a web user interface, as a minimum, for filing, and search and retrieval of records. This shall provide a minimum of 128-bit encryption and be PK-enabled, as well as provide all the mandatory access controls.

C2.2.8.7. RMAs shall support simultaneous multiple-user access to all RMA components including the metadata and the records.

C2.2.9. System Audits

C2.2.9.1. RMAs in conjunction with their operating environments, shall provide an audit capability to log the actions, date, time, unique object identifier(s) and user identifier(s) for actions performed on the following RMA objects:

C2.2.9.1.1. User accounts.

C2.2.9.1.2. User groups.

C2.2.9.1.3. Records and record folders.

C2.2.9.1.4. Associated metadata elements.

C2.2.9.1.5. File plan components.

C2.2.9.2. The audit actions include retrieving, creating, deleting, searching, and editing actions (Reference (e)). RMAs shall provide a capability for only authorized individuals to determine which of the objects and specified actions listed in subparagraph C2.2.9.1. are audited (Reference (e)).

C2.2.9.3. RMAs, in conjunction with their operating environment, shall provide audit analysis functionality whereby an authorized individual can set up specialized reports to:

C2.2.9.3.1. Determine what level of access a user has and to track a user's actions over a specified time period. These are the specified actions listed in subparagraph C2.2.9.1 (References (e) and (y)).

C2.2.9.3.2. Facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service.

C2.2.9.4. RMAs shall provide the capability to file the audit data as a record (Reference (y)).

C2.2.9.5. RMAs, in conjunction with their operating environment, shall allow only authorized individuals to export and/or backup and remove audit files from the system.

C2.2.9.6. RMAs, in conjunction with their operating environment, shall not allow audit logs to be edited.

C2.2.10. Product Combinations. Product combinations that are the result of integrating two or more distinct products, where typically one product primarily creates records and another product performs the records' retention schedule tracking, shall meet the following requirements. For clarity, the product that creates records is referred to as a "producing system" throughout this Standard.

C2.2.10.1. Preventing Naming Conflicts. If the producing system maintains metadata with a name specified by this Standard, the content and context of the metadata shall meet the content and context criteria of this Standard.

C2.2.10.2. Metadata Mapping Defaults. Metadata specifically named in this Standard shall be mapped to like-named metadata in the RMAs by default.

C2.2.10.3. Metadata Mapping Management. Product combinations shall provide a graphical user interface capability for an authorized individual or an automated method to map producing system standards and organization-defined metadata to RMA standard or organization-defined metadata fields.

C2.2.10.4. Data Collection Management. Product combinations shall manage metadata such that users shall enter information only once per record.

C2.2.10.5. Metadata Synchronization and Integrity. If metadata is kept in multiple locations, product combinations shall ensure metadata is synchronized across all locations within 5 minutes of being changed in any location.

C2.2.10.6. Filing Support. Product combinations shall provide a single user interface that supports all filing operations including establishing links and/or references among records.

C2.2.10.7. Search and Retrieval. Product combinations shall allow users to search and retrieve records from the same interface used to file them. (e.g., the user shall not have to open a separate records application interface to search for records if that user was able to file directly from a producing system.)

C2.2.10.8. Permissions Management. Product combinations shall automatically incorporate or coordinate user permissions in the RMA component of the producing system. The RMA component permissions shall take precedence for all records.

C2.2.10.9. Permissions Synchronization. Product combinations shall synchronize user permissions among the associated components when multiple copies of the permissions are maintained.

C2.2.11. System Management Requirements. The following functions are typically provided by the operating system or by a database management system. These functions are also considered requirements to ensure the integrity and protection of organizational records. They shall be implemented as part of the overall records management system even though they may be performed externally to an RMA.

C2.2.11.1. Backup of Stored Records. An RMA system shall provide the capability to automatically create backup or redundant copies of the records and their metadata (part 1234.28 of Reference (g), References (y) and (ad)). An RMA backup capability shall ensure synchronization between all record category, file plan, folder, record metadata, and content repositories.

C2.2.11.2. Storage of Backup Copies. The method used to back up RMA database files shall provide copies of the records and their metadata that can be stored off-line and at separate location(s) to safeguard against loss due to system failure, operator error, natural disaster, or willful destruction (part 1234.30 of Reference (g)).

C2.2.11.3. Data Integrity and Disaster Recovery Capability. Following any system failure, the backup and recovery procedures provided by the system shall:

C2.2.11.3.1. Ensure integrity of data by providing the capability to do system evaluation, data validation and data integrity checks.

C2.2.11.3.2. Ensure any full updates are reflected in RMA files, and that any partial updates to RMA files are separately identified. Also, any user whose updates are incompletely recovered, shall, upon next use of the application, be notified that a recovery has been attempted. RMAs shall also provide the option to continue processing using all in-progress data not reflected in RMA files (part 1234.28 of Reference (g) and Reference (y)).

C2.2.11.4. Rebuild Capability. The system shall provide the capability to rebuild from any backup copy, using the backup copy and all subsequent system audit trails (Reference (y)).

C2.2.11.5. Storage Availability and Monitoring. The system shall provide for the monitoring of available storage space. The storage statistics shall provide a detailed accounting of the amount of storage consumed by RMA processes, data, and records. The system shall notify individuals of the need for corrective action in the event of critically low storage space (Reference (y)).

C2.2.11.6. Safeguarding. The RMA, in conjunction with its operating environment, shall have the capability to activate a keyboard lockout feature and a screen-blanking feature (Reference (e)).

C2.2.12. Additional Baseline Requirements. Following are records management requirements that shall be implemented by the organization, but not necessarily by RMAs.

C2.2.12.1. Electronic Calendars and Task Lists. Some electronic systems provide calendars and task lists for users. These may meet NARA's definition of a record (Reference (i)). Calendars and task lists that meet the definition of records shall be managed as any other record. If the RMA being acquired does not have the capability to extract calendars and task lists from the software application that generates them, the user organization shall implement processes or procedures to enable the RMA to manage those records.

C2.2.12.2. External E-mail. Some organizations use separate e-mail systems for Internet e-mail or other wide-area network e-mail. These records shall be handled as any other e-mail records. If the RMA being acquired does not provide the capabilities specified in paragraph C2.2.3, the user organization shall implement processes or procedures to enable the RMA to manage these records (part 1234.24 of Reference (g)).

C2.2.12.3. Ability to Read and Process Records. Since RMAs are prohibited from altering the format of stored records (subparagraph C2.2.3.8.), the organization shall ensure that it has the ability to view, copy, print, and, if appropriate, process any record stored in RMAs for as long as that record must be retained. The organization may meet this requirement by any of the following means:

C2.2.12.3.1. Maintaining the hardware and software used to create or capture the record.

C2.2.12.3.2. Maintaining hardware and software capable of viewing the record in its native format.

C2.2.12.3.3. Ensuring backward compatibility when hardware and software is updated.

C2.2.12.3.4. Migrating the record to a new format before the old format becomes obsolete. Any migration shall be pre-planned and controlled to ensure continued reliability of the record (part 1234.30 of Reference (g)).

C2.2.12.4. Distribution Lists. If the RMA is unable to access and store e-mail distribution lists from the e-mail server, the organization shall implement procedures to extract and store them as records, but reliably linked to the original e-mail.

C2.2.12.5. Accessioning Records to NARA. When accessioning records and metadata to NARA, if conforming to formats and media specified in part 1228.270 of Reference (g) causes a violation of the records' authenticity and/or integrity (e.g. record formats that are dependent on specific hardware or software) , the organization shall contact NARA for guidance.

C2.2.12.6. Applying Records Retention Schedule to Backup Copies. The using organization shall schedule the backup copies and recycle or destroy the medium in accordance with the retention schedule.

C3. CHAPTER 3MANAGEMENT OF CLASSIFIED RECORDSC3.1. MANAGEMENT REQUIREMENTS OF CLASSIFIED RECORDS

The following requirements address the management of classified records. As such, these requirements are only mandatory for those RMAs that manage classified records. These requirements are in addition to those requirements outlined in Chapter 2. In this chapter, the word “shall” identifies mandatory system standards for vendors who support the management of classified records. The word “should” identifies design objectives that are desirable but not mandatory for supporting classified records management. Additionally, requirements for safeguarding and providing security for classified records are not in the scope of this document, since they are provided in other more applicable directives and regulations.

C3.1.1. Mandatory Metadata Fields for Classified Records. RMAs shall provide a capability by which a user can add metadata that describes a classified record. These metadata elements are shown in Table C3.T1. (References (e), (ag), and part 2001 of Title 32 CFR (Reference (ah))). Mandatory Data Collection indicates that RMAs shall ensure population of the associated data structure with non-null values. Conditional Data Collection indicates that RMAs shall check values in interdependent fields and require population as described. Mandatory Data Support indicates that RMAs shall provide a capability to support creating and managing the metadata. Where data collection is not mandatory, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.

Table C3.T1. Classified Record Components

Requirement	Classified Record Component	Reference/ Comment
Mandatory Data Collection		
C3.T1.1.	Initial Classification	Sections 1.2 and 1.6a(1) of Reference (e) and part 2001.21 (b) of Reference (ah). Application should be capable of using markings as listed in CAPCO Register (Reference (ai)) as applicable.
C3.T1.2.	Current Classification	Sections 1.2 and 1.6a(1) of Reference (e) and part 2001.21 (b) of Reference (ah). Application should be capable of using markings as listed in Reference (ai) as applicable.
Conditional Data Collection		
C3.T1.3.	Reason(s) For Classification	Sections 1.4 and 1.6a(5) of Reference (e), Reference (ad), and parts 2001.21 (a)(3) and 2001.22(c) of Reference (ah). Mandatory only when “Classified By” is not blank or null.

Requirement	Classified Record Component	Reference/ Comment
C3.T1.4.	Classified By (also called classification authority)	Sections 1.3 and Sec. 1.6a(2) of Reference (e) and section 2001.21(a)(1) of Reference (ah). Mandatory if Derived From field is blank or null.
C3.T1.5.	Classifying Agency	
C3.T1.6.	Derived From	Sections 2.1 and 2.2 of Reference (e) and sections 2001.22(a)(2) and (b) of Reference (ah). Mandatory if Classified By field is blank or null.
C3.T1.7.	Declassify On	Sections 1.5 and 1.6(a)(4) of Reference (e) and sections 2001.21(a)(4), (d), (e) and 2001.22(d) of Reference (ah). Mandatory for all but restricted data or formerly restricted data. The declassify trigger can be a date, an event, an exemption category and date, or a combination of dates or events.
Mandatory Data Support		
C3.T1.8.	Downgrade On	Section 6.1(s) of Reference (e), Reference (ad), and section 2001.32 (b) (4)(ii) of Reference (ah). The downgrade trigger can be a date, an event, or a combination of dates or events.
C3.T1.9.	Downgrade Instructions	Mandatory if Downgrade On is populated.
C3.T1.10.	Reviewed On	Sections 3.4 and 3.5 of Reference (e) and sections 2001.31 and 2001.33 of Reference (ah).
C3.T1.11.	Reviewed By	Mandatory if Reviewed On is populated.
C3.T1.12.	Downgraded On	Section 2001.24 of Reference (ah).
C3.T1.13.	Downgraded By	Mandatory if Downgrade On is populated.
C3.T1.14.	Declassified On	Part 3 of Reference (e) and section 2001.24 of Reference (ah).
C3.T1.15.	Declassified By	Mandatory if Declassified On is populated.
C3.T1.16.	Upgraded On	
C3.T1.17.	Reason(s) for Upgrade	Mandatory if Upgraded On is populated.
C3.T1.18.	Upgraded By	Mandatory if Upgraded On is populated.

C3.1.2. Initial Classification. RMAs shall provide a capability by which a user can select and/or edit the Initial Classification prior to or after filing.

C3.1.3. Current Classification. RMAs shall provide a capability by which a user can select and/or edit the Current Classification prior to filing.

C3.1.4. Originally Classified Records. RMAs shall require that when the “Derived From” field is not completed, the “Classified By” and “Reason(s) for Classification” fields must be completed (part I, section 1.7 of Reference (e)).

C3.1.5. Derivatively Classified Records. RMAs shall provide 1 or more fields to indicate when records have been derivatively classified. These fields shall support entering 1 or more of the following:

C3.1.5.1. Multiple sources.

C3.1.5.2. Title(s) of classification guide(s).

C3.1.5.3. The title, publication date, and originating organization of the source document(s) (section 2001.22 of Reference (ah)).

C3.1.6. Multiple Derivative Sources. When the user enters “Multiple Sources” in the “Derived From” fields, RMAs shall provide the capability to enter the title, date, and originating organization for each source (section 2.2 (b) of Reference (e) and section 2001.22 of Reference (ah)).

C3.1.7. Declassify On Event. When “Event” is selected in the “Declassify On” field, RMAs shall prompt the user to enter text that describes the declassification event.

C3.1.8. Declassify On Time Frame. When a date is inserted in the “Declassify On” field, RMAs shall verify that the date is no more than the mandated period of time from the Publication Date. If that time frame is exceeded, an alert shall be presented to the user. (section 1.6 (4) of Reference (e)).

C3.1.8.1. Maintaining the Declassify On Time Frame. RMAs shall provide the capability for authorized individuals to establish and maintain the period of time used to verify the dates in the “Declassify On” fields, both to make the classification period more restrictive or to accommodate changes to the mandatory classification period (section 1.6 (4) of Reference (e)).

C3.1.8.2. Updating Declassify On when Time Frame is Updated. Upon request of an authorized individual, RMAs shall automatically calculate a new declassify on date for all records that were marked with the automatic declassification date. (These are records that had a declassify date calculated from the Declassify On time frame.) RMAs shall allow authorized users to update declassification dates whether manually or automatically calculated.

C3.1.9. Storing Declassified Records. RMAs shall provide a capability to automatically transfer and expunge declassified records from the classified repository upon direction by an authorized individual or set up during initial configuration. RMAs shall allow the authorized individual to indicate whether the record metadata and history shall be retained annotated with the new location of the declassified record in an unclassified repository.

C3.1.10. Classification Guides. RMAs shall provide a capability that allows an authorized individual to input and manage multiple classification guides. Each guide record or object shall include the title, date, and originating organization, which shall be populated into an appropriate

“Derived From” field when a user selects a guide (Reference (ae)). RMAs shall provide the capability to allow the user to select topics from 1 or more classification guides.

C3.1.11. Mapping Classification Guide Fields. RMAs shall provide a capability to allow only an authorized individual to map the fields of a classification guide to the record metadata fields that they should automatically populate, when a user selects a topic. By default, RMAs shall automatically populate the following fields, which shall be editable prior to filing:

C3.1.11.1. Initial and Current Classification (if available from the guide).

C3.1.11.2. Supplemental Markings (if available from the guide) (section 2001.15 (b)(7) of Reference (ah)).

C3.1.11.3. Declassify On (if available from the guide).

C3.1.12. Confirming Accuracy Prior to Filing. RMAs shall provide the capability to confirm the accuracy of all user editable metadata items prior to filing.

C3.1.13. Editing Records. RMAs shall allow only authorized individuals to edit metadata items after a record has been filed.

C3.1.14. Current Classification. When the entry in the “Current Classification” field is changed, RMAs shall ensure that the “Upgraded On,” “Downgraded On,” or “Declassified On” field, whichever is appropriate, is populated with an appropriate date (Part 3 of Reference (e)).

C3.1.15. Exemption Categories. RMAs shall provide the capability for an authorized individual to enter or update exemption category(ies) in the “Declassify On” field and optionally enter a declassify on date or event that surpasses the declassify on timeframe (Section 3.4 (b) of Reference (e) and section 2001.21 (e) of Reference (ah)).

C3.1.16. Record History Audit. RMAs shall capture and link an audit history of each record by capturing the replaced metadata value and the identity of the person who entered that value, and appending them to a record audit history file. The metadata fields to be captured shall be authorized individual selectable. The record history audit shall be included with the other record metadata when transferring or accessioning records (Part 3 of Reference (e) and section 2001.21 (e) of Reference (ah)).

C3.1.17. Using the Record History Audit. The RMA shall provide the capability to view, copy, save, and print the record history audit based on user permissions; shall not allow the editing of the record history audit; and shall provide the capability for only authorized individuals to delete the record history audit if it has been filed as record.

C3.1.18. Marking Search and Screening Results Lists Printouts and Displays. Current Classification shall always be the leftmost column in any results list and shall not be movable (section 2001.20 of Reference (ah)).

C3.1.19. Access Conflicts. RMAs in conjunction with its operating environment, shall ensure that if there is a conflict between the individual's access criteria and the access criteria of the group(s) assigned, the individual's access criteria shall take precedence (Part 4 of Reference (e)).

C3.1.20. Searching Classified Records. RMAs shall provide a mechanism whereby users can search for records based on metadata contained in Table C3.T1.

C3.1.21. Restricting Access. RMAs shall provide a capability whereby authorized individuals may restrict access to records and their metadata based on access criteria. In addition to baseline access restriction capabilities, these additional criteria include (Part 4 of Reference (e)).

C3.1.21.1. Current Classification (subparagraph C3.T1.2.).

C3.1.21.2. Supplemental Marking List (subparagraph C2.T2.6.).

C3.1.21.3. Metadata Elements identified by the organization to be used for access control.

C3.1.22. Access Control. Table C3.T2. summarizes requirements that refer to “authorized individuals” and offers additional information regarding user-type responsibilities. In general, Application Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users.

Table C3.T2. Classified Records Authorized Individual Requirements

Requirement	Application Administrator	Records Manager	Privileged User
C3.T2.1. (C3.1.8.1) <u>Maintaining the Declassify On Time Frame.</u> ...establish and maintain the period of time used to verify the dates in the “Declassify On” fields,	Database installed and properly set up. Enter and maintain data.	None	None
C3.T2.2. (C3.1.8.2.) <u>Updating Declassify On when Time Frame is updated.</u> Upon request of an authorized individual, the RMA shall automatically calculate a new declassify on date	None	Request	Request
C3.T2.3. (C3.1.9.) <u>Storing Declassified Records.</u> ... automatically transfer and expunge declassified records from the classified repository upon direction by an authorized individual or set up during initial configuration. ... indicate whether the record metadata and history shall be retained annotated with the new location of the declassified record, in an unclassified repository.	During setup.	Direction	None
C3.T2.4. (C3.1.10.) <u>Classification Guides.</u> ... input and manage multiple classification guides. ... select topics from 1 or more classification guides.	Database installed and properly set up.	None	Enter and maintain data (security person).
C3.T2.5. (C3.1.11.) ... map the fields of a classification guide to the record metadata fields ...	Database installed and properly set up.	Map	None
C3.T2.6. (C3.1.13.) ... edit metadata items after a record has been filed.	As necessary.	As necessary.	As necessary (downgrading and reclassification, etc.).
C3.T2.7. (C3.1.15.) Enter or update exemption category(ies) in the “Declassify On” field.	Database installed and properly set up.	None	Enter and maintain data (security person).
C3.T2.8. (C3.1.16.) Select which metadata fields to capture.	As necessary.	As necessary.	None
C3.T2.9. (C3.1.17.) Delete the record history audit after filing as a record.	As necessary.	As necessary.	None
C3.T2.10. (C3.1.21.) ... restrict access to records and their metadata based on access criteria.	User accounts, access control lists and databases properly set up.	None	None
C3.T2.11. (C3.2.1.) (Optional) Determine which metadata fields require classification for a given organization.	Database and business rules properly defined, installed and set up.	None	None

C3.1.23. Classified National Security Information Not Declared as Records

C3.1.23.1. Software applications handling working papers that contain classified national security information shall provide the capability for metadata to be entered and linked to the document as follows:

C3.1.23.1.1. Working Paper Indicator.

C3.1.23.1.2. Security Classification Level/Current Classification.

C3.1.23.1.3. Title.

C3.1.23.1.4. Creation Date.

C3.1.23.1.5. Creator.

C3.1.23.2. Software applications handling working papers that contain classified national security information shall provide the capability for users to search on the working paper indicator. The search metadata should be compliant with the DDMS (Reference (d)).

C3.1.23.3. Software applications handling classified national security information that do not qualify as working papers, even if not declared as records, shall satisfy all the mandatory requirements of Chapter 3 of this Standard.

C3.1.23.4. Software applications shall provide the capability for user-selected working papers to satisfy paragraph C3.1.21.3.

C3.1.23.5. Software applications shall satisfy paragraph C3.1.19 for all classified national security information.

C3.1.24. Tracking Recipients of Classified Records. RMAs shall provide capabilities to assist organizations in tracking recipients or holders of classified information sent from or copied out of the RMA (section 2001.13 of Reference (ah)).

C3.2. OPTIONAL SECURITY FEATURES

C3.2.1. Field-level Classification. RMAs should provide the capability to allow an authorized individual to classify individual metadata fields. "Field level classifications" apply to those selected fields as defined in Table C3.T1.

C3.2.2. Marking Printouts and Displays. Current classification, reasons for classification, and downgrading instructions should be required metadata items for displays, printouts, reports, queries, review lists, etc. when organizations implement classification restrictions on individual-selected metadata fields. The highest classification level shall be displayed (in the header and footer of the printout) when aggregate results are displayed (section 2001.20 of Reference (ah)).

C3.2.3. Redacted Version Notification. Where appropriate, RMAs should have the capability to inform the user that a redacted version is available in an open repository.

C3.2.4. Populating “Reasons for Classification” from the Guide. RMAs should provide the capability for the “Reasons for Classification” to be appropriately automatically populated (if available) when a topic from a classification guide is selected.

C3.3. PRODUCT COMBINATIONS

RMAs should interact with auto-classifiers, tools for downgrading and declassifying, and other tools that support the creation of classified records. When RMAs are integrated with or use services of these tools, the tools should automatically pass record metadata from the creating environment to the appropriate RMA record metadata fields as mapped by the organization.

C4. CHAPTER 4MANAGING RECORDS FOR PRIVACY ACT AND
FREEDOM OF INFORMATION ACTC4.1. MANAGEMENT OF PRIVACY ACT RECORDS

The following requirements address RMAs that support managing records stored in systems of records (SORs). As such, these requirements are mandatory for only those RMAs that host SORs. These requirements are in addition to those requirements outlined in Chapters 2 and 3. In this chapter, the word “shall” identifies mandatory system standards for managing SOR records. The word “should” identifies design objectives that are desirable but not mandatory. Additionally, requirements for safeguarding and providing security for SOR records are not in the scope of this document, since they are provided in other more applicable directives and regulations.

C4.1.1. System of Records Notifications. RMAs shall provide functionality that supports authorized personnel in preparing and posting System of Records Notices (SORNs) to the Federal Register.

C4.1.1.1. System of Record Notice Metadata. At a minimum, RMAs shall link the SORN metadata components specified in Table C4.T1. to the SORN record (section 552a (e)(4) of Reference (aj) and section C6.3 of Reference (ak)).

Table C4.T1. System of Record Components

Requirement	System of Record Component	Reference/ Comment
Mandatory Data Collection		
Notice Record		
C4.T1.1.	System Identification	Section 552a (e)(4a) of Reference (aj) and sections C6.3, C6.3.1.1.1, and C6.3.2 of Reference (ak). Limited to 21 alphanumeric characters for DoD systems.
C4.T1.2.	System Name	Section 552a (e)(4a) of Reference (aj) and sections C6.3, C6.3.1.1.2, and C6.3.3 of Reference (ak). Limited to 55 alphanumeric characters for DoD systems.
C4.T1.3.	Responsible Official	Section 552a (e)(4f) of Reference (aj) and sections C6.3, C6.3.1.1.10, and C6.3.10 of Reference (ak). Title and business address of responsible agency official.
C4.T1.4.	System Location	Section 552a (e)(4a) of Reference (aj) and sections C6.3, C6.3.1.1.3, and C6.3.4 of Reference

Requirement	System of Record Component	Reference/ Comment
		(ak). Addresses (repeating field) of each location where the system or segment of the system is maintained. Classified addresses are not listed, but the fact that they are classified is indicated.
C4.T1.5.	Category of Individuals	Section 552a (e)(4b) of Reference (aj) and sections C6.3, C6.3.1.1.5, of C6.3.5 of Reference (ak). Discussion that includes specific categories of individuals to whom records pertain.
C4.T1.6.	Category of Records	Section 552a (e)(4b) of Reference (aj) and sections C6.3, C6.3.1.1.5, and C6.3.6 of Reference (ak). Clear description of the types of records maintained in the system.
C4.T1.7.	Authority	Section 552a. (e)(3a) of Reference (aj) and sections C6.3, C6.3.1.1.6, and C6.3.7 of Reference (ak). Links to authority records. Could be a repeating field.
C4.T1.8.	Routine Uses	Section 552a. (e)(3a) of Reference (aj) and sections C6.3, C6.3.1.1.8, and C6.3.9 of Reference (ak). Information for how the information shall be used. Blanket uses include Law Enforcement, Disclosure when Requesting Information, Congressional Inquiries, Private Relief Legislation, Disclosure Required by International Agreements, Disclosure to State and Local Taxing Authorities, and Disclosure to the Office of Personnel Management. This list may be supplemented by specific routine use information.
C4.T1.9.	Rules	Sections 552a (e)(4e, f, g, h) of Reference (aj) and sections C6.3, C6.3.1.1.12, and C6.3.22 of Reference (ak). The name of the documentation providing the access rules for this SOR.
	Administrative Data	
C4.T1.10.	NID	The unique identifier for this notice.
C4.T1.11.	NType	One of: New, Alteration, Amendment, Deletion.
C4.T1.12.	NPosting	Indicates the date and volume of the Federal Register.
C4.T1.13.	NDate	The date this notice was published in the Federal Register.
C4.T1.14.	NComments	Any comments documenting unique circumstances of this notice.
C4.T1.15.	Preparer	The author or preparer of this SORN.
	ReleasedBy	The name of the person responsible for ensuring publication of the SORN.

Requirement	System of Record Component	Reference/ Comment
Conditional Data Collection		
C4.T1.16.	Purpose of System	Section 552a (e)(3a) of Reference (aj) and sections C6.3, C6.3.1.1.7, and C6.3.8 of Reference (ak). Discussion of the system purpose. Mandatory for new system.
C4.T1.17.	Nature of Last Change (Alteration or Amendment)	Discussion of the changes to the purpose and/or use of the system. Includes deletion. Mandatory for altered systems.
C4.T1.18.	Exemptions	Sections 552a (j, k) of Reference (aj) and sections C6.3, C6.3.1.1.15, and C6.3.15 of Reference (ak). Classified materials are covered by a blanket exemption under Section K (1) of the Privacy Act of 1974. Mandatory if exemptions apply.
C3.T1.19.	Matching Programs	Links to matching program records or descriptions. Mandatory if SOR participates in 1 or more matching program.
Mandatory Data Structure		
C4.T1.20.	Notices	Section 552a (e)(4) of Reference (aj) and Sections C6.3, C6.3.1.1.11, and C6.3.11 of Reference (ak). Link to/from notices about this SOR.
C4.T1.21.	Information Collection	Identify or link to the form(s) used to collect the personal information stored in this system of records.
Mandatory Support		
C4.T1.22.	Organization-Defined Fields	

C4.1.1.2. System of Record Notice Preparation. RMAs shall provide interfaces with common office applications or document management systems to support the drafting of the SORN and rules documents. RMAs shall collect pertinent metadata from the office application or document management system file properties/metadata to pre-populate metadata elements to the degree possible (section 552a (e)(4) of Reference (aj) and section C6.3 of Reference (ak)).

C4.1.2. Privacy Case Files. RMAs shall provide authorized individuals the capability to create and manage Privacy Case Files (section C3.3.16 of Reference (ak)).

C4.1.2.1. Privacy Case File Metadata. At a minimum, RMAs shall capture Privacy Act file metadata as specified in Table C4.T2. (section C3.3.16 of Reference (ak)).

Table C4.T2. Privacy Act File Components

Requirement	Privacy Act File Component	Reference/ Comment
Mandatory Data Collection		
C4.T2.1.	FileID	Section 552a (e)(4a) of Reference (aj) and Sections C6.3, C6.3.1.1.1, and C6.3.2 of Reference (ak). Limited to 21 alphanumeric characters for DoD systems.
C4.T2.2.	FileName	Section 552a (e)(4a) of Reference (aj) and Sections C6.3, C6.3.1.1.2, and C6.3.3 of Reference (ak). Limited to 55 alphanumeric characters for DoD systems.
Mandatory Support		
C4.T2.3.	Organization-Defined Fields	

C4.1.2.2. Privacy Case File Links. RMAs shall link to or copy into Privacy Case files the following:

- C4.1.2.2.1. Requests for amendment or access.
- C4.1.2.2.2. Access Grant or Denial Records.
- C4.1.2.2.3. Appeals Records.
- C4.1.2.2.4. Appeal Response Records.
- C4.1.2.2.5. Amended Records.
- C4.1.2.2.6. Disputes/Statements of Disagreement.
- C4.1.2.2.7. Correspondence and Coordination Records relating to any of the above.

C4.1.3. Individual Access Requests. RMAs shall provide functionality that supports authorized personnel in recording, tracking and managing a request from a private individual (section 552a (d) of Reference (aj) and section C3.1 of Reference (ak)).

C4.1.3.1. Individual Access Request (IAR) Metadata. At a minimum, RMAs shall support gathering the IAR metadata components specified in Table C4.T3. and store and manage the request as a record (section C3.1 of Reference (ak)).

Table C4.T3. Individual Access Request Components

Requirement	Individual Access Component	Reference/ Comment
Mandatory Data Collection		
C4.T3.1.	Request ID	Unique identifier for this request.
C4.T3.2.	Request Author	Identification and contact information for person requesting information.
C4.T3.3	Nature of Request	One of Access, Amendment, or Disclosure Accounting.
C4.T3.4	Details	Details of the request.
C4.T3.5	Access Rule Cited	This can be a link to the rule under which the request was made if that rule is kept in the system. If not, it can be a text field that captures the title, date, and version of the rule.
C4.T3.6	Request Date	Date request was received.
Mandatory Support		
C4.T3.7.	Organization-Defined Fields	

C4.1.3.2. Individual Access Request Time Limits. RMAs shall provide the capability for an authorized individual to set time limits that shall apply to acknowledging requests for access and for providing access (section C3.1.11 of Reference (ak)).

C4.1.3.3. Tracking Individual Access Requests. RMAs shall provide authorized individuals the capability to track IARs.

C4.1.3.3.1. Assigning Suspense Dates. RMAs shall automatically assign acknowledgement and access grant suspense dates to the IAR by adding the relevant time limit to the "Request Date" (section C3.1.11 of Reference (ak)).

C4.1.3.3.2. Workflow/Interim Suspense Dates. RMAs shall provide the capability for an authorized individual to assign the IAR to a workflow or to create and assign alert logic to organization-defined interim suspense dates and extensions to suspense dates (section C3.1.11 of Reference (ak)).

C4.1.4. Managing Individual Access Requests. RMAs shall provide the capability for the authorized individual to capture and link authorization and denial decision documents or data to the IAR.

C4.1.4.1. Managing Individual Access Authorizations. RMAs shall provide the capability for an authorized individual to create a record of actual individual accesses, including in-person access, authorized agent by mail access, and by fax access. Access data shall include the components specified in Table C4.T4.

Table C4.T4. Access Record Components

Requirement	Access Record Component	Reference/ Comment
Mandatory Data Collection		
C4.T4.1.	Access Type	One of a selection list that includes “In Person, Authorized Agent, By Mail, or By FAX.”
C4.T4.2.	Access Date	In Person, the date the person visited. If Authorized Agent, the date the Agent visited. If By Mail, or By FAX, the date the package was sent.
C4.T4.3.	Records Accessed	A listing of the records accessed by or provided to the individual.
C4.T4.4.	Record Description	A discussion of the record state, Original, redacted, summary, data collection, etc.
Mandatory Support		
C4.T4.5.	Organization-Defined Fields	

C4.1.4.2. Record Collection. RMAs shall provide the capability for an authorized individual to search for and retrieve records meeting access request criteria.

C4.1.4.3. Providing Individual Access. RMAs shall provide interfaces with common office applications or document management systems to support the drafting of non-original documents such as redacted, summarized, reports, data listings. The RMA shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements for filing these as new records.

C4.1.4.4. Managing Records Accessed. RMAs shall link the records accessed with the access record. In the case where non-original records such as redacted, summarized, reports, data listings, are created to provide access, RMAs shall prompt users to file them as new records. The RMA shall automatically link the new records to original records that were referenced, but not released for access.

C4.1.4.5. Preparing Individual Access Denials Notices. RMAs shall provide interfaces with common office applications or document management systems to support the drafting of denial notification documents. RMAs shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements.

C4.1.4.5.1. Managing Individual Access Denials Metadata. RMAs shall provide the capability for an authorized individual to create a record of access denials (section C3.2.3 of Reference (ak)). Denial data shall include the components specified in Table C4.T5.

Table C4.T5. Denial Components

Requirement	Denial Component	Reference/ Comment
Mandatory Data Collection		
C4.T5.1.	Link to Access Request	
C4.T5.2.	Denial Authority	Name, title, position, signature or electronic signature of designated denial authority.
C4.T5.3.	Denial Date	
C4.T5.4.	Denial Reason	Text or link to sections of laws allowing denial.
C4.T5.5.	Appeal Suspense	60 calendar days from Denial Date. Suspense duration depends on published policy. 60 days is current DoD policy.
C4.T5.6.	Appeals Official	Name, title, position, signature or electronic signature of designated appeals authority.
Mandatory Support		
C4.T5.7.	Organization-Defined Fields	

C4.1.4.6. Managing Appeals and Appeal Metadata. RMAs shall link the appeal record with the denial record(s). RMAs shall provide the capability for an authorized individual to create records of appeals (section C3.2.4 of Reference (ak)). Appeal data shall include the components specified in Table C4.T6.

Table C4.T6. Appeal Components

Requirement	Appeal Component	Reference/ Comment
Mandatory Data Collection		
C4.T6.1.	Appeal ID	Unique identifier for this appeal.
C4.T6.2.	Denial ID Link	Link to denial being appealed.
C4.T6.3.	Original Request ID Link	Link to original request.
C4.T6.4.	Nature of Appeal	One of Review, Dispute, or Disclosure Accounting.
C4.T6.5.	Details	Details of the appeal.
C4.T6.6.	Appeal Date	Date Appeal was received.
Mandatory Support		
C4.T6.7.	Organization-Defined Fields	

C4.1.4.7. Appeal Time Limits. RMAs shall provide the capability for an authorized individual to set time limits that shall apply to processing appeals (section C3.2.4.5 of Reference (ak)).

C4.1.4.8. Tracking Appeals

C4.1.4.8.1. Assigning Suspense Dates. RMAs shall automatically assign acknowledgement and appeal response suspense dates to the appeal by adding the relevant time limit to the “Appeal Date.” (section C3.2.4.5 of Reference (ak)).

C4.1.4.8.2. Workflow/ Interim Suspense Dates. RMAs shall provide the capability for an authorized individual to assign the appeal to a workflow or to create and assign alert logic to organization-defined interim suspense dates and extensions to suspense dates (sections C3.2.4.5 and C3.2.5.3 of Reference (ak)).

C4.1.4.9. Managing Amendment Requests and Amendment Requests Metadata. RMAs shall link the amendment request record with the record(s) to be amended(s). RMAs shall provide the capability for an authorized individual to create a record of an amendment request (section C3.3.2 of Reference (ak)). Amendment request data shall include the components specified in Table C4.T7.

Table C4.T7. Amendment Components

Requirement	Amendment Component	Reference/ Comment
Mandatory Data Collection		
C4.T7.1.	Request ID	Unique identifier for this appeal.
C4.T7.2.	Record Link	Link to record(s) to be amended.
C4.T7.3.	Amendment Justification	
C4.T7.4.	Amendment Type	One of Deletion Correction, Addition.
C4.T7.5.	Amendment Request Date	Date amendment request was received.
C4.T7.6.	Reference Links	Links to records supplied by requestor as documentary evidence.
C4.T7.7	Amendment Resolution	How the amendment request was resolved.
C4.T7.8	Amendment Resolution Date	Date request was resolved.
Mandatory Support		
C4.T7.9.	Organization-Defined Fields	

C4.1.4.10. Amendment Request Time Limits. RMAs shall provide the capability for an authorized individual to set time limits that shall apply to processing amendment requests (section C3.3.7 of Reference (ak)).

C4.1.4.11. Tracking Amendments

C4.1.4.11.1. Assigning Suspense Dates. RMAs shall automatically assign acknowledgement and appeal response suspense dates to the appeal by adding the relevant time limit to the “Amendment Request Date” (section C3.3.7 of Reference (ak)).

C4.1.4.11.2. Workflow/ Interim Suspense Dates. RMAs shall provide the capability for an authorized individual to assign the amendment request to a workflow or to create and assign alert logic to organization-defined interim suspense dates and extensions to suspense dates (section C3.3.7 of Reference (ak)).

C4.1.4.11.3. Previous Recipient Notification. RMAs shall provide links to relevant disclosure accounting records so that an authorized individual can identify previous recipients of the record and notify them of the amendment (section C3.3.9 of Reference (ak)).

C4.1.4.12. Managing Disputes/Statements of Disagreement. RMAs shall link the dispute or statement of disagreement record with the disputed record(s) and with the Amendment Request Record(s).

C4.1.4.13. Disputes/Statements of Disagreement Metadata. RMAs shall provide an authorized individual the capability to collect and manage metadata about Disputes and Disagreements shall include the components listed in Table C4.T8.

Table C4.T8. Dispute Components

Requirement	Dispute Component	Reference/ Comment
Mandatory Data Collection		
C4.T8.1.	Dispute ID	Unique identifier for this appeal.
C4.T8.2.	Disclosure ID	Link to disclosure record.
C4.T8.3.	Dispute Author	Person initializing the dispute.
C4.T8.4.	Dispute Date Received	Date organization received the dispute.
C4.T8.5.	Dispute Date Closed	Date of final action on dispute.
C4.T8.6.	Nature of Dispute	Summary of dispute allegations.
C4.T8.7.	Discussion	Discussion of the dispute allegations.
C4.T8.8.	Resolution	Discussion of the final resolution of the dispute.
Conditional Data Collection		
C4.T8.9.	Statement of Disagreement	Mandatory if dispute author provides a statement.
C4.T8.10.	Civil Action	Mandatory if civil action arises from dispute.
C4.T8.11.	Preparer	Identification of individual preparing disclosure or individual access response that led to dispute. Mandatory if dispute is related to a disclosure(s).
C4.T8.12.	Released By	Identification of person approving disclosure, or individual access response. Mandatory if dispute is related to a disclosure(s).
C4.T8.13.	Request ID	Link to original access request. Mandatory if dispute is related to a disclosure(s) or individual access response(s).
Mandatory Support		
C4.T8.14.	Organization-Defined Fields	

C4.1.4.13.1. Disclosing Disputes. RMAs shall retrieve disputes or statements of disagreement with affected records when those records meet disclosure search criteria.

C4.1.5. Disclosures. RMAs shall provide authorized individuals the capability to record disclosure requests and track, manage, and account for disclosures (Reference (ab) and section C4 of Reference (ak)).

C4.1.5.1. Managing Disclosure Request Metadata. RMAs shall provide the capability for an authorized individual to create a record of a disclosure request. Disclosure request data shall include the components specified in Table C4.T9.

Table C4.T9. Disclosure Request Components

Requirement	Disclosure Request Component	Reference/ Comment
Mandatory Data Collection		
C4.T9.1.	Disclosure Request ID	Unique identifier for this request.
C4.T9.2.	Disclosure Requestor	Contact Information for the authorized agent requesting the disclosure.
C4.T9.3.	Details	Details about the requested disclosure.
C4.T9.4.	Disclosure Request Date	Date Disclosure Request was received.
Conditional Data Collection		
C4.T9.5.	Individual Consent	Mandatory if consent is required, for requests that include individually identifying information.
Mandatory Support		
C4.T9.6.	Organization-Defined Fields	

C4.1.5.2. Managing Disclosure Metadata. RMAs shall provide the capability for an authorized individual to create a record of a disclosure. Disclosure metadata shall include the components specified in Table C4.T10.

Table C4.T10. Disclosure Metadata Components

Requirement	Disclosure Component	Reference/ Comment
Mandatory Data Collection		
C4.T10.1.	Disclosure ID	Unique identifier for this Disclosure.
C4.T10.2.	Disclosure Request ID	Link to the Disclosure Request or NARA transfer identifier.
C4.T10.3.	Disclosure Date	Date the disclosure was released to requestor.
C4.T10.4.	Disclosure Description	Description of the information released. This may also be links to actual records disclosed.
C4.T10.5.	Disclosure Recipient	Name of recipient of disclosed records.
C4.T10.6.	Disclosure Recipient Unit	Organization receiving disclosed records.
C4.T10.7.	Preparer	The identification of the person responsible for preparing the disclosure.

Requirement	Disclosure Component	Reference/ Comment
C4.T10.8.	Released By	The identification of the person responsible for releasing the information.
C4.T10.9.	Records Disclosed	A link to the records disclosed by this disclosure. If original records were redacted and new records created, this shall point to the actual records released.
C4.T10.10.	Dispute Information	Indicate if disclosed information has been corrected or disputed.
C4.T10.11.	System of Records	Link to System of records disclosure was made from.
Conditional Data Collection		
C4.T10.12.	FOIA Request	Optional Link to FOIA Request. Mandatory if requests for both FOIA and Privacy Act are similar. One of the FOIA, Other, or Privacy Act request fields is mandatory, unless this is a NARA transfer.
C4.T10.13.	Other Request	Could be court order, subpoena, etc.
C4.T10.14.	Privacy Act Request	Optional Link to Privacy Act Request. Mandatory if requests for both FOIA and Privacy Act if request requirements are similar.
Mandatory Support		
C4.T10.15.	Organization-Defined Fields	

C4.1.5.3. Tracking Disclosures. RMAs shall provide the capability for authorized individuals to manage and account for disclosures.

C4.1.5.3.1. Assigning Suspense Dates. RMAs shall provide the capability for an authorized individual to assign suspense dates to a disclosure request.

C4.1.5.3.2. Workflow/ Interim Suspense Dates. RMAs shall provide the capability for an authorized individual to assign the disclosure request to a workflow or to create and assign alert logic to user defined interim suspense dates and extensions to suspense dates.

C4.1.5.3.3. Record Collection. RMAs shall provide the capability for an authorized individual to search for and retrieve records meeting disclosure request criteria. RMAs shall provide the capability for an authorized individual to create a copy of a retrieved record for redacting and/or summarizing.

C4.1.5.3.4. Preparing Disclosures. The RMA shall provide interfaces with common office applications or document management systems to support the drafting of disclosure documents. The RMA shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements. The organization is to “map” information from their environment into the RMA metadata set. If they do, the

RMA shall copy the contents of the mapped “property” or other metatagging fields into the RMA metadata set for the record being recorded.

C4.1.5.3.5. Managing Redacted and Summarized Records. RMAs shall provide the capability for authorized individuals to link redacted versions of records and record summaries to the original records.

C4.1.5.4. Disclosure Accounting. RMAs shall provide authorized individuals with the capability to account for each disclosure of information from the SOR.

C4.1.5.4.1. Accounting Records. RMAs shall provide the capability for an authorized individual to create an accounting record. Accounting Record data shall include the components specified in Table C4.T11.

Table C4.T11. Accounting Record Components

Requirement	Accounting Component	Reference/ Comment
Mandatory Data Collection		
C4.T11.1.	Accounting ID	Unique identifier for this Account Record.
C4.T11.2.	Accounting Review Date	Date disclosure was reviewed.
C4.T11.3.	Accounting Reviewed By	Name and contact information for person conducting the review.
C4.T11.4.	Disclosure ID	Link to reviewed disclosure(s).
Conditional Data Collection		
C4.T11.5.	Accounting Release Date	Date accounting was released to individuals concerned.
C4.T11.6.	Individual Access Request	Link to access request if applicable.
Mandatory Support		
C4.T11.7.	Organization-Defined Fields	

C4.1.5.4.2. Linking Accounting Records to Disclosures. RMAs shall automatically link an accounting record to the disclosure being reviewed.

C4.1.5.5. Disclosure Exemptions. RMAs shall provide an authorized individual the capability to create and manage exemption records (Reference (ab) and section C5 of Reference (ak)).

C4.1.5.5.1. Exemption Records. RMAs shall provide the capability for an authorized individual to create an exemption record. Exemption Record data shall include the components specified in Table C4.T12.

Table C4.T12. Exemption Components

Requirement	Exemption Component	Reference/ Comment
Mandatory Data Collection		
C4.T12.1.	Exemption ID	Unique identifier for this Exemption.
C4.T12.2.	Privacy Act Section Ref	Reference in the Privacy Act that allows the exemption.
Conditional Data Collection		
C4.T12.3.	Privacy Act Text	Optional exemption text.
C4.T12.4.	General Exemption	Optional exemption text.
C4.T12.5.	Specific Exemption	Optional exemption text.
Mandatory Support		
C4.T12.6.	Organization-Defined Fields	

C4.1.5.5.2. Linking Exemptions to Records. RMAs shall provide an authorized individual the capability to link an exemption record to a record or a group of records.

C4.1.6. Matching Programs. RMAs shall provide an authorized individual the capability to create and manage matching program records (section C11 of Reference (ak)).

C4.1.6.1. Matching Program Records. RMAs shall provide the capability for an authorized individual to create a matching program record. Matching Program Record data shall include the components specified in Table C4.T13.

Table C4.T13. Matching Program Components

Requirement	Matching Program Component	Reference/ Comment
Mandatory Data Collection		
C4.T13.1.	Matching Program ID	Unique identifier for this Matching Program Record.
C4.T13.2.	Sibling System Identification	System Name or identifier of systems with which information shall be cross-matched.
C4.T13.3.	Sibling System POC	Matching Program Point of Contact for the other system.
C4.T13.4.	Purpose	Purpose of the matching program.
Mandatory Support		
C4.T13.6.	Organization-Defined Fields	

C4.1.6.2. Linking Matching Programs to SORs. RMAs shall provide an authorized individual the capability to link matching program record to the referenced system of records.

C4.1.6.3. Preparing Matching Program Notices. RMAs shall provide interfaces with common office applications or document management systems to support the drafting of

matching program notices. RMAs shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements. The organization is to “map” information from their environment into the RMA metadata set. If they do, the RMA shall copy the contents of the mapped “property” or other metatagging fields into the RMA metadata set for the record being recorded.

C4.1.7. Electronic Privacy Act Elements (Optional). RMAs shall provide graphical user interface capabilities to allow authorized individuals to create and publish web portals to support electronic Privacy Act requests.

C4.2. MANAGEMENT OF FREEDOM OF INFORMATION ACT RECORDS

The following requirements are mandatory for only those RMAs that support the Freedom of Information Act (FOIA). Organizational compliance to FOIA may be implemented outside the scope of an RMA. These requirements are in addition to those requirements outlined in Chapters 2 and 3. In this chapter, the word “shall” identifies mandatory system standards for managing FOIA records. The word “should” identifies design objectives that are desirable but not mandatory. Additionally, requirements for safeguarding and providing security for FOIA records are not in the scope of this document, since they are provided in other directives and regulations.

C4.2.1. Organization Access Rules. RMAs shall provide functionality that supports authorized personnel in preparing and posting access rules for the public to gain access to FOIA information.

C4.2.1.1. Access Rule Metadata. RMAs shall provide the capability for an authorized individual to create an access rules record. Access Rules data shall include the components specified in Table C4.T14.

Table C4.T14. Access Rules Components

Requirement	Access Rules Component	Reference/ Comment
Mandatory Data Collection		
C4.T14.1.	FOIA Rule Identifier	Unique identifier for this Access Rule document.
C4.T14.2.	Access Rules	Pointer to the rules document. The requirements for capturing information about and publishing access rules may be similar enough between Privacy Act and FOIA to share one set of metadata elements for other metadata.

C4.2.1.2. Preparing Access Rules. RMAs shall provide interfaces with common office applications or document management systems to support the drafting of access rules documents.

RMA shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements. The organization is to “map” information from their environment into the RMA metadata set. If they do, the RMA shall copy the contents of the mapped “property” or other metatagging fields into the RMA metadata set for the record being recorded.

C4.2.2. FOIA Access Requests. RMA shall provide functionality that supports authorized personnel in recording, tracking and managing a FOIA request.

C4.2.2.1. FOIA Request Metadata. FOIA requests and Privacy Act Individual Access Requests are very similar. One object could be used to support both. At a minimum, RMA shall support the collection of the following FOIA metadata and store and manage the request as a record.

Table C4.T15. FOIA Request Components

Requirement	FOIA Request Component	Reference/ Comment
Mandatory Data Collection		
C4.T15.1.	Request ID	Unique identifier for this request.
C4.T15.2.	Request Author	Identification and contact information for person requesting information.
C4.T15.3.	Nature of Request	Summary of request focus.
C4.T15.4.	Details	Details of the request.
C4.T15.5.	Access Rule Cited	This can be a link to the rule under which the request was made if that rule is kept in the system. If not, it can be a text field that captures the title, date, and version of the rule.
C4.T15.6.	Request Date	Date request was received.
Mandatory Support		
C4.T15.7.	Organization-Defined Fields	

C4.2.2.2. FOIA Request Time Limits. RMA shall provide the capability for an authorized individual to set time limits that shall apply to acknowledging requests for access and for providing access.

C4.2.2.3. Tracking FOIA Requests. RMA shall provide authorized individuals the capability to track FOIA Requests.

C4.2.2.3.1. Assigning Suspense Dates. RMA shall automatically assign acknowledgement and access grant suspense dates to the FOIA request by adding the relevant time limit to the “Request Date.”

C4.2.2.3.2. Workflow/Interim Suspense Dates. RMAs shall provide the capability for an authorized individual to assign the FOIA request to a workflow or to create and assign alert logic to user defined interim suspense dates and extensions to suspense dates.

C4.2.3. Disclosures. RMAs shall provide authorized individuals the capability to record disclosure requests and track, manage, and account for disclosures (Reference (ab) and section C4 of Reference (ak)).

C4.2.3.1. Managing Disclosure Request Metadata. RMAs shall provide the capability for an authorized individual to create a record of a FOIA disclosure request. Disclosure metadata shall include the components specified in Table C4.T16.

Table C4.T16. FOIA Disclosure Request Components

Requirement	FOIA Disclosure Request Component	Reference/ Comment
Mandatory Data Collection		
C4.T16.1.	Disclosure Request ID	Unique identifier for this request.
C4.T16.2.	Disclosure Requestor	Contact information for the authorized agent requesting the disclosure.
C4.T16.3.	Details	Details about the requested disclosure, (i.e. which records).
C4.T16.4.	Disclosure Request Date	Date Disclosure Request was received.
Conditional Data Collection		
C4.T16.5.	Disclosure Purpose	Purpose to which the disclosed information shall be put.
C4.T16.6.	Individual Consent	Some disclosures require individual consent. This field could link to that consent document.
Mandatory Support		
C4.T16.7.	Organization-Defined Fields	Organizational-defined fields may be used to capture extra information, including whether or not the FOIA disclosure request was denied.

C4.2.3.2. Managing Disclosure Metadata. RMAs shall provide the capability for an authorized individual to create a record of a FOIA disclosure. Disclosure metadata shall include the components specified in Table C4.T17.

Table C4.T17. FOIA Disclosure Components

Requirement	FOIA Disclosure Component	Reference/ Comment
Mandatory Data Collection		
C4.T17.1.	Disclosure ID	Unique identifier for this Disclosure.
C4.T17.2.	Disclosure Request ID	Link to the Disclosure Request or NARA transfer identifier.

DoD 5015.02-STD, April 25, 2007

Requirement	FOIA Disclosure Component	Reference/ Comment
C4.T17.3.	Disclosure Date	Date the disclosure was released to requestor.
C4.T17.4.	Disclosure Description	Description of the information released. This may also be links to actual records disclosed.
C4.T17.5.	Disclosure Notes	Discussion of deletions or changes to records disclosed. Also may be other information pertinent to the disclosure.
C4.T17.6.	Disclosure Purpose	Reason for Disclosure.
C4.T17.7.	Disclosure Recipient	Name of recipient of disclosed records.
C4.T17.8.	Disclosure Recipient Unit	Organization receiving disclosed records.
C4.T17.9.	Preparer	The identification of the person responsible for preparing the disclosure.
C4.T17.10.	Released By	The identification of the person responsible for releasing the information.
C4.T17.11.	Records Disclosed	A link to the records disclosed by this disclosure. If original records were redacted and new records created, this shall point to the actual records released.
C4.T17.12.	Dispute Information	Indicate if disclosed information has been corrected or disputed.
C4.T17.13.	System of Records	Link to System of Records disclosure was made from.
Conditional Data Collection		
C4.T17.14.	FOIA Request	Optional Link to FOIA Request. May generalize requests for both FOIA and Privacy Act if request requirements are sufficiently similar. One of the FOIA, Other, or Privacy Act request fields is mandatory, unless this is a NARA transfer.
C4.T17.15.	Other Request	Could be court order, subpoena, etc. One of the FOIA, Other, or Privacy Act request fields is mandatory, unless this is a NARA transfer.
C4.T17.16.	Privacy Act Request	Optional Link to Privacy Act Request. May generalize requests for both FOIA and Privacy Act if request requirements are sufficiently similar. One of the FOIA, Other, or Privacy Act request fields is mandatory, unless this is a NARA transfer.
Mandatory Support		
C4.T17.17.	Organization-Defined Fields	

C4.2.3.3. Tracking Disclosures. RMAs shall provide the capability for authorized individuals to manage and account for disclosures.

C4.2.3.3.1. Assigning Suspense Dates. RMAs shall provide the capability for an authorized individual to assign suspense dates to a FOIA request.

C4.2.3.3.2. Workflow/ Interim Suspense Dates. RMAs shall provide the capability for an authorized individual to assign the FOIA request to a workflow or to create and assign alert logic to user defined interim suspense dates and extensions to suspense dates.

C4.2.3.3.3. Record Collection. RMAs shall provide the capability for an authorized individual to search for and retrieve records meeting FOIA request criteria. RMAs shall provide the capability for an authorized individual to create a copy of a retrieved record for redacting and/or summarizing.

C4.2.3.3.4. Preparing Disclosures. RMAs shall provide interfaces with common office applications or document management systems to support the drafting of disclosure documents. The RMA shall collect pertinent metadata from the office application or document management system file properties to pre-populate relevant metadata elements. The organization is to “map” information from their environment into the RMA metadata set. If they do, the RMA shall copy the contents of the mapped “property” or other metatagging fields into the RMA metadata set for the record being recorded.

C4.2.3.3.5. Managing Redacted and Summarized Records. RMAs shall provide the capability for authorized individuals to link redacted versions of records and record summaries to the original records.

C4.2.3.4. Disclosure Exemptions. RMAs shall provide an authorized individual the capability to create and manage exemption records (Reference (ab) and section C5 of Reference (ak)).

C4.2.3.4.1. Exemption Records. RMAs shall provide the capability for an authorized individual to create an exemption record. Exemption Record data shall include the components specified in Table C4.T18.

Table C4.T18. FOIA Exemption Components

Requirement	Exemption Component	Reference/ Comment
Mandatory Data Collection		
C4.T18.1.	Exemption ID	Unique identifier for this Exemption.
C4.T18.2.	FOIA Section Ref	Reference in the legal documentation that allows the exemption.
Conditional Data Collection		
C4.T18.3.	Privacy Act Text	Optional exemption text.
C4.T18.4.	General Exemption	Optional exemption text.
C4.T18.5.	Specific Exemption	Optional exemption text.
Mandatory Support		
C4.T18.6.	Organization-Defined Fields	

C4.2.3.4.2. Linking Exemptions to Records. RMAs shall provide an authorized individual the capability to link an exemption record to a record or a group of records.

C4.2.3.5. Managing Appeals. RMAs shall link the appeal record with the denial record(s).

C4.2.3.5.1. Managing Appeal Metadata. RMAs shall provide the capability for an authorized individual to create a record of appeals. Appeal data shall include the components specified in Table C4.T19.

Table C4.T19. FOIA Appeal Components

Requirement	FOIA Appeal Component	Reference/ Comment
Mandatory Data Collection		
C4.T19.1.	Appeal ID	Unique identifier for this appeal.
C4.T19.2.	FOIA Disclosure	Link to disclosure record.
C4.T19.3.	Appeal Author	
C4.T19.4.	Appeal Date Received	Date appeal was received.
C4.T19.5.	Appeal Date Closed	Date appeal was closed.
C4.T19.6.	Appeal Justification	Justification for appeal.
C4.T19.7	Appeal Resolution	Date the appeal was resolved.
C4.T19.8	Appeal Preparer	Name of person preparing response to appeal.
C4.T19.9	Released By	Authority for releasing response to appeal.
C4.T19.10	FOIA Request	Link to original request record.
Conditional Data Collection		
C4.T19.11	Discussion	Mandatory if critical to documenting appeal.
Mandatory Support		
C4.T19.12.	Organization-Defined Fields	

C4.2.3.6. Appeal Time Limits. RMAs shall provide the capability for an authorized individual to set time limits that shall apply to processing appeals.

C4.2.3.7. Tracking Appeals

C4.2.3.7.1. Assigning Suspense Dates. RMAs shall automatically assign acknowledgement and appeal response suspense dates to the appeal by adding the relevant time limit to the “Appeal Date.”

C4.2.3.7.2. Workflow/ Interim Suspense Dates. RMAs shall provide the capability for an authorized individual to assign the appeal to a workflow or to create and assign alert logic to organization-defined interim suspense dates and extensions to suspense dates.

C4.2.4. FOIA Reports. RMAs shall provide authorized individuals the capability to create, file, and manage FOIA Reports.

C4.2.4.1. FOIA Reports Metadata. At a minimum, RMAs shall capture the components specified in Table C4.T20.

Table C4.T20. FOIA Reports Metadata Disclosure Components

Requirement	Disclosure Component	Reference/ Comment
Mandatory Data Collection		
C4.T20.1.	Denials	Number of determinations made to deny requests for records and the reasons for those denials.
C4.T20.2.	Appeals	Results of appeals.
C4.T20.3.	Requests Pending	Number of requests pending from previous year.
C4.T20.4.	Requests Received	Number of requests received in current year.
C4.T20.5.	Request Processed	Number of requests processed in current year.
C4.T20.6.	Processing Time	Median number of days to process different types of requests.
C4.T20.7.	Total Fees	Amount of fees collected for fulfilled requests.
C4.T20.8.	Staff Allocated	Number of fulltime staff dedicated to FOIA in current year.
C4.T20.9.	Amount expended	Total amount expended to meet FOIA requirements.
Mandatory Support		
C4.T20.10.	Organization-Defined Fields	

C4.2.4.2. FOIA Reporting Links. RMAs shall be able to link the following to the FOIA report:

C4.2.4.2.1. Requests.

C4.2.4.2.2. Appeals.

C4.2.4.2.3. Denials.

C4.2.4.2.4. Other records or metadata objects used in creating the report.

C4.2.5. Electronic FOIA Elements (Optional). RMAs shall provide graphical user interface capabilities to allow authorized individuals to create and publish web portals to support electronic FOIA requests.

C4.3. ACCESS CONTROL FOR PRIVACY ACT AND FREEDOM OF INFORMATION ACT RECORDS

Software applications shall include IA controls for availability, integrity, confidentiality, authentications, non-repudiation and shall be National Telecommunications and Information Systems Security Policy compliant, which requires independent evaluation and certification of IA functionality either by a National Information Assurance Partnership lab or NSA. Table C4.T21. summarizes requirements that refer to “authorized individuals” and offers additional information regarding user-type responsibilities. In general, Application Administrators are responsible for setting up the RMA infrastructure. System Administrators are responsible for the network infrastructure. Life Cycle Support personnel function under the application administrator. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users.

Table C4.T21. Authorized Individual Requirements for Privacy Act and FOIA Records

Requirement	Application/System Administrator/Life Cycle Support Personnel	Records Manager	Privileged User
C4.T21.1 (C4.1.2.) <u>Privacy Case Files</u>create and manage Privacy Case Files.	NA	Create and manage.	Create and manage.
C4.T21.2. (C4.1.3.) <u>Individual Access Requests</u> recording, tracking and managing a request.	Record, track and manage.	Record, track and manage.	Record, track and manage.
C4.T21.3. (C4.1.3.2.) <u>Individual Access Request Time Limits</u> set time limits that shall apply to acknowledging requests for access and for providing access.	At setup.	Set time limits.	NA
C4.T21.4. (C4.1.3.3.) <u>Tracking Individual Access Requests</u> track IARs.	NA	Track	Track
C4.T21.5. (C4.1.3.3.2.) <u>Workflow/Interim Suspense Dates</u> assign the IAR to a workflow or to create and assign alert logic to organization-defined interim suspense dates and extensions to suspense dates.	Create logic.	Create logic/assign workflow.	Assign workflow.
C4.T21.6. (C4.1.4.) <u>Managing Individual Access Requests</u> capture and link authorization and denial decision documents or data to the IER.	NA	Link/unlink	Link

Requirement	Application/System Administrator/Life Cycle Support Personnel	Records Manager	Privileged User
C4.T21.7. (C4.1.4.1.) <u>Managing Individual Access Authorizations.</u> ... create record of actual individual accesses...	NA	Create	Create
C4.T21.8. (C4.1.4.2.) <u>Record Collection.</u> ...search for and retrieve records	Create logic.	Search/retrieve	Search/retrieve
C4.T21.9. (C4.1.4.5.1.) <u>Managing Individual Access Denials Metadata.</u> ...create record of access denials.	NA	Create	Create
C4.T21.10. (C4.1.4.6.1.) <u>Managing Appeal Metadata.</u> ... create records of appeals.	NA	Create	Create
C4.T21.11. (C4.1.4.7.) <u>Appeal Time Limits.</u> ... set time limits that shall apply to processing appeals.	At setup.	Set time limits.	NA
C4.T21.12. (C4.1.4.8.2.) <u>Workflow/ Interim Suspend Dates.</u> ... assign the appeal to a workflow or to create and assign alert logic to organization-defined interim suspend dates and extensions to suspend dates.	Create logic.	Create logic/assign workflow.	Assign workflow.
C4.T21.13. (C4.1.4.9.) <u>Managing Amendment Requests and Amendment Requests Metadata.</u> ...create a record of an amendment request.	NA	Create	Create
C4.T21.14. (C4.1.4.10.) <u>Amendment Request Time Limits.</u> ...set time limits that shall apply to processing amendment requests.	Create logic, at setup.	Set time limits.	NA
C4.T21.15. (C4.1.4.11.2.) <u>Workflow/ Interim Suspend Dates.</u> ...assign the amendment request to a workflow or to create and assign alert logic to organization-defined interim suspend dates and extensions to suspend dates.	Create logic.	Create logic/assign workflow.	Assign workflow.
C4.T21.16. (C4.1.4.11.3.) <u>Previous Recipient Notification.</u> ... identify previous recipients of the record and notify them of the amendment.	NA	Create/edit/run	Run
C4.T21.17. (C4.1.4.13) <u>Disputes/Statements of Disagreement Metadata.</u> ...collect and manage metadata about Disputes and Disagreements.	NA	Create and manage.	Create

Requirement	Application/System Administrator/Life Cycle Support Personnel	Records Manager	Privileged User
C4.T21.18. (C4.1.5.) <u>Disclosures.</u> ... record disclosure requests and track, manage, and account for disclosures.	NA	Create/edit/run	Run
C4.T21.19. (C4.1.5.1.) <u>Managing Disclosure Request Metadata.</u> ... create a record of a disclosure request.	NA	Create	Create
C4.T21.20. (C4.1.5.2.) <u>Managing Disclosure Metadata.</u> ... create a record of a disclosure.	NA	Create	Create
C4.T21.21. (C4.1.5.3.) <u>Tracking Disclosures.</u> ... manage and account for disclosures.	NA	Create/edit/run	Run
C4.T21.22. (C4.1.5.3.1.) <u>Assigning Suspend Dates.</u> ... assign suspend dates to a disclosure request.”	Create logic.	Create logic/assign workflow.	Assign workflow.
C4.T21.23. (C4.1.5.3.2.) <u>Workflow/ Interim Suspend Dates.</u> ... assign the disclosure request to a workflow or to create and assign alert logic to user defined interim suspend dates and extensions to suspend dates.	Create logic.	Create logic/assign workflow.	Assign workflow.
C4.T21.24. (C4.1.5.3.3.) <u>Record Collection.</u> ... search for and retrieve records meeting disclosure request criteria. ... create a copy of a retrieved record for redacting and/or summarizing.	NA	Search/retrieve	Search/retrieve
C4.T21.25. (C4.1.5.3.5.) <u>Managing Redacted and Summarized Records.</u> ... link redacted versions of records and record summaries to the original records.	NA	Link/unlink	Link
C4.T21.26. (C4.1.5.4.) <u>Disclosure Accounting.</u> ... account for each disclosure of information from the SOR.	NA	Create/edit/run	Run
C4.T21.27. (C4.1.5.4.1.) <u>Accounting Records.</u> ... create an accounting record. :	NA	Create	Create
C4.T21.28. (C4.1.5.5.) <u>Disclosure Exemptions.</u> ... create and manage exemption records.	NA	Create and manage.	Create
C4.T21.29. (C4.1.5.5.1.) <u>Exemption Records.</u> ... create an exemption record:	NA	Create	Create

Requirement	Application/System Administrator/Life Cycle Support Personnel	Records Manager	Privileged User
C4.T21.30. (C4.1.5.5.2.) <u>Linking Exemptions to Records.</u> ... link an exemption record to a record or a group of records.	NA	Link/unlink	Link
C4.T21.31. (C4.1.6.) <u>Matching Programs.</u> ... create and manage matching program records.	NA	Create and manage.	Create
C4.T21.32. (C4.1.6.1.) <u>Matching Program Records.</u> ... create a matching program record.	NA	Create	Create
C4.T21.33. (C4.1.6.2.) <u>Linking Matching Programs to SORs.</u> ... link matching program record to the referenced system of records.	NA	Link/unlink	Link
C4.T21.34. (C4.1.7.) <u>Electronic Privacy Act Elements (optional).</u> ... create and publish web portals to support electronic Privacy Act requests.	Create page.	Create and edit pages.	None
C4.T21.35. (C4.2.1.) <u>Organization Access Rules.</u> ...preparing and posting access rules for the public to gain access to FOIA information.	Create and post rules.	Create and manage.	Create and manage.
C4.T21.35. (C4.2.1.1.) <u>Access Rule Metadata.</u> ... create an access rules record.	NA	Create	Create
C4.T21.36. (C4.2.2.2.) <u>FOIA Request Time Limits.</u> ... set time limits that shall apply to acknowledging requests for access and for providing access.	At setup.	Set time limits.	NA
C4.T21.37. (C4.2.2.3.) <u>Tracking FOIA Requests.</u> ... track FOIA Requests.	NA	Track	Track
C4.T21.38. (C4.2.2.3.2.) <u>Workflow/Interim Suspense Dates.</u> ... assign the FOIA request to a workflow or to create and assign alert logic to user defined interim suspense dates and extensions to suspense dates.”	Create logic.	Create logic/assign workflow.	Assign workflow.
C4.T21.39. (C4.2.3.) <u>Disclosures.</u> ... record disclosure requests and track, manage, and account for disclosures	NA	Create/edit/destroy	Create

Requirement	Application/System Administrator/Life Cycle Support Personnel	Records Manager	Privileged User
C4.T21.40. (C4.2.3.1.) <u>Managing Disclosure Request Metadata.</u> ...create a record of a FOIA disclosure request.	NA	Create	Create
C4.T21.41. (C4.2.3.2.) <u>Managing Disclosure Metadata.</u> ... create a record of a FOIA disclosure.	NA	Create	Create
C4.T21.42. (C4.2.3.3.) <u>Tracking Disclosures.</u> ... manage and account for disclosures.	NA	Create/edit/run	Run
C4.T21.43. (C4.2.3.3.1.) <u>Assigning Suspend Dates.</u> ... assign suspend dates to a FOIA request.”	Create logic.	Create logic/assign workflow.	Assign workflow.
C4.T21.44. (C4.2.3.3.2.) <u>Workflow/ Interim Suspend Dates.</u> ... assign the FOIA request to a workflow or to create and assign alert logic to user defined interim suspend dates and extensions to suspend dates.	Create logic.	Create logic/assign workflow.	Assign workflow.
C4.T21.45. (C4.2.3.3.3.) <u>Record Collection</u> ... search for and retrieve records meeting FOIA request criteria. ... create a copy of a retrieved record for redacting and/or summarizing.	NA	Search/retrieve/ create	Search/retrieve
C4.T21.46. (C4.2.3.3.5.) <u>Managing Redacted and Summarized Records.</u> ... link redacted versions of records and record summaries to the original records.	NA	Link/unlink	Link
C4.T21.47. (C4.2.3.4.) <u>Disclosure Exemptions.</u> ... create and manage exemption records.	NA	Create and manage.	Create
C4.T21.48. (C4.2.3.4.1) <u>Exemption Records</u> ... create an exemption record. :	NA	Create	Create
C4.T21.49. (C4.2.3.4.2.) <u>Linking Exemptions to Records.</u> ... link an exemption record to a record or a group of records.	NA	Link/unlink	Link
C4.T21.50. (C4.2.3.5.1.) <u>Managing Appeal Metadata.</u> ... create record of appeals.	NA	Create	Create
C4.T21.51. (C4.2.3.6.) <u>Appeal Time Limits.</u> ... set time limits that shall apply to processing appeals.	At setup.	Set time limits.	NA

Requirement	Application/System Administrator/Life Cycle Support Personnel	Records Manager	Privileged User
C4.T21.52. (C4.2.3.7.2.) <u>Workflow/ Interim Suspense Dates.</u> ... assign the appeal to a workflow or to create and assign alert logic to organization-defined interim suspense dates and extensions to suspense dates.	Create logic.	Create logic/assign workflow.	Assign workflow.
C4.T21.53. (C4.2.4.) <u>FOIA Reports.</u> ... create, file, and manage FOIA Reports.	NA	Create and manage.	Create
C4.T21.54. (C4.2.5.) <u>Electronic FOIA Elements (optional).</u> ... create and publish web portals to support electronic FOIA requests.	Create page.	Create and edit pages.	None

C5. CHAPTER 5

TRANSFERS

C5.1. RMA TO RMA TRANSFER INTEROPERABILITY

A record to be transferred may still be in its active lifecycle. As such it needs to be linked to sufficient information to allow continued tracking either by the receiving organization or by the originating organization using a new RMA. This Standard defines two levels of transfer. Mandatory transfer involves records and record folders. All RMAs are required to provide this capability. Optionally, RMAs should transfer file plans and links to the file plan context of a record or record folder. File Plan transfers shall follow the guidance in Paragraph C5.3.

C5.1.1. Context Management. RMAs shall support maintaining the transferred records' context.

C5.1.1.1. Writing Out Context. RMAs shall write out record metadata and content, including contextual links to other records in the transfer set in a non-proprietary, clearly structured format (e.g. plain text). RMAs shall include the records' or record folders' lifecycle status.

C5.1.1.2. Ingesting Context. RMAs shall ingest record metadata and content and restore contextual links to other records in the transfer set as well as the record's status in its lifecycle.

C5.1.2. Organization-Defined Optional Metadata Interoperability and Support of Organization-Defined Elements. Organization-defined elements are necessary to support a variety of agency functions. RMAs shall support definition, writing out, ingesting and linking of organization-defined metadata elements to required elements and to affected records and record groupings. RMAs shall provide capabilities for defining, capturing data, storing, writing out, ingesting, and linking organization-defined metadata elements to other elements as specified in this Standard.

C5.1.3. Transfer Schema Structure. RMAs shall support reading from and writing to a standard transfer structure.

C5.1.3.1. Transfer Schema Default. Vendors shall contact JITC for the most current version.

C5.1.3.2. Transfer Schema Organization-Defined. RMAs shall provide a graphical user interface capability for an authorized individual to add to or remove from the schema organization-defined, defined optional, and any vendor provided metadata fields.

C5.1.4. Transfer Schema Metadata Mapping. RMAs shall support mapping metadata defined in this Standard to the archival and transfer schemas.

C5.1.4.1. Transfer Schema Metadata Default Mapping. By default RMAs shall map metadata defined by this Standard to the same named element in the archival and transfer schemas.

C5.1.4.2. Transfer Schema Metadata Organization-Defined Mapping. RMAs shall provide a graphical user interface capability to allow an authorized individual to map metadata to schema elements to support export and ingest. RMAs shall not allow users to override default mapping of mandatory metadata elements for export.

C5.1.5. Organization-Defined Elements Export Schemas and Rendering Aids. RMAs shall provide schema extensions for all system and organization-defined metadata elements, attributes, and acceptable values for all metadata that may be exported. Such schema extensions may be provided in the form of extensions to the DDMS (Reference (d)). RMAs shall provide the capability for an authorized individual to implement an export schema based on this Standard and the vendor provided DTD. RMA-provided export DTDs and schemas shall not cause namespace conflicts with the metadata elements and attributes defined in this Standard. RMAs shall include the Export DTD and export schemas as part of the transfer as a default. RMAs shall allow an authorized individual to remove the default if not needed by recipient. If required for proper metadata content rendering and presentation of metadata context, or as appropriate, RMAs shall provide CSS or another open-standard rendering aid such as XSLT transformations as a component of the transfer.

C5.1.6. Record Elements. RMAs shall manage writing out records for transfer with the metadata shown in the following paragraphs. RMAs shall parse and process all metadata elements during ingestion. Optionally RMAs shall provide authorized individuals with graphical user interface capabilities to support merging ingested records into existing file plans.

C5.1.6.1. Standard Record Elements. RMAs shall write out metadata with records in the standard transfer formats. RMAs shall parse, ingest and link received standard formatted record information into the receiving database and/or repository.

C5.1.6.2. Record Level Core Mandatory Elements. RMAs shall associate core elements with all records no matter the type or source. RMAs shall write out and ingest the following metadata and content elements for each record being transferred as specified in Table C5.T1.

Table C5.T1. Record Level Core (Defined Mandatory)

Data Element	Data Source	Content, Reference and Notes
Record		
Record Identifier	RMA generated based on NARA assigned organizational identifiers. Paragraph C2.T3.1	Unique record identifier.
Folder Identifier	RMA generated Paragraph C2.T2.1.2.	Foreign Key from Folder Grouping Level May be replaced by grouping for NARA archival action.
Title	RMA captured Paragraph C2.T3.2	Name of record required by DoD 5015.02.
Creator	RMA captured Paragraph C2.T3.5	Creator in Dublin Core Person/Organization creating record Author in DoD 5015.02.
Media	RMA captured Paragraph C2.T3.8	Physical manifestation of record. DoD 5015.02.
Format	RMA captured Paragraph C2.T3.9	Electronic File Application Type. Binding or grouping of physical records DoD 5015.02.
Date Published	RMA captured Paragraph C2.T3.4	Date Created in Dublin Core Date Released/Published DoD 5015.02.
Link to supporting records/files	RMA captured Paragraph C2.2.3.17	Links to other records/files that are necessary to properly render this content. DoD 5015.02. Not record-record links for context.
Original Content	RMA captured Paragraph C2.2.3.1	Embedded original computer file content.
Open Content	RMA shall prompt user to create a file using an accepted standard markup language, such as XML, if one does not already exist.	Embedded XML or other standard markup language content. This is the original record content file converted to a machine readable format.

C5.1.6.3. E-mail. RMAs shall write out and ingest additional information from e-mail messages. These elements are in addition to core record elements.

C5.1.6.3.1. Record Level E-mail Mandatory. RMAs shall write out and ingest the following mandatory metadata for each e-mail record being transferred as specified in Table C5.T2.

Table C5.T2. Record Level E-mail (Defined Mandatory)

Data Element	Data Source	Content, Reference and Notes
Record Email	NA	
Record Identifier	RMA Generated Paragraph C2.T3.1	Link to Core mandatory elements.
Sender	RMA captured Paragraph C2.T3.5	“From” element.
Primary Addresses	RMA captured Paragraph C2.T3.11	“To” element.
Secondary Addresses	RMA captured Paragraph C2.T3.12	“CC” element.
Hidden Addresses	RMA captured Paragraph C2.T3.12	“BCC” element.
Subject	RMA captured Paragraph C2.T3.2	From email subject.
Sent Timestamp	RMA captured. Paragraph C2.T4	Time email left server.
Received Timestamp	If filed on receipt, RMA captured from email header. Paragraph C2.T3.10	If filed on receipt, time email is received on server.
Attachment reference	RMA Generated Paragraph C2.2.4.3	If attachment(s).

C5.1.6.3.2. Record Level Mandatory for Records to be Transferred to NARA

C5.1.6.3.2.1. Scanned Records. RMAs shall write out and ingest the following mandatory metadata for each scanned record being transferred as specified in Table C5.T3.

Table C5.T3. Record Level Scanned (Defined Mandatory)

Data Element	Data Source	Content, Reference and Notes
Record Scanned	NA	
Record Identifier	RMA Generated Paragraph C2.T3.1	

Data Element	Data Source	Content, Reference and Notes
Scanned Image Format and Version	RMA captured Paragraph C2.T5.1.	NARA allows one of the following only; check with NARA for changes: TIFF 4.0 TIFF 5.0 TIFF 6.0 JPEG (all versions) GIF 87a GIF 89a BIIF PNG 1.0.
Image Resolution	RMA captured Paragraph C2.T5.2	Image resolution relative to image encoding standard.
Image Bit Depth	RMA captured Paragraph C2.T5.14	Bit Depth relative to image encoding standard.

C5.1.6.3.2.2. PDF Records. RMAs shall write out and ingest the following mandatory metadata for each PDF record being transferred as specified in Table C5.T4.

Table C5.T4. Record Level PDF (Defined Mandatory)

Data Element	Data Source	Content, Reference and Notes
Record PDF	NA	
Record Identifier	RMA Generated Paragraph C2.T3.1	
Producing Application	RMA captured Paragraph C2.T5.3.	Application used to render content to PDF.
Producing Application Version	RMA captured Paragraph C2.T5.4	
PDF Version	RMA captured Paragraph C2.T5.5	NARA allows versions 1.0 through 1.4 only; check with NARA for changes.

C5.1.6.3.2.3. Digital Photographs. RMAs shall write out and ingest the following mandatory metadata for each digital photograph record being transferred as specified in Table C5.T5.

Table C5.T5. Record Level Digital Photograph (Defined Mandatory)

Data Element	Data Source	Content, Reference and Notes
Record Digital Photograph	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	

Data Element	Data Source	Content, Reference and Notes
Caption	RMA captured Paragraph C2.T5.6.	Narrative text describing each individual image in order to understand and retrieve it. Standard caption information typically includes the “who, what, when, where, why” about the photograph.

C5.1.6.3.2.4. Web Records. RMAs shall write out and ingest the following mandatory metadata for each web record being transferred as specified in Table C5.T6.

Table C5.T6. Record Level Web Records (Defined Mandatory)

Data Element	Data Source	Content, Reference and Notes
Record Web Record	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	
File Name	RMA captured Paragraph C2.T5.7.	The file name of each web site file shall not exceed 99 ASCII characters, and with the path the name shall not exceed 254 ASCII characters.
Web Platform	RMA captured Paragraph C2.T5.8.	Include the specific software applications and where available intended browser applications and versions.
Web Site Name	RMA captured Paragraph C2.T5.9.	Title of the website from the main entry page.
Web Site URL	RMA captured Paragraph C2.T5.10.	Include the filename of the starting page of the transferred content.
Capture Method	RMA captured Paragraph C2.T5.11.	Include name and description of harvester if used. If PDF, include the software and version used to capture the PDF. If more than 1 clearly identify which content was captured by which method.
Capture Date	RMA captured Paragraph C2.T5.12.	Date record was captured.
Contact	RMA captured Paragraph C2.T5.13.	Point of Contact information for person responsible for capturing the web record.

C5.1.6.3.3. Record Level Defined Optional for Records to be transferred to NARA. RMAs should write out and ingest the following defined optional metadata for each record being transferred to NARA.

C5.1.6.3.3.1. Scanned Records. RMAs should write out and ingest the following defined optional metadata for each scanned record being transferred to NARA as specified in Table C5.T7.

Table C5.T7. Record Level Scanned (Defined Optional)

Data Element	Data Source	Content, Reference and Notes
Record Scanned Optional	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	

C5.1.6.3.3.2. PDF Records. RMAs should write out and ingest the following defined optional metadata for each PDF record being transferred to NARA as specified in Table C5.T8.

Table C5.T8. Record Level PDF (Defined Optional)

Data Element	Data Source	Content, Reference and Notes
Record PDF Optional	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	
Creating Application	RMA captured Paragraph C2.T5.15.	Application used to create initial record content, includes version.
Document Security Settings	RMA captured Paragraph C2.T5.16.	Additional Security added during PDF rendering. The document may have multiple pieces that collectively require handlers or a higher classification.

C5.1.6.3.3.3. Digital Photographs. RMAs should write out and ingest the following defined optional metadata for each digital photograph record being transferred to NARA as specified in Table C5.T9.

Table C5.T9. Record Level Digital Photograph (Defined Optional)

Data Element	Data Source	Content, Reference and Notes
Record Digital Photograph Optional	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	
Photographer	RMA captured Paragraph C2.T5.17.	Identify the full name (and rank, if military) and organization (agency, if Federal) of the photographer credited with the photograph, if available.
Copyright	RMA captured Paragraph C2.T5.18.	Indicate for each image whether there is a restriction on the use of that image because of a copyright or other property rights. Agencies must provide, if applicable, the owner of the copyright and any conditions on the use of the photograph(s), such as starting and ending dates of the restriction.

Data Element	Data Source	Content, Reference and Notes
Bit Depth	RMA captured Paragraph C2.T5.19.	Identify the bit depth of the transferred files.
Image Size	RMA captured Paragraph C2.T5.20.	Specify the image height and width of each image in pixels.
Image Source	RMA captured Paragraph C2.T5.21.	Identify the original medium used to capture the images.
Compression	RMA captured Paragraph C2.T5.22.	Identify the file compression method used (if applicable) and the compression level (e.g., medium, high) selected for the image(s).
ICC/ICM profile	RMA captured Paragraph C2.T5.23.	Provide custom or generic color profiles, if available, for the digital camera or scanner used [e.g., sRGB].
EXIF Information	RMA captured Paragraph C2.T5.24.	If available, preserve and transfer to NARA the Exchangeable Image File Format (EXIF) information embedded in the header of image files (as TIFF tags or JPEG markers) by certain digital cameras (e.g., make and model of the digital camera).

C5.1.6.3.3.4. Web Records. RMAs should write out and ingest the following defined optional metadata for each web record being transferred to NARA as specified in Table C5.T10.

Table C5.T10. Record Level Web Record (Defined Optional)

Data Element	Data Source	Content, Reference and Notes
Record Web Record Optional	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	
Content Management System	RMA captured Paragraph C2.T5.25.	Application used to manage files on the web.

C5.1.6.3.4. Mandatory Standard Record Elements. RMAs shall be able to export and import all record core mandatory metadata as well as the mandatory metadata in Table C5.T11.

Table C5.T11. Record (Transfer Mandatory)

Data Element	Data Source	Content, Reference and Notes
Record		
Record Identifier	RMA Generated Paragraph C2.T3.1	Unique record identifier.
Supplemental Marking List	RMA captured Paragraph C2.T3.7	
Date Filed	RMA Generated Paragraph C2.T3.3	

Originating Organization	RMA captured Paragraph C2.T3.6	
--------------------------	-----------------------------------	--

C5.1.6.3.5. Defined-Optional Standard Record Elements. RMAs should be able to export and import the defined optional metadata in the following table when this metadata is included in the RMA as specified in Table C5.T12.

Table C5.T12. Record (Transfer Defined Optional)

Data Element	Data Source	Content, Reference and Notes
Record Defined		
Record Identifier	RMA Generated Paragraph C2.T3.1	Unique record identifier.
Date Received	RMA captured Paragraph C2.T3.10	
Addressees	RMA captured Paragraph C2.T3.11	
Other Addressees	RMA captured Paragraph C2.T3.12	
Location	RMA captured Paragraph C2.T3.13	

C5.1.6.3.6. User Defined-Optional Record Elements. RMAs should be able to export and import Organization-Defined Optional Record Elements as specified in Table C5.T13.

Table C5.T13. Record (Transfer Organization-Defined)

Data Element	Data Source	Content, Reference and Notes
Record Organization Defined	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	Unique record identifier.
Additional Information	As described in provider schema Paragraph C2.T3.14	Provider shall describe in extension schema.

C5.1.6.4. Lifecycle Status Elements. RMAs shall capture and link additional life cycle metadata to records written out for bulk transfer. RMAs shall parse, ingest and link received record lifecycle information into the receiving database and/or repository.

C5.1.6.4.1. Lifecycle Status Elements. RMAs shall be able to export and import the mandatory lifecycle metadata as specified in Table C5.T14.

Table C5.T14. Record Level Lifecycle (Transfer Mandatory)

Data Element	Data Source	Content, Reference and Notes
Record Lifecycle		
Record Identifier	RMA Generated Paragraph C2.T3.1	Unique record identifier.
Folder Identifier	RMA Generated Paragraph C2.T2.2	If folder is used.
Record Category Identifier	RMA Generated Paragraph C2.T1.2	Link to the record category.
Last Disposition Action	RMA Generated Paragraph C2.2.2.3	Lifecycle phase of the record.
Last Disposition Action Date	RMA Generated Paragraph C2.2.2.3	Date the current phase started.
Final Disposition Action	RMA Generated Paragraph C2.2.2.3	From retention schedule of the associated record category.
Final Disposition Date	RMA Generated Paragraph C2.2.2.3	Date final disposition action is to occur.

C5.1.6.4.2. Record Level Organization-Defined Lifecycle Elements. RMAs shall be able to export and import any organization-defined lifecycle metadata as specified in Table C5.T15.

Table C5.T15. Record Level Lifecycle (Transfer Organization-Defined)

Data Element	Data Source	Content, Reference and Notes
Record Lifecycle Organization Defined	N/A	
Record Identifier	RMA Generated Paragraph C2.T3.1	Unique record identifier.
Additional Information	As described in provider schema Paragraph C2.T3.14	Provider shall describe in extension schema.

C5.1.6.5. Record Folder Elements. When records are associated with folders, RMAs shall manage writing out record folders for bulk transfer with the metadata shown in the following paragraphs. RMAs shall parse and process all metadata elements during ingestion. Optionally RMAs shall provide authorized individuals with graphical user interface capabilities to support merging ingested folders into existing file plans.

C5.1.6.5.1. Record Folder Lifecycle Status Elements. RMAs shall capture and link additional life cycle metadata to record folders written out for bulk transfer. RMAs shall parse and ingest the record folder lifecycle information into the receiving RMA.

C5.1.6.5.2. Record Folder Level Mandatory Lifecycle Elements. RMAs shall be able to export and import all mandatory record folder lifecycle elements as specified in Table C5.T16.

Table C5.T16. Folder Level (Defined Transfer Lifecycle Mandatory)

Data Element	Data Source	Content, Reference and Notes
Folder Lifecycle		
Folder Identifier	RMA Generated Paragraph C2.T2.2	If folder is used.
Record Category Identifier	RMA Generated Paragraph C2.T1.2	Link to the record category.
Last Disposition Action	RME Generated Paragraph C2.2.2.3	Lifecycle phase of the folder.
Last Disposition Action Date	RMA Generated Paragraph C2.2.2.3	Date the current phase started.
Final Disposition Action	RMA Generated Paragraph C2.2.2.3	From retention schedule of the associated record. category
Final Disposition Date	RMA Generated Paragraph C2.2.2.3	Date final disposition action is to occur.

C5.1.6.5.3. Record Folder Level Organization-Defined Lifecycle Elements. RMAs shall be able to export and import organization-defined record folder lifecycle elements as specified in Table C5.T17.

Table C5.T17. Folder Level Lifecycle (Transfer Lifecycle Organization-Defined)

Data Element	Data Source	Content, Reference and Notes
Folder Lifecycle Organization Defined	N/A	
Folder Identifier	RMA Generated Paragraph C2.T2.2	If folder is used.
Additional Information	As described in provider schema Paragraph C2.T2.7	Provider shall describe in extension schema.

C5.1.6.5.4. Standard Folder Elements. RMAs shall be able to export and import standard metadata to record folders written out for bulk transfer.

C5.1.6.5.5. Record Folder Level Mandatory Elements. RMAs shall be able to export and import mandatory record folder elements as specified in Table C5.T18.

Table C5.T18. Folder Level (Transfer Mandatory)

Data Element	Data Source	Content, Reference and Notes
Folder		
Folder Identifier	RMA Generated Paragraph C2.T2.2	If folder is used.
Record Category Identifier	RMA Generated Paragraph C2.T1.2	Link to the record category.
Location	RMA captured Paragraph C2.T3.13	If location information is required.
Vital Record Indicator	RMA captured Paragraph C2.T2.4	
Vital Record Review and Update Cycle Period	RMA captured Paragraph C2.T2.5	

C5.1.6.5.6. Record Folder Level Defined Optional Elements. RMAs should be able to export and import defined optional record folder elements as specified in Table C5.T19.

Table C5.T19. Folder Level (Transfer Defined Optional)

Data Element	Data Source	Content, Reference and Notes
Folder Defined Optional		
Folder Identifier	RMA Generated Paragraph C2.T2.2	Link to folder.
Supplemental Marking List	RMA captured Paragraph C2.T2.6	

C5.1.6.5.7. Record Folder Level Organization-Defined Elements. RMAs shall be able to export and import organization-defined record folder elements as specified in Table C5.T20.

Table C5.T20. Folder Level (Transfer Organization-Defined)

Data Element	Data Source	Content, Reference and Notes
Folder Organization Defined	N/A	
Folder Identifier	RMA Generated Paragraph C2.T2.2	Link to folder.
Additional Information	As described in provider schema Paragraph C2.T2.7	Provider shall describe in extension schema.

C5.1.7. Computer Files. RMAs shall be able to transfer and receive any type of computer files.

C5.1.7.1. Computer File Grouping. RMAs shall be able to group records according to the transfer schema and copy them to physical media or via media-less transfer methods (e.g. file transfer protocol) to support archiving and transfer.

C5.1.7.2. Computer File Media Support. RMAs shall be able to read records from transfer media.

C5.1.7.3. Computer File Elements. RMAs shall associate Computer File elements with all record content, no matter the type or source as specified in Table C5.T21.

Table C5.T21. Computer File Core (Defined Mandatory)

Data Element	Data Source	Content, Reference and Notes
Computer File	N/A	
Unique File ID	RMA Generated Paragraph C2.1.1	Unique identifier for this computer file.
File Name	Creating Applications or RMA captured	File name as stored on the media and may be accessible from the file properties.
File Extension	Creating Applications or RMA identified link Paragraph C2.1.1	Extension as stored on the media. The extension may be specific to an application, but that is not consistent. This information may be available from the file properties.
Creating Application	User entered specified or RMA identified link Paragraph C2.1.1	This is a pointer to the specific application that created this computer file. The information may be accessible from the file properties.
File Create Date	RMA and Operating System Paragraph C2.1.1	Date and time stamp for this file's creation. This information is available from the file properties, but may not be the original creation date of the record content.
File Size	RMA and Operating System Paragraph C2.1.1	Computer file size in bytes. (Need to verify that file size is consistent across operating systems that use different data block sizes.)
File Encoding	User Entered Paragraph C2.1.1	ASCII, UNICODE, EBCDIC, encryption standard, compression scheme, etc.
Specific Security	RMA Captured Paragraph C2.1.1	Optional. This covers internal security items such as sheet, protection, macros, PKI and digital signatures, and other features built into document formats.
Computer File	RMA and Operating System Paragraph C2.1.1	Binary content of the file. This data may be text or data associated with a specific application. The information is stored as binary on the media.

C5.2. SUPPORT OF SECURITY INTEROPERABILITY ELEMENTS

RMAAs shall write out and ingest security and/or protective marking information to each record exported from the repository.

C5.2.1. Security Markings. If Chapter 3 is implemented, RMAAs shall write out and ingest security classification marking metadata to each record exported from the repository as specified in Table C5.T22.

Table C5.T22. Security Marking Metadata

Data Element	Data Source	Content, Reference and Notes
Security Classification	N/A	Classification object or record.
Current Classification	RMA Captured Paragraph C3.T1.2	One of Confidential, Secret, Top Secret, or other CAPCO marking.
Initial Classification	RMA Captured Paragraph C3.T1.1	One of Confidential, Secret, Top Secret, or other CAPCO marking.
Supplemental Marking	RMA Captured Paragraph C3.T1.7	List of agency provided informational or protective markings.

C5.2.2. Downgrading and Declassification. If Chapter 3 is implemented, RMAAs shall write out and ingest downgrading and declassification metadata to each record exported from the repository as specified in Table C5.T23. The markings required by the Authorized Classification & Controlled Markings Register (Reference (ai)) should be used.

Table C5.T23. Downgrading and Declassification Metadata

Data Element	Data Source	Content, Reference and Notes
Downgrading/Declassification Data	N/A	Downgrading/declassification object or record.
Event	N/A	Text description of the event upon which information shall be downgraded or declassified.
Date	RMA Captured Paragraph C3.T1.14	Date upon which information shall be downgraded or declassified.
By	RMA Captured Paragraph C3.T1.13	Individual responsible for downgrading or declassifying information.
Reason	RMA Captured Paragraph C3.T1.9	Text reason for downgrade or declassification.
Type	N/A	One of downgrade or declassification.

C5.3. OPTIONAL TRANSFER ELEMENTS

C5.3.1. File Plan Elements (Optional). RMAs should be able to export and import file plan components.

C5.3.1.1. Record Category Mandatory Elements. RMAs should indicate whether disposition management is conducted at the folder or record level for each Record Category. RMAs should be able to export and import mandatory record category elements as specified in Table C5.T24.

Table C5.T24. Record Category (Defined Transfer Mandatory)

Data Element	Data Source	Content, Reference and Notes
Record Category		
Record Category Identifier	RMA Generated Paragraph C2.T1.2	Link to the record category.
Record Category Name	RMA captured Paragraph C2.T1.1	Currently required by DoD 5015.02.
Record Category Description	RMA captured Paragraph C2.T1.3	Currently required by DoD 5015.02.
Disposition Authority	RMA captured Paragraph C2.T1.5	Currently required by DoD 5015.02.
Permanent Record Indicator	RMA captured Paragraph C2.T1.6	Currently required by DoD 5015.02 as transfer or accession to NARA indicator.
Vital Record Indicator	RMA captured Paragraph C2.T1.7	Currently required by DoD 5015.02.
Vital Record Review and Update Cycle Period	RMA captured Paragraph C2.T1.8	Currently required by DoD 5015.02.
Disposition Level	RMA captured Paragraph C2.T1.4	One of Folder or Record.

C5.3.1.2. Disposition Elements. RMAs should be able to export and import disposition components.

C5.3.1.2.1. Event Elements. RMAs should be able to export and import event metadata.

C5.3.1.2.2. Event Mandatory Elements. RMAs should be able to export and import mandatory event elements as specified in Table C5.T25.

Table C5.T25. Events (Defined Transfer Mandatory)

Data Element	Data Source	Content, Reference and Notes
Event		
Event Identifier	RMA Generated Paragraph C2.2.2.8	Unique identifier for this event object.
Event Name	RMA captured Paragraph C2.2.2.8	Text description or name of event.

C5.3.1.2.3. Event Organization-Defined Elements. RMAs should be able to export and import organization-defined event elements as specified in Table C5.T26.

Table C5.T26. Events (Transfer Organization-Defined)

Data Element	Data Source	Content, Reference and Notes
Event Organization Defined		
Event Identifier	RMA Generated Paragraph C2.2.2.8	Link to event.
Additional Information	As described in provider schema Paragraph C2.2.2.8	Provider should describe in extension schema.

C5.3.1.2.4. Trigger Elements. RMAs should be able to export and import disposition trigger metadata.

C5.3.1.2.5. Trigger Mandatory Elements. RMAs should be able to export and import mandatory trigger elements as specified in Table C5.T27.

Table C5.T27. Trigger (Defined Transfer Mandatory)

Data Element	Data Source	Content, Reference and Notes
Trigger		
Trigger Identifier	RMA captured Paragraph C2.2.2.4	Unique identifier for this trigger.
Trigger type	RMA captured Paragraph C2.2.2.4	One of Cutoff, Vital Records Review, or Interim Transfer.
Trigger mode	RMA captured Paragraph C2.2.2.4	One of Event, Time, or Time-Event.
Event	RMA captured Paragraph C2.2.2.8	If Trigger mode is Event or Time-Event.
Time Unit	RMA captured Paragraph C2.2.2.3	One of Daily, Weekly, Monthly, Quarterly, Semi-Annually, or Annually.

Data Element	Data Source	Content, Reference and Notes
Time Unit Type	RMA captured Paragraph C2.2.2.3	One of Calendar or Fiscal.
Time Unit Multiplier	RMA captured Paragraph C2.2.2.3	Number of time units used in calculations.
Trigger Execution Date	User-Entered or RMA Generated where Trigger Mode involves time calculation Paragraph C2.2.2.4	The calendar date the trigger is tripped.
Lifecycle Start Date	RMA Generated Paragraph C2.2.2.5	Retention start date based on trigger.

C5.3.1.2.6. Trigger Organization-Defined Elements. RMAs should be able to export and import organization-defined trigger elements as specified in Table C5.T28.

Table C5.T28. Trigger (Transfer Organization-Defined)

Data Element	Data Source	Content, Reference and Notes
TriggerOrganizationDefined		
Trigger Identifier	RMA Generated Paragraph C2.2.2.4	Unique identifier for this trigger.
Additional Information	As described in provider schema Paragraph C2.2.2.4	Provider should describe in extension schema.

C5.3.1.2.7. Vital Record Review Elements. RMAs should be able to export and import Vital Record Review metadata.

C5.3.1.2.8. Vital Record Review Mandatory Elements. RMAs should be able to export and import mandatory Vital Record Review elements as specified in Table C5.T29.

Table C5.T29. Vital Record Review (Defined Transfer Mandatory)

Data Element	Data Source	Content, Reference and Notes
Vital Record Review		
Vital Record Review Identifier	RMA Generated Paragraph C2.2.7.7.1	Unique identifier for this Vital Record Review.
Vital Record Review type	RMA captured Paragraph C2.2.7.7.1	One of Cutoff, Vital Records Review, or Interim Transfer.
Vital Record Review mode	RMA captured Paragraph C2.2.7.7.1	One of Event, Time, or Time-Event.

Data Element	Data Source	Content, Reference and Notes
Event	RMA captured Paragraph C2.2.2.8	If Vital Record Review mode is Event or Time-Event.
Time Unit	User-Entered Paragraph C2.2.7.7.1	One of Daily, Weekly, Monthly, Quarterly, Semi-Annually, or Annually.
Time Unit Type	User-Entered Paragraph C2.2.7.7.1	One of Calendar or Fiscal.
Time Unit Multiplier	User-Entered Paragraph C2.2.7.7.1	Number of time units used in calculations.
Vital Record Review Execution Date	User-Entered or RMA Generated where Vital Record Review Mode involves time calculation Paragraph C2.2.7.7.1	The calendar date the Vital Record Review is tripped.

C5.3.1.2.9. Vital Record Review Organization-Defined Elements. RMAs should be able to export and import organization-defined Vital Record Review elements as specified in Table C5.T30.

Table C5.T30. Vital Record Review (Transfer Organization-Defined)

Data Element	Data Source	Content, Reference and Notes
Vital Record Review Organization Defined		
Vital Record Review Identifier	RMA Generated Paragraph C2.2.7.7.1	Unique identifier for this Vital Record Review.
Additional Information	As described in provider schema Paragraph C2.2.7.7.1	Provider should describe in extension schema.

C5.3.1.2.10. Lifecycle Phase Elements. RMAs should be able to export and import lifecycle phase metadata.

C5.3.1.2.11. Lifecycle Phase Mandatory Elements. RMAs should be able to export and import mandatory lifecycle phase elements as specified in Table C5.T31.

Table C5.T31. Lifecycle Phase (Defined Transfer Mandatory)

Data Element	Data Source	Content, Reference and Notes
Lifecycle Phase		
Lifecycle Phase Identifier	RMA Generated Paragraph C2.2.2.3	Unique identifier for this phase object.
Lifecycle Phase Name	RMA captured Paragraph C2.2.2.3	Phase Name such as Records Holding Area, Current File Area, etc.
Lifecycle Phase Precedence	RMA captured Paragraph C2.2.2.3	Order or precedence of this phase. Phases may share precedence.

C5.3.1.2.12. Lifecycle Phase Organization-Defined Elements. RMAs should be able to export and import organization-defined lifecycle phase elements as specified in Table C5.T32.

Table C5.T32. Lifecycle Phase (Transfer Organization-Defined)

Data Element	Data Source	Content, Reference and Notes
Lifecycle Phase Organization Defined	NA	
Lifecycle Phase Identifier	RMA Generated Paragraph C2.2.2.3	If folder is used.
Additional Information	As described in provider schema Paragraph C2.2.2.3	Provider should describe in extension schema.

C5.4. TRANSFER ACCESS CONTROL

Table C5.T33. summarizes requirements that refer to “authorized individuals” and offers additional information regarding user-type responsibilities. In general, Application Administrators are responsible for setting up the RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users.

Table C5.T33. Authorized Individual Requirements for Transfers

Requirement	Application Administrator	Records Manager	Privileged User
C5.T33.1. (C5.1.3.2.) <u>Transfer Schema Organization-Defined</u> add to or remove from the schema organization-defined, defined optional, and any vendor provided metadata fields.	During setup or at export.	At export.	NA

Requirement	Application Administrator	Records Manager	Privileged User
C5.T33.2. (C5.1.4.2.) <u>Transfer Schema Metadata Organization-Defined Mapping.</u> ... map metadata to schema elements to support export and ingest..	During setup or at export/import.	At export/import.	NA
C5.T33.3. (C5.1.5.) <u>Organization-Defined Elements Export Schemas and Rendering Aids.</u> ... implement an export schema based on this Standard and the vendor provided DTD. ... remove the default if not needed by recipient.	During setup or at export/import.	At export/import.	NA
C5.T33.4. (C5.1.6.) <u>Record Elements.</u> ... merging ingested records into existing file plans.	During setup or at import.	At import.	NA
C5.T33.5. (C5.1.7.4) <u>Record Folder Elements.</u> ... merging ingested folders into existing file plans.	During setup or at import.	At import.	NA

C6. CHAPTER 6

NON-MANDATORY FEATURES

C6.1. REQUIREMENTS DEFINED BY THE ACQUIRING OR USING ACTIVITY

In addition to the baseline requirements defined by this Standard, the acquiring or using activity should identify the following Agency-, site-, and installation-unique requirements. These requirements are not mandatory for DoD compliance.

C6.1.1. Storage Availability. The size of the storage space required for its organizational records, along with the related record metadata and associated audit files.

C6.1.2. Documentation. The type and format of desired documentation, such as user guides, technical manuals, and installation procedures, to be provided by the vendor.

C6.1.3. System Performance. The RMA system availability, reliability, response times, and downtimes that shall satisfy its business requirements.

C6.1.4. Hardware Environment. The hardware environment (e.g., mainframe, client-server, or personal computer) and identify the platforms (servers and workstations) on which an RMA is to run.

C6.1.5. Operating System Environment. The operating system environment (e.g., UNIX, Windows, Linux, Macintosh) on which an RMA is to be run.

C6.1.6. Network Environment. The Local Area Network (LAN), Wide Area Network (WAN) or other network topology (e.g., Ethernet bus, star, or token-ring) and the Network Operating System (NOS) (e.g., Novell, Banyan Vines, Windows 2003 Server) on which an RMA is to be run.

C6.1.7. Protocols. The protocols, (e.g. Transmission Control Protocol/Internet Protocol (TCP/IP), Simple Mail Transfer Protocol (SMTP), or X.400) that an RMA is to support.

C6.1.8. Electronic Mail Interface. The e-mail application(s) with which an RMA is to interface.

C6.1.9. End-User Orientation and Training. The training requirements for Records Managers and end-users.

C6.1.10. Harvesting Web Records. The requirements necessary to meet NARA's guidance on harvesting web content records. This includes links redirection, collection of script and business logic, and other archival management specific to web records.

C6.2. OTHER USEFUL RMA FEATURES

Many RMA products provide the following time and laborsaving functions, either as standard or optional features to enhance the utility of the system. The acquiring or using activity should determine local requirements for any of the following RMA features.

C6.2.1. Making Global Changes. RMAs should provide the capability for authorized individuals to make global changes to the record category names, record category identifiers, disposition components, and originating organization. In addition, RMAs should provide the capability to reorganize the file plan and automatically propagate the changes resulting from the reorganization to the affected records and record folders.

C6.2.2. Bulk Loading Capability. RMAs should provide the capability for authorized individuals to bulk load:

C6.2.2.1. An Agency's pre-existing file plan.

C6.2.2.2. Electronic records.

C6.2.2.3. Record metadata.

C6.2.3. Interfaces to Other Software Applications. RMAs should interface with various office automation packages such as electronic mail, word processors, spreadsheets, databases, desktop publishers, web site harvesters, handheld devices, instant messengers, declassification review systems and electronic data interchange systems, as specified by the using activity.

C6.2.4. Report Writer Capability. RMAs should provide the capability to generate reports on the information held within the RMA's repository based upon user-developed report templates or user queries.

C6.2.5. On-Line Help. RMAs should have an on-line help capability for access to user operational information. Help should be context sensitive to the screens from which help was launched. Global help should be available from a toolbar menu item or keyboard shortcut.

C6.2.6. Document Imaging Tools. RMAs should be capable of interfacing with document imaging and workflow software and hardware. These should be consistent with the DoD Automated Document Conversion Master Plan.

C6.2.7. Fax Integration Tools. An organization may determine a need for RMAs to interface with desktop or server-based fax products to capture fax records in their electronic format.

C6.2.8. Bar Code Systems. An organization may determine a need to use a bar code system with RMAs. The following items show how bar code technology can be used to support records management tasks:

C6.2.8.1. File and correspondence tracking to positions, sections, or staff members.

C6.2.8.2. Creating, printing, and reading labels for non-electronic records.

C6.2.8.3. Boxing records for transfer.

C6.2.8.4. Box tracking for records-holding facility operations.

C6.2.8.5. Workflow tracking.

C6.2.8.6. Posting changes in disposition.

C6.2.8.7. Recording audit and census functions.

C6.2.9. Retrieval Assistance. RMAs should have additional search and retrieval features, such as full text search, to assist the user in locating records. The search utility should include the capability to create, modify, or import additional thesauri.

C6.2.10. File Plan Component Selection/Search Capability. RMAs should provide methods for assisting the user in the selection of the file plan components to be assigned to a record, such as priority-ordered lists or directed searches.

C6.2.11. Workflow and/or Document Management Features. An organization may determine that RMAs should have the capability to manage working and draft versions of documents and other potential record materials as they are being developed.

C6.2.12. Records Management Forms and Other Forms. An organization may determine that RMAs should be capable of interfacing with forms generating software and/or have the capability to generate completed standard records management forms, such as:

C6.2.12.1. Standard Forms 115 and 115-A, "Request for Records Disposition Authority."

C6.2.12.2. Standard Forms 135 and 135-A, “Records Transmittal and Receipt.”

C6.2.12.3. Standard Form 258, “Agreement To Transfer Records To The National Archives Of The United States.”

C6.2.12.4. NARA Form 14012, “Database Record Layout.”

C6.2.12.5. NARA Form 14097, “Technical Description for Transfer of Electronic Records to the NARA.”

C6.2.13. Printed Labels. RMAs should provide the capability to produce hard-copy codes or identifiers in the form of labels or other products, as required.

C6.2.14. Viewer. RMAs should provide the capability to view each file in its stored format or a human-readable rendition.

C6.2.15. Web Capability. RMAs should provide the capability to allow the user to interface through a web browser or other platform independent means.

C6.2.16. Government Information Locator Service (GILS). RMAs should have the capability to implement the requirements of GILS (Reference (k)). GILS was established to identify public information resources throughout the Federal Government, describe the information available in those resources, and provide assistance in obtaining this information.

C6.2.17. Enhanced Support for Off-line Records. RMAs should provide additional features for managing boxes of hard copy records and other off-line archives.

C6.2.18. Organizational Customization

C6.2.18.1. Data Entry Screens. RMAs should provide the capability for authorized individuals to arrange record metadata components and organization-defined record components on data entry screens to be used for filing.

C6.2.18.2. Default Metadata Values. RMAs should provide the capability for authorized individuals to assign default values to record metadata components and organization-defined record components that shall be shown data entry screens to be used for filing.

C6.2.18.3. User Picklists. RMAs should provide the capability for authorized users to create and maintain shortened “quick-pick” lists from the authorized lists.

C6.2.18.4. User Templates. RMAs should provide the capability for authorized users to create and maintain templates that automatically populate commonly used data into record metadata fields.

C6.3. SEARCH AND DISCOVERY INTEROPERABILITY

RMAs should make designated records available for public search and retrieval and optionally support e-FOIA/e-Privacy Act requests.

C6.3.1. Service-Oriented Discovery. RMAs should provide graphical user interface capabilities to allow authorized individuals to make holdings available via a service-oriented architecture. RMA implementation should support compliance with the Global Information Grid's Service Oriented Architecture policies (OASIS Specification (References (al)), Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Plan (Reference (am)), DoD Chief Information Officer Architecture (Reference (an)), Joint Requirements Oversight Council Memorandum (Reference (ao)), and DoD Directive (Reference (ap))).

C6.3.1.1. Holdings Announcement. RMAs should provide graphical user interface capabilities to allow authorized individuals to create/update and publish a holdings announcement to the enterprise services registry. Such a holdings announcement should include DDMS-formatted (Reference (d)) metadata, in order to provide visibility for holdings compliant with DoDD 8320.2 (References (r) and (s)). RMAs shall provide graphical user interface capabilities to allow authorized individuals to create and publish a removal of services announcement to the enterprise services registry.

C6.3.1.2. Service Connection Instructions. RMAs should provide graphical user interface capabilities to allow authorized individuals to create/update and publish service connection instructions to the enterprise services registry.

C6.3.1.3. Service Requests and Queries. RMAs should make their holdings accessible to the Enterprise, conforming to DoDD 8320.2 (Reference (r) and (s)) by responding to service requests and queries that are composed in accordance with the published service connection instructions. RMAs should include the capability to provide access to record metadata visible to both known and authorized unanticipated users in the DoD enterprise. Additionally, RMAs should include the capability to make web-enabled records management business and computing processes visible to the DoD enterprise.

C6.4. ACCESS CONTROL

Table C6.T1. summarizes requirements that refer to “authorized individuals” and offers additional information regarding user-type responsibilities. In general, Application

Administrators are responsible for setting up an RMA infrastructure. Records Managers are responsible for records management administration. Privileged Users are those who are given special permissions to perform functions beyond those of typical users.

Table C6.T1. Authorized Individual Requirements (Defined Optional)

Requirement	Application Administrator	Records Manager	Privileged User
C6.T1.1. (C6.2.1.) <u>Making Global Changes</u> make global changes to the record category names, record category identifiers, disposition components, and originating organization. ... reorganize the file plan and automatically propagate the changes .	Optional access as needed.	As needed.	Permitted portions of file plan only.
C6.T1.2. (C6.2.2.) <u>Bulk Loading Capability</u> . RMAs should provide the capability for authorized individuals to bulk load:	Optional access as needed.	As needed.	NA
C6.T1.3. (C6.2.18.1.) <u>Data Entry Screens</u> arrange record metadata components and organization-defined record components on data entry screens to be used for filing.	During setup.	As needed.	NA
C6.T1.4. (C6.2.18.2.) <u>Default Metadata Values</u> assign default values to record metadata components and organization-defined record components ...	During setup.	As needed.	NA
C6.T1.5. (C6.2.18.3.) <u>User Picklists</u>provide the capability for authorized users to create and maintain shortened “quick-pick” lists from authorized lists.	During setup.	As needed.	NA
C6.T1.6. (C6.3.1.) <u>Service Oriented Discovery</u> allow authorized individuals to make holdings available via a service oriented architecture.	Optional access as needed.	As needed.	NA
C6.T1.7. (C6.3.1.1.) <u>Holdings Announcement</u> create/update and publish a holdings announcement to the enterprise services registry. ...create and publish a removal of services announcement to the enterprise services registry.	Optional access as needed.	As needed.	NA
C6.T1.8. (C6.3.1.2.) <u>Service Connection Instructions</u> create/update and publish service connection instructions to the enterprise services registry.	Optional access as needed.	As needed.	NA