REPUBLIC OF NAMIBIA

OFFICE OF THE PRIME MINISTER

PUBLIC SERVICE OF NAMIBIA

DESIGN CRITERIA STANDARDS FOR ELECTRONIC RECORDS MANAGEMENT SOFTWARE APPLICATIONS

April 2007

PROJECT DOCUMENT:
ELECTRONIC DOCUMENTS AND RECORDS MANAGEMENT SYSTEM (2007)

This document is based on US Department of Defense Standard: DoD 5015.2-STD, June 19, 2002

TABLE OF CONTENTS

Page

TABLES

REFERENCES

Namibian Sources:

(aa) The National Archives Act of 1992 (Act no 12 of 1992)

(bb) Code of Procedure on Archives and Records, issued in terms of section 12 of the National Archives Act (1999) current edition

(cc) Office of Prime Minister Filing System (file 2/7/3/1), approved by the Director of Archives, current edition

(dd) Treasury Instructions of Namibia, current edition (chapter FE on records)

(ee) Public Service Act of 1995 (Act no 13 of 1995)

(ff) Staff Rules chapter issued in terms of the Public Service Act

(gg) ISO (standard) XXXX on electronic records

(hh) ISO standard 2788 or 5964 thesaurus

(ii) IRMT advisories on electronic records management

DL1. DEFINITIONS

DL1.1.1. Access.

The ability or opportunity to gain knowledge of stored information.

DL1.1.2. Accession.

To transfer physical and legal custody of documentary materials to an archival institution.

DL1.1.3. Addressee.

The name of the organization to which or individual to whom a record is addressed.

DL1.1.4. Application Administrators.

Individuals who are responsible for setting up the RMA infrastructure.

DL1.1.5. 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.

DL1.1.6. 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. May be used to identify unauthorized actions in relation to the records, e.g., modification, deletion, or addition.

DL1.1.7. Authenticity.

A condition that proves that a record is genuine based on its mode (i.e., method by which a record is communicated over space or time), form (i.e., 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.

DL1.1.8. Authorized Individual.

A Records Officer or other person specifically designated by the Records Officer as responsible for managing various aspects of an organization's records.

DL1.1.9. Author or Originator.

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

DL1.1.10. Biometrics.

Biometrics are automated methods of authenticating or verifying an individual based upon a physical or behavioral characteristic of that individual.

DL1.1.11. Bulk Load.

Automatically importing data.

DL1.1.12. Classified Information.

Information that has been determined pursuant to Archives Code (see reference xxx) or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

DL1.1.13. Classification Markings.

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.

DL1.1.14. Copy.

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

DL1.1.15. Create.

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

DL1.1.16. Cutoff.

To cut off records in a file means to break, or end, them at regular intervals to permit their 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.

DL1.1.16.1. For records with retention periods of less than 1 year. Cut off 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).

DL1.1.16.2. For records with retention periods of 1 year or more. Cut off 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.

DL1.1.16.3. For records with retention periods based on an event or action. Cut off on the date the event occurs or 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.

DL1.1.16.4. For records with retention periods based on a specified time period after an event or action:

DL1.1.16.4.1. Place in an inactive file on the date the event occurs or the action is completed and cut off the inactive file at the end of each fiscal (or calendar) year; then apply the retention period. 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.

DL1.1.16.4.2. Cutoff is sometimes abbreviated as COFF and is also called file cutoff or file break.

DL1.1.17. 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 the Archives Code or Treasury Instructions, or by the records officer.

DL1.1.18. Database.

In electronic records, a set of data elements, consisting of at least one file or of a group of integrated files, usually stored in one location and made available to several users.

DL1.1.19. Database Management System (DBMS).

A software system used to access and retrieve data stored in a database.

DL1.1.20. Data Element.

A combination of characters or bytes refers to one separate piece of information, such as name, address, or age.

DL1.1.21. Date Filed.

The date and time that an electronic document was filed in the RMA and thus became a record. This date and time will normally be assigned by the computer at the time the record is filed in the RMA.

DL1.1.22. Declassification.

The authorized change in the status of information from classified information to unclassified information.

DL1.1.23. Declassification Guide.

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.

DL1.1.24.

DL1.1.25. Delete.

The process of permanently removing, erasing, or obliterating recorded information from a medium, especially a reusable magnetic disk or tape.

DL1.1.26.

DL1.1.27.

DL1.1.28. 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.

DL1.1.29. Disposition.

Those actions taken regarding Public Service records after they are no longer required to conduct current ministerial business. These actions include:

DL1.1.29.1. Transfer of records to ministerial storage facilities or National Archives(NA)

DL1.1.29.2. Transfer of records from one ministry to another.

DL1.1.29.3. Transfer of permanent records to the National Archives.

DL1.1.29.4. Disposal of temporary records no longer needed to conduct ministry 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 NA has approved the donation.

DL1.1.30. Disposition Action.

Action to be taken when a disposition date occurs (e.g., freeze, interim transfer, accession, or destroy).

DL1.1.31. Disposition Action Date.

The fixed date on which the records in a file become due for final disposition.

DL1.1.32. Disposition Authority.

Legal authority that empowers an ministry to transfer permanent records to the National Archives or to carry out the disposal of temporary records. Must be obtained from NA and also, for certain records proposed as temporary, from the Treasury

DL1.1.33. Disposition Instruction.

Directions for cutting off records and carrying out their disposition (transfer, retirement, or destruction) in compliance with NA's regulations and the Treasury Disposition instructions in an RMA include retention-related fields such as authority, transfer location, active or dormant chronological retention periods, and conditional retention periods.

DL1.1.34. Disposition Instruction Type.

One of three ways of scheduling a disposition instruction: time, event, or a combination of both time and event. See **DL1.1.43.**, **DL1.1.86.**, and **DL1.1.87.**

DL1.1.35. Document.

Information set down in any physical form or characteristic. A document may or may not meet the definition of a record. See section 1 of Act no 2 of 1992

DL1.1.36. Document Management Application (DMA).

A system used for managing documents that allows users to store, retrieve, and share them with security and version control. A word processor can integrate DMA support so that you can create, edit, and manage your documents through the word processor. DMAs are sometimes called Electronic Document Management Systems (EDMSs).

DL1.1.37. 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.

DL1.1.38. Edit.

Function that allows the user to change an existing record's metadata.

DL1.1.39. Electronic Document Management (EDM).

The management of different kinds of documents in an enterprise that uses computer programs and storage. An EDM system allows an enterprise and its users to create a document or capture a hard copy in electronic form, store, edit, print, process, and otherwise manage documents in image, video, and audio, as well as in text form. An EDM system usually provides a single view of multiple databases and may include scanners for document capture, printers for creating hard copies, storage devices such as redundant array of independent disks systems, and computer server and server programs for managing the databases that contain the documents.

DL1.1.40. 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.

DL1.1.41. Electronic Mail System.

A computer application used to create, receive, and transmit messages and other documents electronically. This definition does not include file transfer utilities (software that transmits files between users but that does not retain any transmission data); computer systems used to

collect and process data organized into data files or databases; and word-processing documents not transmitted via an e-mail system.

DL1.1.42. Electronic Record.

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 the Archives Act of 1992.

DL1.1.43. 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 when no longer needed for current operations."

DL1.1.44. File.

An arrangement of records.

DL1.1.44.1. 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.

DL1.1.44.2. When used as a verb, this term is used to define the act of assigning and storing records in accordance with the file plan.

DL1.1.45. File Plan.

A document containing the identifying number, title, description, and disposition authority of files held or used in an office. See reference (on OPM filing system)

DL1.1.46. Format.

For electronic records, format 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 6.1 for Windows; or Microsoft Word 7.0 for Windows. For non-electronic records, the format refers to its physical form: e.g., paper, microfilm, and video.

DL1.1.47. 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.

DL1.1.48. Government Information Locator Service (GILS).

A Government service to help the general public locate and access information throughout the Government (to be revised dependant on GRN Portal requirements / access to records laws, etc).

DL1.1.49. Imaging Tools.

Software and hardware that works together to capture, store, and recreate images.

DL1.1.50. 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.

DL1.1.51. Location of Record.

A pointer to a record's location. Examples: an operating system path and filename, the location of a file cabinet, or the location of a magnetic tape rack.

DL1.1.52. Media Type.

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

DL1.1.53. Metadata.

Data describing stored data: that is, data describing the structure, data elements, interrelationships, and other characteristics of electronic records.

DL1.1.54. Move.

Function that allows the user to relocate records and metadata.

DL1.1.55. Multiple Sources.

Information classified based on two or more source documents, classification guides or combination of both.

DL1.1.56. Office Applications.

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.

DL1.1.57. Optical Character Recognition (OCR).

The recognition of printed or written text character by a computer. This involves photoscanning of the text character-by-character, analysis of the scanned-in image, and then translation of the character image into character codes, such as ASCII, commonly used in data processing.

DL1.1.58. Original Classification.

An initial determination that information requires, in the interest of national security, protection against unauthorized disclosure.

DL1.1.59. Originating Organization.

Official name or code identifying the office responsible for the creation of a document.

DL1.1.60. Permanent Record.

Records appraised by NA as having sufficient historical or other value to warrant continued preservation by the Government beyond the time they are normally needed for a particular ministry's administrative, legal, or fiscal purposes.

DL1.1.61. Privileged Users.

Individuals who are given special permission to perform functions beyond those of typical users.

DL1.1.62. Publication Date.

The date and time that the author or originator completed the development of or signed the document (ISBN number). 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 and thus became a record.

DL1.1.63. Rebuild.

Reconstructing the RM environment after a disaster.

DL1.1.64. Receipt Data.

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 ministry. If receipt data are provided by the computer system, they are a required part of documents or records received through electronic mail.

DL1.1.65. Record.

Information, regardless of medium, detailing 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 ministry under law or in connection with the transaction of public business. Records are preserved or appropriate for preservation by that ministry 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.

DL1.1.66. 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.

DL1.1.67. Record Category Identifier.

An ministry's alphanumeric or numeric identifier indicating a unique record category.

DL1.1.68. 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.

DL1.1.69. 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.

DL1.1.70. 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 government policies and transactions and effective and economical management of ministry and organizational operations.

DL1.1.71. Records Management Application (RMA).

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.

DL1.1.72. Records Officers.

Individuals who are responsible for records management administration.

DL1.1.73. Referential Integrity.

Ensuring that all references are updated or deleted as necessary when a key reference is changed in a database environment.

DL1.1.74. 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.

DL1.1.75. Relational Integrity.

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."

DL1.1.76. Rendition.

Replication that provides the same content but differs from the reference because of storage format, or storage medium.

DL1.1.77. Repository for Electronic Records.

A direct access device on which the electronic records and associated metadata are stored.

DL1.1.78. 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.

DL1.1.78.1. 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).

DL1.1.78.2. 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:

DL1.1.78.2.1. "After completion" (as of a study, project, audit).

DL1.1.78.2.2. "After sale or transfer" (as of personal or real property).

DL1.1.78.2.3. "After publication" (as of monthly reports).

DL1.1.78.2.4. "After superseded" (as of an administrative directive).

DL1.1.78.2.5. "After revision or cancellation" (as of a form).

DL1.1.78.2.6. "After acceptance or rejection" (as of an application).

DL1.1.79. Scheduled Records.

Records whose final disposition has been approved by NA.

DL1.1.80. Screening.

Aggregating and reviewing records for management and disposition purposes.

DL1.1.81. Source Document.

An existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

DL1.1.82.

DL1.1.83. Storage.

Space for non-active records. Can be digital, optical, or cubic feet OR cubic metres.

DL1.1.84. Subject.

The principal topic addressed in a record.

DL1.1.85. Supplemental Markings.

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)."

DL1.1.86. 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."

DL1.1.87. Time-Event Disposition.

A disposition instruction specifying that a record shall be disposed of 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.

DL1.1.88. 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 ministry storage facilities or FRCs, from one ministry to another, or from office or storage space to the National Archives for permanent preservation. Transfer does not relieve the owning organization of legal and management responsibilities for non-permanent records. Accessioning permanent records to NA does transfer legal ownership and responsibility for the records to NA.

DL1.1.89. Transmission Data.

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.

DL1.1.90. Unscheduled Records.

Records that do not have a NA-approved final disposition.

DL1.1.91. Upgrade.

A determination that certain classified 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.

DL1.1.92. User-Definable Fields.

Fields defined during application configuration by authorized individuals to support organization-specific information management and access requirements.

DL1.1.93. Version.

One of a sequence of documents having the same general form and specific subject and purpose. The sequence often reflects successive changes to a document.

DL1.1.94. View.

Function that allows the user to look at the metadata and content of a record in a viewer or other application.

DL1.1.95. Vital Records.

Essential ministry 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 ministry operations, and related policy or procedural records assisting ministry 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.

DL1.1.96. 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.

AL1.1. ABBREVIATIONS AND ACRONYMS

AL1.1.1.	**AIS**	Automated Information Systems
AL1.1.4.	**CAC**	Common Access Card
AL1.1.6.	**CGM**	Computer Graphics Metafile
AL1.1.7.	**COFF**	Cutoff
AL1.1.8.	**COTS**	Commercial-off-the-Shelf
AL1.1.9.	**DBMS**	Database Management System
AL1.1.12.	**DMA**	Document Management Application
AL1.1.16.	**EDM**	Electronic Document Management
AL1.1.17.	**EDMS**	Electronic Document Management System
AL1.1.18.	**E-mail**	Electronic mail
AL1.1.22.	**GAO**	**(Treasury of Namibia)**
AL1.1.23.	**GILS**	Government Information Locator Service
AL1.1.24.	**GRS**	General Records Schedule
AL1.1.25.	**ISO**	International Standards Organization
AL1.1.26.	**IT**	Information Technology
AL1.1.28.	**JPEG**	Joint Photographic Experts Group
AL1.1.29.	**LAN**	Local Area Network
AL1.1.30.	**NA**	National Archives of Namibia
AL1.1.32.	**NOS**	Network Operating System
AL1.1.34.	**OCR**	Optical Character Recognition
AL1.1.38.	**PKI**	Public Key Infrastructure
AL1.1.39.	**RM**	Records Management
AL1.1.40.	**RMA**	Records Management Application
AL1.1.41.	**RMTF**	Records Management Task Force
AL1.1.42.	**SDE**	Standardized Data Element
AL1.1.43.	**SMTP**	Simple Mail Transfer Protocol
AL1.1.44.	**SQL**	Structured Query Language
AL1.1.45.	**STD**	Standard
AL1.1.46.	**TCP/IP**	Transmission Control Protocol/Internet Protocol
AL1.1.49.	**WAN**	Wide Area Network

C1. CHAPTER 1
GENERAL INFORMATION

C1.1. PURPOSE

This (draft) Standard sets forth mandatory baseline functional requirements, and identifies non-mandatory features deemed desirable for Records Management Application (RMA) software. This standard incorporates requirements for classified marking, access control, declassification and downgrading, and other issues which have the functional equivalent application of the Public Service manual filing system directives. All Offices/Ministries/Agencies shall use this (draft) Standard in the implementation of their records management programs. This standard describes the minimum records management requirements that must be met in accordance with and complies with the guidance and implementing code and directives promulgated by the National Archives. Also, the word "shall" identifies mandatory system standards and the word "should" identifies design objectives that are desirable but not mandatory.

(Note: This (draft) Standard is the equivalent of Staff Rules issued in terms of the Public Service Act no 13 of 1995. It is issued in draft format as guide in the execution of the Electronic Documents and Records Management Systems (EDRMS) project being piloted first in the Office of the Prime Minister. It will be finalized once the pilot phase of EDRMS is concluded and will be issued as a final version Staff Rule to coincide with the implementation of the project across the Public Service.)

C1.2. LIMITATIONS

This Standard addresses a minimum set of baseline functional requirements applicable to all RMAs used within the Government of Namibia. For the NA/DPSITM to certify that an RMA is compliant with this Standard, these minimum requirements must be met, regardless of organizational and site-specific needs. User organizations may identify additional requirements to satisfy their site-specific needs, but these functions will not be certified as compliant by NA/DPSITM until certified according to this standard. Some examples of site-specific needs are the capability to label prvacy data and data exempt from release under the relevant statutes, and the capability of adopting features described as optional in Chapter 3 of this Standard. These requirements will be addressed in a later version of this Standard. Additionally, future versions of this Standard will address interface with the incorporation of standard data elements, and interoperability within the organization's enterprise information environment, and among disparate RMAs.

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.

C2.1.2. Accommodating Dates and Date Logic. RMAs shall correctly accommodate and process information that contains dates in current, previous, and future centuries. The capability shall include, but not be limited to, century recognition, calculation, and logic that accommodates 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. Implementing Standard Data. RMAs shall allow for the implementation of standardized data i accordance with)). 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 data standards. This requirement implies the capability for adding user-defined metadata fields and modifying existing field labels.

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 one previously verified version of backward compatibility.

C2.1.5. Accessibility. The available documentation for RMAs shall include product information that describes features that address For web-based applications, 36

C2.2. DETAILED REQUIREMENTS

C2.2.1. Implementing File Plans

C2.2.1.1. RMAs shall provide the capability for 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). Mandatory file plan components are shown in Table C2.T1. Mandatory in the 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. Mandatory in the Data Collection Required by User column indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not mandatory in the Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated. The file plan components should be organized into logical sets that, when populated, will provide all the file plan references necessary to properly annotate (file) a record.

Table C2.T1. File Plan Components:

Table C2.T1. File Plan Components				
Requirement	**File Plan Component**	**Structure**	**Data Collection Required by User**	**Reference / Comment**
C2.T1.1.	Record Category Name	Mandatory	Mandatory	RMTF
C2.T1.2.	Record Category Identifier	Mandatory	Mandatory, RMAs shall ensure unique	RMTF
C2.T1.3.	Record Category Description	Mandatory	Mandatory	RMTF
C2.T1.4.	Disposition Instructions	Mandatory	Mandatory	NA Code and Treasury Instructions
C2.T1.5.	Disposition Authority	Mandatory	Mandatory	RMTF & TI
C2.T1.6	Permanent Record Indicator	Mandatory	Mandatory	
C2.T1.7.	Vital Record Indicator	Mandatory	Mandatory	
C2.T1.8.	Vital Record Review and Update Cycle Period	Mandatory, conditional on Vital Record Indicator	Mandatory, conditional on Vital Record Indicator	
C2.T1.9.	User Definable Fields	Mandatory / Undefined	Optional	Multiple user-defined fields shall be supported

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

C2.2.1.3. RMAs shall provide the capability for only authorized individuals to create, edit, and delete record folder components and their identifiers. Each component identifier shall be linked to its associated component and to its higher-level file plan component identifier(s). Mandatory record folder components are shown in Table C2.T2. Mandatory in the Structure column 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. Mandatory in the Data Collection Required by User column indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not mandatory in the Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.

Table C2.T2. Record Folder Components:

Table C2.T2. Record Folder Components				
Requirement	**File Plan Component**	**Structure**	**Data Collection Required by User**	**Reference / Comment**
C2.T2.1.	Record Folders	Mandatory	Optional (although the user is not required to create folders for every category, the RMA shall provide the capability to allow the user to do so)	Folders are not required for all categories. For example, categories with the disposition "destroy when superseded" can be managed at the record level rather than at the folder level.
C2.T2.1.1.	Folder Name	Mandatory	Mandatory	
C2.T2.1.2.	Folder-Unique Identifier	Mandatory	Mandatory, RMAs shall ensure unique	
C2.T2.1.3.	Location	Mandatory	Mandatory if not in RMA repository	RMTF
C2.T2.1.4.	Vital Record Indicator	Mandatory	Mandatory, inherited from Record Category (can be changed by authorized individuals)	
C2.T2.1.5.	Vital Record Review and Update Cycle Period	Mandatory, conditional on Vital Record Indicator	Mandatory, conditional on Vital Record Indicator	
C2.T2.1.6.	Supplemental Marking List	Mandatory	Optional	Multiple supplemental marking entry selections shall be supported.
C2.T2.1.7.	User Definable Fields	Mandatory / Undefined	Optional	Multiple user-definable field

C2.2.1.4. RMAs shall ensure that identifiers (e.g., folder identifiers, record category identifiers) are unique so that ambiguous assignments, links, or associations cannot occur.

C2.2.1.5. RMAs shall provide the capability to allow only an authorized individual to define and attach user-defined business rules and/or access logic to any metadata field including user-defined fields.

C2.2.1.6. RMAs shall provide the capability to sort, view, save, and print user-selected portions of the file plan, including record folders.

C2.2.2. Scheduling Records

C2.2.2.1. RMAs shall provide the capability for only authorized individuals to view, create, edit, and delete disposition schedule components of record categories.

C2.2.2.2. RMAs shall provide the capability for defining multiple phases (e.g., transfer to inactive on-site storage, transfer to off-site storage) within a disposition schedule.

C2.2.2.3. RMAs shall provide the capability for only authorized individuals to define the cutoff criteria and, for each life-cycle phase, the following disposition components for a record category:

C2.2.2.3.1. Retention Period (e.g., fiscal year).

C2.2.2.3.2. Disposition Action (interim transfer, accession, permanent, or destroy).

C2.2.2.3.3. Interim Transfer or Accession Location (if applicable).

C2.2.2.4. RMAs shall, as a minimum, be capable of scheduling and rescheduling each of the following three types of cutoff and disposition instructions. See reference (d).

C2.2.2.4.1. Time Dispositions, where records are eligible for disposition immediately after the conclusion of a fixed period of time following user-defined cutoff (e.g., days, months, years).

C2.2.2.4.2. Event Dispositions, where records are eligible for disposition immediately after a specified event takes place (i.e., event acts as cutoff and there is no retention period).

C2.2.2.4.3. Time-Event Dispositions, where the timed retention periods are triggered after a specified event takes place (i.e., event makes the record folder eligible for closing and/or cutoff and there is a retention period).

C2.2.2.5. RMAs shall provide the capability to automatically calculate the complete life cycle, including intermediate phases, of record folders and records not in folders.

C2.2.2.6. RMAs shall provide the capability for rescheduling dispositions of record folders and/or records (those 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 associated with a disposition.

C2.2.2.7. The RMA shall provide recalculation of the record life cycle based on changes to any life-cycle date and set the filing status (i.e., open, closed) of the folder 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 one or more record folder(s) to a record, or for categories to be managed at the record level, provide the capability to associate a record category to a record.

C2.2.3.2. Mandatory record metadata components are shown in Table C2.T3. Mandatory in the Structure column 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. Mandatory in the Data Collection Required column indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not mandatory in the Data Collection column, RMAs 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	Structure	Data Collection Required	Reference/Comment
	Record Identifiers, Markings, and Indicators			
C2.T3.1.	Unique Record Identifier	Mandatory, system generated (All)	Mandatory (System Generated, not editable)	

Table C2.T3. Record Metadata Components (Continued)				
Requirement	**Record Metadata Component**	**Structure**	**Data Collection Required**	**Reference/Comment**
C2.T3.2.	Supplemental Marking List	Mandatory (All)	Optional	Multiple Supplemental Markings entry selections shall be supported
	Record Descriptors			
C2.T3.3.	Subject or Title	Mandatory (All)	Mandatory	
C2.T3.4.	Media Type	Mandatory (All)	Mandatory	RMTF
C2.T3.5.	Format	Mandatory (All)	Mandatory	RMTF
	Record Dates			
C2.T3.6.	Date Filed	Mandatory (All)	Mandatory (System Date, not editable)	RMTF
C2.T3.7.	Publication Date	Mandatory (All)	Mandatory	
C2.T3.8.	Date Received	Mandatory	Optional	
Record People and Organizations				
C2.T3.9.	Author or Originator	Mandatory (All)	Mandatory	
C2.T3.10.	Addressee(s)	Mandatory (All)	Mandatory for correspondence	
C2.T3.11.	Other Addressee(s)	Mandatory (All)	Mandatory for correspondence	
C2.T3.12.	Originating Organization	Mandatory (All)	Mandatory	
	Additional Metadata			
C2.T3.13.	Location	Mandatory	Optional	RMTF
C2.T3.14.	Vital Record Indicator	Mandatory	Optional	
C2.T3.15.	Vital Record Review and Update Cycle Period	Mandatory, conditional on Vital Record Indicator	Mandatory, conditional on Vital Record Indicator	
C2.T3.16.	User-Defined Fields	Mandatory/ Undefined	Optional	Multiple User-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 components, and their associated selection lists.

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.

C2.2.3.6. RMAs shall provide the capability to create, view, save, and print the complete record metadata, or user-specified portions thereof, in user-selectable order.

C2.2.3.7. RMAs shall provide the capability for authorized individuals to arrange record metadata components and user-defined record components on data entry screens to be used for filing.

C2.2.3.8. RMAs shall prevent subsequent changes to electronic records stored in its supported repositories. The content of the record, once filed, shall be preserved.

C2.2.3.9. RMAs shall not permit modification of the metadata fields indicated by this Standard as not editable.

C2.2.3.10. RMAs shall (for all records) 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 collections are non-null before filing the record.

C2.2.3.11. 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 autofiling, RMAs shall provide the user the option of editing the record metadata prior to filing.

C2.2.3.12. 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 error. These prompts shall provide guidance to the user in making corrective actions; for example, "Date format incorrect - use MM/DD/YYYY."

C2.2.3.13. RMAs shall restrict the capability to only authorized individuals to define and add user-defined metadata fields (e.g., project number, budget line) for site-specific requirements.

C2.2.3.14. RMAs shall provide the capability to view, save, or print the metadata associated with a specified record or set of records, or user-specified portions thereof, in user-selectable order.

C2.2.3.15. 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.

C2.2.3.16. 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, etc., to a specified record. RMAs shall allow only authorized individuals to change or delete links and associations.

C2.2.3.18. RMAs shall provide the capability to link original superseded records to their successor records.

C2.2.3.19. RMAs shall provide the capability to support multiple renditions of a record. These shall be associated and linked.

C2.2.3.20. RMAs shall provide the capability to increment versions of records when filing. RMAs shall associate and link the versions.

C2.2.3.21. RMAs shall link the record metadata to the record so that it can be accessed for display, export, etc.

C2.2.3.22. 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.

C2.2.3.23. RMAs shall enforce data integrity, referential integrity, and relational integrity.

C2.2.3.24. RMAs shall provide the capability to automatically synchronize multiple databases and repositories.

C2.2.3.25. RMAs shall provide the capability for users to create and maintain shortened "quick-pick"lists from the authorized lists.

C2.2.3.26. RMAs shall provide the capability for users to create and maintain templates that automatically populate commonly used data into record metadata fields.

C2.2.4. Filing Electronic Mail Messages (E-mail)

C2.2.4.1. RMAs shall treat e-mail messages the same as any other record, and these shall be subject to all requirements of this Standard.

C2.2.4.2. RMAs shall 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. RMAs shall provide the capability for editing Subject or Title, Author or Originator, Addressee(s), and the Other Addressee(s) metadata fields prior to filing. All other fields shall not be editable.

TABLE C2.T4. Transmission and Receipt Data

Transmission and Receipt Data	Record Metadata Mapping
The intelligent name[1] of the sender	RMAs shall automatically enter this data into the Author or Originator data field (paragraph C2.T3.9.).
The intelligent name of all primary addressees (or distribution lists).	RMAs shall automatically enter this data into the Addressee(s) data field of the record metadata (paragraph C2.T3.10.).
The intelligent name of all other addressees (or distribution lists).	RMAs shall automatically enter this data into the Other Addressee(s) data field (paragraph C2.T3.11.).
The date and time the message was sent.	RMAs shall automatically enter this data into the Publication Date data field (paragraph C2.T3.7.).
For messages received, the date and time the message was received (if available).	RMAs shall automatically enter this data (if available) into the Date Received data field (paragraph C2.T3.8.).
The subject of the message.	RMAs shall automatically enter this data into the Subject or Title data field of the record metadata (paragraph C2.T3.3.).

C2.2.4.3. RMAs shall provide the user the option of filing e-mail and all its attachment(s) as a single record, or filing selected e-mail item(s) as individual record(s), or to do both. When the attachment(s) is (are) filed as individual record(s), the user shall be provided the capability to enter the metadata required in table C2.T3

C2.2.5. Storing Records.

C2.2.5.1. RMAs shall provide at least one portal that provides access to all associated repositories and databases storing electronic records and their metadata.

[1] Intelligent names are clear, uncoded, identifications of the individual.

C2.2.5.2. The RMAs shall prevent unauthorized access to the repository(ies).

C2.2.5.3. RMAs shall manage and preserve any record in any supported repository, regardless of its format or structure, so that, when retrieved, it can be reproduced, viewed, and manipulated in the same manner as the original.

C2.2.5.4. RMAs shall allow only authorized individuals to move or delete records from the repository.

C2.2.6. Retention and Vital Records Management

C2.2.6.1. Screening Records

C2.2.6.1.1. RMAs shall provide for sorting, viewing, saving, and printing list(s) of record folders and/or records (regardless of media) based on any combination of the following:

C2.2.6.1.1.1. Disposition Action Date.

C2.2.6.1.1.2. Disposition Action.

C2.2.6.1.1.3. Location.

C2.2.6.1.1.4. Transfer or Accession Location.

C2.2.6.1.1.5. Vital Records Review and Update Cycle Period or Date.

C2.2.6.1.1.6. Record Category Identifier.

C2.2.6.1.1.7. Folder Unique Identifier.

C2.2.6.1.1.8. User Definable Fields.

C2.2.6.1.2. RMAs shall provide for sorting, viewing, saving, and printing life-cycle information, eligibility dates, and events of user-selected record folders and records.

C2.2.6.1.3. RMAs shall allow the user to select and order the columns presented in the screening result list(s).

C2.2.6.1.4. RMAs shall provide authorized individuals with the capability to indicate when the specified event has occurred for records and record folders with event- and time-event-driven dispositions.

C2.2.6.1.5. RMAs shall provide for sorting, viewing, saving, and printing lists and partial lists of record folders and/or records that have no assigned disposition.

C2.2.6.2. Closing Record Folders

C2.2.6.2.1. RMAs shall provide a capability for authorized individuals to close record folders to further filing after the specified event occurs.

C2.2.6.2.2. RMAs shall provide the capability only to authorized individuals to add records to a previously closed record folder or to reopen a previously closed record folder for additional public filing.

C2.2.6.3. Cutting Off Record Folders

C2.2.6.3.1. RMAs shall be capable of implementing 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. The cutting off of a folder shall start the first phase of its life cycle controlled by the records schedule. See reference (z).

C2.2.6.3.2. RMAs shall provide the capability to only authorized individuals to add records or make other alterations to record folders that have been cut off.

C2.2.6.4. Freezing/Unfreezing Records

C2.2.6.4.1. RMAs shall provide the capability for only authorized individuals to extend or suspend (freeze) the retention period of record folders or records beyond their scheduled disposition.

C2.2.6.4.2. RMAs shall provide a field for authorized individuals to enter the reason for freezing a record or record folder.

C2.2.6.4.3. RMAs shall identify record folders and/or records that have been frozen and provide authorized individuals with the capability to unfreeze them.

C2.2.6.4.4. RMAs shall allow authorized individuals to search, update, and view the reason for freezing a record or record folder.

C2.2.6.5. Transferring Records

C2.2.6.5.1. RMAs shall identify and present those record folders and records eligible for interim transfer and/or accession.

C2.2.6.5.2. RMAs shall, for records approved for interim transfer or accession and that are stored in the RMA's supported repository(ies), copy the pertinent records and associated metadata of the records and their folders to a user-specified filename, path, or device. For permanent records to be accessioned to the National Archives, the accessioning file(s) shall be made to conform to one of the formats and media specified in the Archives Code.

C2.2.6.5.3. RMAs shall, 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 user-specified filename, path, or device. For permanent records to be accessioned to the National Archives, the metadata shall be made to conform to one of the formats and media specified.

C2.2.6.5.4. RMAs shall, for records approved for interim transfer or accession, provide the capability for only authorized individuals to delete the records and/or related metadata after successful transfer has been confirmed. RMAs shall provide the capability to allow the organization to retain the metadata for records that were transferred or accessioned.

C2.2.6.5.5. RMAs shall provide documentation of transfer activities. This documentation shall be stored as records.

C2.2.6.6. Destroying Records

C2.2.6.6.1. RMAs shall identify and present the record folders and records, including record metadata, that are eligible for destruction, as a result of reaching that phase in their life cycle. Records assigned more than one 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.

C2.2.6.6.2. RMAs shall, for records approved for destruction, present a second confirmation requiring authorized individuals to confirm the delete command, before the destruction operation is executed.

C2.2.6.6.3. RMAs shall delete electronic records approved for destruction in a manner such that the records cannot be physically reconstructed.

C2.2.6.6.4. RMAs shall provide an option allowing the organization to select whether to retain or delete the metadata of destroyed records.

C2.2.6.6.5. RMAs shall restrict the records destruction commands to authorized individuals.

C2.2.6.6.6. RMAs shall provide documentation of destruction activities. This documentation shall be stored as records.

C2.2.6.7. Cycling Vital Records

C2.2.6.7.1. RMAs shall provide the capability for authorized individuals to enter the Vital Records Review and Update Cycle Period when creating or updating the file plan.

C2.2.6.7.2. RMAs shall provide the capability to enter the date when the records associated with a vital records folder have been reviewed and updated.

C2.2.6.7.3. RMAs shall provide a means for identifying and aggregating vital records due for cycling.

C2.2.6.7.4. RMAs shall provide a means for identifying and aggregating vital records by previous cycle dates.

C2.2.6.8. Searching for and Retrieving Records

C2.2.6.8.1. RMAs shall allow users to browse the records stored in the file plan based on their user access permissions.

C2.2.6.8.2. RMAs shall allow searches using any combination of the record and/or folder metadata elements.

C2.2.6.8.3. RMAs shall allow the user to specify partial matches and shall allow designation of "wild card" fields or characters.

C2.2.6.8.4. RMAs shall allow searches using Boolean and relational operators: "and", "and not", "or", "greater than" (>), "less than" (<), "equal to" (=), and "not equal to" (< >), and provide a mechanism to override the default (standard) order of precedence.

C2.2.6.8.5. RMAs shall 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 order the columns presented in the search results list for viewing, transmitting, printing, etc.

C2.2.6.8.6. RMAs shall allow users the ability to search for null or undefined values.

C2.2.6.8.7. RMAs shall 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 format in which they were provided to the RMA for filing.

C2.2.6.8.8. RMAs shall 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.

C2.2.6.8.9. When the user selects a record for retrieval, RMAs shall present a list of available versions, defaulting to the latest version of the record for retrieval, but allow the user to select and retrieve any version.

C2.2.6.8.10. RMAs shall allow users to select any number of records, and their metadata, for retrieval from the search results list.

C2.2.6.8.11. RMAs shall allow the user to abort a search.

C2.2.7. Access Controls.

Table C2.T5. 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.T5. Authorized Individual Requirements

Requirement	Application Administrator	Records Manager	Privileged User
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
C2.2.1.2. Designate the metadata fields that are to be constrained to selection lists. Create and maintain selection lists (e.g., drop-down lists) for metadata items that are constrained to a pre-defined set of data.	Ensure database is correctly set up and installed	Define Lists	User abilities
C2.2.1.3. Create, edit, and delete record folder components and their identifiers.	Ensures that data structures are correctly installed and database links are in place	Enters folder data	Enters folder data
C2.2.1.5. Define and attach user-defined business rules and/or access logic to metadata fields including user-defined fields.	Creates rules and connects them to fields	Manually execute rules if necessary	None
C2.2.2.1. View, create, edit, and delete disposition schedule components of record categories.	Ensures that data structures are correctly installed and database links are in place	Enters disposition data, enters event data, closes folders	Enters event data and closes folders
C2.2.2.3. 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
C2.2.2.6. Change the disposition instructions.	None	Edits disposition information and manually executes rules necessary to reschedule	None
C2.2.3.3. Create, edit, and delete record metadata components, and their associated selection lists.	Ensures that data structure is correctly installed and database links are in place	Creates Selection Lists	Enters data (all users)
C2.2.3.4. Select where data collection for optional metadata fields is mandatory for a given organization.	During setup	Advising	None
C2.2.3.7. Arrange record metadata components and user-defined record components on data entry screens to be used for filing.	During setup	Advising	None
C2.2.3.13. Define and add user-defined	During setup	Advising	None

Table C2.T5. Authorized Individual Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
metadata fields (e.g., project number, budget line) for site-specific requirements.			
C2.2.3.15. Limit the record folders and record categories presented to a user or workgroup.	Record Categories during setup	Record Folders	Record Folders
C2.2.3.16. Change a record folder or record category associated with a record.	As necessary	As necessary	None
C2.2.3.17. Change or delete links and associations.	Database is correctly installed and configured	Change links as necessary	Make links
C2.2.3.22. Modify the metadata of stored records.	As necessary	Change data as necessary	Time-Event and Event folders
C2.2.5.3. Move or delete records from the repository.	As necessary	As necessary	None
C2.2.6.1.4. 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
C2.2.6.2.1. Close record folders to further filing after the specified event occurs.	As necessary	As necessary	As necessary
C2.2.6.2.2. 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
C2.2.6.3.1. Approve cutoff.	As necessary	Routine work	None

Table C2.T5. Authorized Individual Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privileged User**

C2.2.6.3.2. Add records or make other alterations to record folders that have been cut off.	Database support	Enters limits	None
C2.2.6.4.1. Extend or suspend (freeze) the retention period of record folders or records beyond their scheduled disposition.	Database and business rules	Freezing/ Unfreezing	None
C2.2.6.4.2. Enter the reason for freezing a record or record folder.	Database and business rules	Freezing/ Unfreezing	None
C2.2.6.4.3. Unfreeze capability.	Database and business rules	Freezing/ Unfreezing	None
C2.2.6.4.4. Search, update, and view the reason for freezing a record or record folder.	Database and business rules	Freezing/ Unfreezing	None
C2.2.6.5.4. Delete the records and/or related metadata after successful transfer has been confirmed.	As necessary	As necessary	None
C2.2.6.6.2. Confirm the delete command, before	As necessary	As necessary	None

Table C2.T5. Authorized Individual Requirements			
Requirement	**Application Administrator**	**Records Manager**	**Privileged User**
the destruction operation is executed.			
C2.2.6.6.5. Access to records destruction commands.	As necessary	As necessary	None
C2.2.6.7.1. Enter the Vital Records Review and Update Cycle Period when creating or updating the file plan.	Ensuring database structure is adequate and correctly installed	Enters cycling data	Cycles and Updates Records
C2.2.7.1. Allow access to the RMA.	As necessary	As necessary	None
C2.2.7.1.2. Define the minimum length of the Password field.	Define minimum length	None	None
C2.2.8.2. Determine which of the objects and specified actions listed in subparagraph C2.2.8.1. are audited.	Manage audits	None	None
C2.2.8.3. Set up specialized reports to:	Create reports	None	None
C2.2.8.5. 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
C3.2.1. (Optional) Make global changes to the record category names, record category identifiers, disposition components, and originating organization.	As necessary	As necessary	None
C3.2.2. (Optional) Bulk load capability.	As necessary	As necessary	None

C2.2.7.1. The RMA, in conjunction with its operating environment, shall use identification and authentication measures that allow only authorized persons access to the RMA. At a minimum, the RMA will implement identification and authentication measures and these will be made known prior to implementation.

C2.2.7.1.1. Userid.

C2.2.7.1.2. Password. (RMAs shall provide the capability for authorized users to define the minimum length of the Password field.)

C2.2.7.1.3. Alternative methods, such as Biometrics, Common Access Cards (CAC), or Public Key Infrastructure (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.

C2.2.7.2. 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.

C2.2.7.3. 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.

C2.2.7.4. If the RMA provides a web user interface, it shall provide 128-bit encryption and be PKI-enabled, as well as provide all the mandatory access controls.

C2.2.7.5. RMAs shall support simultaneous multiple-user access to all components of the RMA, the metadata, and the records.

C2.2.8. System Audits

C2.2.8.1. The RMA, in conjunction with its operating environment, 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:

C2.2.8.1.1. User Accounts.

C2.2.8.1.2. User Groups.

C2.2.8.1.3. Records.

C2.2.8.1.4. Associated metadata elements.

C2.2.8.1.5. File plan components.

These actions include retrieving, creating, deleting, searching, and editing actions. See references (c) and (ar). Logging of searching and retrieving actions are not required for User Accounts and User Groups.

C2.2.8.2. The RMA shall provide a capability whereby only authorized individuals can determine which of the objects and specified actions listed in subparagraph C2.2.8.1. are audited.

C2.2.8.3. The RMA, in conjunction with its operating environment, shall provide audit analysis functionality whereby an authorized individual can set up specialized reports to:

C2.2.8.3.1. Determine what level of access a user has and to track a user's actions. These are the specified actions listed in subparagraph C2.2.8.1.

C2.2.8.3.2. Facilitate reconstruction, review, and examination of the events surrounding or leading to mishandling of records, possible compromise of sensitive information, or denial of service.

C2.2.8.4. RMAs shall provide the capability to file the audit data as a record.

C2.2.8.5. The RMA, in conjunction with its operating environment, shall allow only authorized individuals to export and/or backup and remove audit files from the system.

C2.2.8.6. The RMA, in conjunction with its operating environment, shall not allow audit logs to be edited.

C2.2.9. 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.

C2.2.9.1. Backup of Stored Records. The RMA system shall provide the capability to automatically create backup or redundant copies of the records and their metadata.

C2.2.9.2. 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.

C2.2.9.3. Recovery/Rollback Capability. Following any system failure, the backup and recovery procedures provided by the system shall:

C2.2.9.3.1. Ensure data integrity by providing the capability to compile updates (records, metadata, and any other information required to access the records) to RMAs.

C2.2.9.3.2. Ensure these updates are reflected in RMA files, and ensuring 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.

C2.2.9.4. Rebuild Capability. The system shall provide the capability to rebuild from any backup copy, using the backup copy and all subsequent system audit trails.

C2.2.9.5. 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.

C2.2.9.6. Safeguarding. The RMA, in conjunction with its operating environment, shall have the capability to activate a keyboard lockout feature and a screen-blanking feature.

C2.2.10. Additional Baseline Requirements.

Following are records management requirements that shall be implemented by the organization, but not necessarily by the RMAs:

C2.2.10.1. Electronic Calendars and Task Lists. Some electronic systems provide calendars and task lists for users. These may meet NA's definition of a record. 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 those records to be managed by the RMA.

C2.2.10.2. 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 these records to be managed by the RMA.

C2.2.10.3. Ability to Read and Process Records. Since RMAs are prohibited (see subparagraph C2.2.3.8.) from altering the format of stored records, 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:

C2.2.10.3.1. Maintaining the hardware and software used to create or capture the record.

C2.2.10.3.2. Maintaining hardware and software capable of viewing the record in its native format.

C2.2.10.3.3. Ensuring backward compatibility when hardware and software is updated, or:

C2.2.10.3.4. 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.

C2.2.10.4. 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.

C2.2.10.5. Accessioning Records to NARA. When accessioning records and metadata to NA, if conforming to formats and media specified and causes a violation of the records' authenticity and/or integrity, the organization shall contact NA for guidance.

C2.2.10.6. Applying Records Disposition Schedule to Backup Copies. The using organization shall schedule the backup copies and recycle or destroy the medium in accordance with the disposition schedule.

C3. CHAPTER 3
NON-MANDATORY FEATURES

C3.1. 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 NA/DPSITM compliance.

C3.1.1. Storage Availability. The acquiring or using activity should define the size of the storage space required for its organizational records, along with the related record metadata and associated audit files.

C3.1.2. Documentation. The acquiring or using activity should determine the type and format of desired documentation, such as user guides, technical manuals, and installation procedures, to be provided by the vendor.

C3.1.3. System Performance. The acquiring or using activity should specify what constitutes acceptable RMA system availability, reliability, response times, and downtimes that will satisfy its business requirements.

C3.1.4. Hardware Environment. The acquiring or using activity should define the hardware environment (for example, mainframe, client-server, or personal computer) and identify the platforms (servers and workstations) on which the RMA is to run.

C3.1.5. Operating System Environment. The acquiring or using activity should define the operating system environment (for example, UNIX, Windows, Linux, Macintosh) on which the RMA is to be run.

C3.1.6. Network Environment. The acquiring or using activity should define 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 NT Server) on which the RMA is to be run.

C3.1.7. Protocols. The acquiring or using activity should identify the protocols, such as Transmission Control Protocol/Internet Protocol (TCP/IP), Simple Mail Transfer Protocol (SMTP), or X.400 that the RMA is to support.

C3.1.8. Electronic Mail Interface. The acquiring or using activity should specify the e-mail application(s) with which the RMA is to interface.

C3.1.9. End-User Orientation and Training. The acquiring or using activity should specify records manager and end-user training requirements.

C3.2. 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).

C3.2.1. 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.

C3.2.2. Bulk Loading Capability. RMAs should provide the capability for authorized individuals to bulk load:

C3.2.2.1. An Office/Ministry /Agency's pre-existing file plan.

C3.2.2.2. Electronic records.

C3.2.2.3. Record metadata.

C3.2.3. Interfaces to Other Software Applications. RMAs should interface with various office automation packages such as electronic mail, word processors, spreadsheets, databases, desktop publishers, and electronic data interchange systems, as specified by the using activity.

C3.2.4. 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.

C3.2.5. 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 hot key.

C3.2.6. 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.

C3.2.7. 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.

C3.2.8. Bar Code Systems. An organization may determine a need to use a bar code system with RMAs. The following examples show how bar code technology can be used to support records management tasks:

C3.2.8.1. File and correspondence tracking to positions, sections, or staff members.

C3.2.8.2. Creating, printing, and reading labels for non-electronic records.

C3.2.8.3. Boxing records for transfer.

C3.2.8.4. Box tracking for records-holding facility operations.

C3.2.8.5. Workflow tracking.

C3.2.8.6. Posting changes in disposition.

C3.2.8.7. Recording audit and census functions.

C3.2.9. 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.

C3.2.10. 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.

C3.2.11. 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.

C3.2.12. 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:

C3.2.12.1. Standard Forms for "Request for Records Disposition Authority."

C3.2.12.2. Standard Forms for "Records Transmittal and Receipt."

C3.2.12.3. Standard Form for "Request to Transfer, Approval, and Receipt of Records to the National Archives of Namibia."

C3.2.12.4. National Archives Form on "Database Record Layout."

C3.2.12.5. National Archives Form for "Technical Description for Transfer of Electronic Records to the National Archives."

C3.2.13. Printed Labels. RMAs should provide the capability to produce hard-copy codes or identifiers in the form of labels or other products, as required.

C3.2.14. Viewer. RMAs should provide the capability to view each file in its stored format or a human-readable rendition.

C3.2.15. Web Capability. RMAs should provide the capability to allow the user to interface through a web browser or other platform independent means.

C3.2.16. Government Information Locator Service. RMAs should have the capability to implement the requirements of the Government to secure public access to records. Public access systems will be established to identify public information resources throughout the Government, describe the information available in those resources, and provide assistance in obtaining this information.

C3.2.17. Enhanced Support for Off-line Records. RMAs should provide additional features for managing boxes of hard-copy records and other off-line archives.

C4. CHAPTER 4

MANAGEMENT OF CLASSIFIED RECORDS

C4.1. REQUIREMENTS FOR RMAs SUPPORTING MANAGEMENT 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 **Chapters 2** and **3**. 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.

C4.1.1. 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 C4.T1.** Mandatory in the Structure column 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. Mandatory in the Data Collection Required by User column indicates that RMAs shall ensure population of the associated data structure with non-null values. For fields that are not mandatory in the Data Collection column, RMAs shall behave in a predictable manner as a result of queries or other operations when the fields are not populated.

Table C4.T1. Classified Record Components

Requirement	Component	Structure	Data Collection Required by User	Reference (to be created)
C4.T1.1.	Initial Classification	Mandatory	Mandatory, Option List is user expandable and must include: Confidential Secret Top Secret No Markings	
C4.T1.2.	Current Classification	Mandatory	Mandatory, Option List is user expandable and must include: Confidential Secret Top Secret No Markings	
C4.T1.3.	Reason(s) For Classification	Mandatory	Mandatory	
C4.T1.4.	Classified By	Mandatory	Mandatory if no data in Derived From, otherwise default	
C4.T1.5.	Derived From	Mandatory	Mandatory if no data in Classified By, otherwise default	

Table C4.T1. Classified Record Components, continued				
Requirement	**Component**	**Structure**	**Data Collection Required by User**	**Reference**
C4.T1.6.	Declassify On	Mandatory for all but restricted data or formerly restricted data	Mandatory, one of: Exemption Category Date Event Date and Event	
C4.T1.7.	Classifying Agency Downgrading, Reviewing, and Regrading Information	Mandatory	Mandatory	
C4.T1.8.	Downgrade On	Mandatory	Optional, One of: Date Event Date and Event	
C4.T1.9.	Downgrade Instructions	Mandatory	Mandatory if the Downgrade On field is populated	
C4.T1.10.	Reviewed On	Mandatory	Optional	
C4.T1.11.	Reviewed By	Mandatory	Mandatory if the Reviewed On field is populated	
C4.T1.12.	Downgraded On	Mandatory	Optional	
C4.T1.13.	Downgraded By	Mandatory	Mandatory if the Downgraded On field is populated	
C4.T1.14.	Declassified On	Mandatory	Optional	
C4.T1.15.	Declassified By	Mandatory	Mandatory if the Declassified On field is populated	
C4.T1.16.	Upgraded On	Mandatory	Optional	
C4.T1.17.	Reason(s) for Upgrade	Mandatory	Mandatory if the Upgraded On field is populated	
C4.T1.18.	Upgraded By	Mandatory	Mandatory if the Upgraded On field is populated	

C4.1.2. Initial and Current Classification. RMAs shall populate the Current Classification field with the Initial Classification data when the Initial Classification is first entered.

C4.1.3. Current Classification. RMAs shall provide a capability by which a user can edit the Current Classification field prior to filing.

C4.1.4. 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.

C4.1.5. Derivatively Classified Records. When the "Derived From" field is populated, RMAs shall provide the option of capturing multiple "Reason(s) for Classification" and "Classified By" fields.

C4.1.6. Derivative Sources. When the classified information is derived from multiple sources, RMAs shall provide the capability to enter multiple sources.

C4.1.7. Declassify On Event. When "Event" is selected in the "Declassify On" field, the RMA shall prompt the user to enter text that describes the declassification event.

C4.1.8. 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. This mandatory period is currently 10 years.

C4.1.9. 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 "Declassify On" field, both to make the retention period more restrictive or to accommodate changes to the mandatory retention period.

C4.1.10. Classification Guides. RMAs shall provide a capability that allows an authorized individual to establish an automatically triggered classification mechanism. See reference (au). When a designated classification guide indicator is entered in the "Derived From" field, the following fields shall be automatically populated:

C4.1.10.1. Reason(s) for Classification.

C4.1.10.2. Initial Classification.

C4.1.10.3. Declassify On.

C4.1.11. Confirming Accuracy Prior to Filing. RMAs shall provide the capability to confirm the accuracy of all user editable metadata items prior to filing.

C4.1.12. Editing Records. RMAs shall allow only authorized individuals to edit metadata items after a record has been filed.

C4.1.13. Restricted Data and Formerly Restricted Data. The following metadata items are not applicable for records containing Restricted Data or Formerly Restricted Data [Supplemental Marking(s)] and shall be disabled.

C4.1.13.1. Downgrade On.

C4.1.13.2. Declassify On.

C4.1.14. Current Classification. When the entry in the "Current Classification" field is changed, RMAs shall ensure that "Upgraded On", "Downgraded On", or "Declassified On" field, whichever is appropriate, is populated with an appropriate date field.

C4.1.15. Exemption Categories. RMAs shall provide the capability for an authorized individual to enter or update exemption category(ies) in the "Declassify On" field.

C4.1.16. Record History Audit. The RMA shall capture and link an audit history of each record by capturing the replaced metadata value and 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.

C4.1.17. Using the Record History Audit. The RMA shall provide the capability to view, copy, save, and print the record history file based on user permissions; shall not allow the editing of the record history file; and shall provide the capability for only authorized individuals to delete the record history file.

C4.1.18. Marking Printouts and Displays. Current classification, reasons for classification, and downgrading instructions shall be required metadata items for displays, printouts, reports, queries, review lists, etc. The highest classification level shall be displayed when aggregate results are displayed.

C4.1.19. Access Criteria Conflict. The RMA, 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.

C4.1.20. Authorized Access Restriction. The RMA shall provide a capability whereby authorized individuals restrict access to records and their metadata based on access criteria. In addition to baseline access restriction capabilities, these additional criteria include.

C4.1.20.1. Current Classification (see paragraph C4.T1.2.).

C4.1.20.2. Supplemental Marking List (see subparagraph C2.T2.1.6.).

C4.1.20.3. Metadata Elements identified by the organization to be used for access control.

C4.1.21. Access Control. Table C4.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 C4.T2. Authorized Individual Requirements

Requirement	Application Administrator	Records Manager	Privileged User
C4.1.9. Establish and maintain the period of time used to verify the "Declassify On" field, both to make the retention period more restrictive or to accommodate changes to the mandatory retention period.	Database installed and properly set up	None	Enter and maintain data (Security person)
C4.1.10. Establish an automatically triggered classification mechanism.	Database installed and properly set up	None	Enter and maintain data (Security person)
C4.1.12. Edit metadata items after a record has been filed.	As necessary	As necessary	As necessary (downgrading and reclassification, etc.)
C4.1.15. Enter or update exemption category(ies) in the "Declassify On" field.	Database installed and properly set up	None	Enter and maintain data (Security person)
C4.1.16. Select which metadata field to capture.	As necessary	As necessary	None
C4.1.17. Delete the record history file.	As necessary	As necessary	As necessary

Requirement	Application Administrator	Records Manager	Privileged User
C4.1.20. Restrict access to records based on access criteria.	User accounts, Access Control Lists and Database properly set up	None	None
C4.2.1. (Optional) Determine which metadata fields require classification for a given organization.	Database and business rules properly defined, installed and set up	None	None

C4.2. OPTIONAL SECURITY FEATURES

C4.2.1. RMAs should provide the capability to allow authorized individual-selected metadata fields to be provided their own classification.

C4.2.2. Where appropriate, RMAs should have the capability to inform the user that a redacted version is available in an open RMA.