DOD 5015.2-STD

DESIGN CRITERIA STANDARD
FOR
ELECTRONIC RECORDS MANAGEMENT SOFTWARE APPLICATIONS

NOVEMBER 1997

ASSISTANT SECRETARY OF DEFENSE
FOR
COMMAND. CONTROL, COMMUNICATIONS, AND INTELLIGENCE

C2. CHAPTER 2

MANDATORY REQUIREMENTS

C2.1 GENERAL REQUIREMENTS

C2.1.1. Managing Records. RMAs shall manage records regardless of storage media or other characteristics. (44 U.S.C. 3103, 41 CFR 201-9, and 36 CFR 1222.10, references (b), (c), and (d))

C2.1.2. Accommodating Year 2000 and Twenty-First Century Dates. RMAs shall correctly accommodate and process information containing the year 2000 and beyond as well as dates in the current and previous centuries. (FIPS 4-1, "Representation for Calendar Date and Ordinal Date for Information Interchange," reference (e)) The capability shall include, but not be limited to, date data century recognition, calculations, and logic that accommodate same century and multi-century formulas and date values, and date data interface values that reflect the century. In addition, leap year calculations shall be accommodated (i.e. 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 in accordance with DoD 8320.1-M, "DoD Data Administration Procedures," (reference (f)). When selecting commercial-off-the-shelf (COTS) products to support RMA requirements, selection criteria should include the feasibility and capability of the COTS to implement and maintain DoD data standards.

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, add, edit, and delete record categories, files and their codes. Each file or category code shall be linked to its associated file or category and to its higher-level category code(s). (44 U.S.C. 3303, 36 CFR 1222.50, and 36 CFR 1228.24, references (g), (h), and (i))

C2.2.1.2. RMAs shall provide the capability for only authorized individuals to create, add, edit, and delete disposition instructions and their associated codes. Each disposition code shall be linked to its associated disposition instruction. (44 U.S.C. 3303, 41 CFR 201-9, 36 CFR 1222.50, and 36 CFR 1228.24, references (g), (c), (h), and (i))

C2.2.1.3. RMAs shall provide authorized individuals with the capability to assign the following data when generating the file plan:

C2.2.1.3.1.	Record Category Name.	(RMTF, reference (j))
C2.2.1.3.2.	Record Category Code.	(RMTF, reference (j))
C2.2.1.3.3.	Record Category Description.	(RMTF, reference (j))
C2.2.1.3.4.	Disposition Authority.	(RMTF, reference (j))
C2.2.1.3.5.	Vital Record Indicator.	(36 CFR 1236.20, reference (k))
C2.2.1.3.6.	Disposition Instruction Name.	(RMTF, reference (j))
C2.2.1.3.7.	Disposition Instruction Code.	(RMTF, reference (j))
C2.2.1.3.8.	Disposition Instruction Type.	(see subparagraph C2.2.5.2., below)
C2.2.1.3.9.	User definable fields.	

C2.2.1.4. RMAs shall provide the capability for only authorized individuals to assign a disposition instruction code to a file or record category. (RMTF, reference (j))

C2.2.1.5. RMAs shall allow for the reschedule of records already in the system when disposition instructions change from the original designations.

C2.2.1.6. RMAs shall provide the capability for only authorized individuals to extend or suspend (freeze) the retention period of individual files or record categories, which are required beyond their scheduled disposition because of special circumstances (such as a court order or an investigation) that altered the normal administrative, legal, or fiscal value of the records or categories. (44 U.S.C. 2909 and 36 CFR 1228.54, references (l) and (m))

C2.2.1.7. RMAs shall provide the capability to output for viewing, saving, and printing record categories and files and their associated codes. (RMTF, reference (j))

C2.2.1.8. RMAs shall provide the capability to output for viewing, saving, and printing the disposition instructions and disposition instruction codes. (RMTF, reference (j))

C2.2.1.9. RMAs shall provide the capability to output for viewing, saving, and printing the record categories and files and their associated disposition. (RMTF, reference (j))

C2.2.2. Identifying and Filing Records

C2.2.2.1. RMAs shall provide users with the capability to select and assign a file code to a record. (36 CFR 1222.50, reference (h))

C2.2.2.2. RMAs shall assign a unique computer-generated record identifier to each record they manage regardless of where the record is stored. (RMTF, reference (j))

C2.2.2.3. RMAs shall prevent subsequent changes to documents that have been designated as records. The content of the record, once filed, shall be preserved. Changed or revised records shall be designated as new records with different identification data. (36 CFR 1222.50 and RMTF, references (h) and (j))

C2.2.2.4. RMAs shall not permit modification of the record identifier once assigned.

C2.2.2.5. RMAs shall (for all records) capture or provide the user with the capability to assign, as appropriate, the following minimum profile data (metadata) when the record is filed: (36 CFR 1234.22 and 36 CFR 1222.50, references (n) and (h))

C2.2.2.5.1. Subject.	(36 CFR 1234.22, reference (n))
C2.2.2.5.2. Date Filed.	(RMTF, reference (j))
C2.2.2.5.3. Addressee(s).	(36 CFR 1234.22, reference (n))
C2.2.2.5.4. Media Type.	(RMTF, reference (j))
C2.2.2.5.5. Format.	(RMTF, reference (j))
C2.2.2.5.6. Location of Record.	(RMTF, reference (j))
C2.2.2.5.7. Document Creation Date.	(36 CFR 1234.22, reference (n))
C2.2.2.5.8. Author or Originator.	(36 CFR 1234.22, reference (n))
C2.2.2.5.9. Originating Organization.	(36 CFR 1234.22, reference (n))
C2.2.2.5.10. Vital Record Indicator	(36 CFR 1236.20, reference (k))

C2.2.2.6. RMAs shall provide the user with the capability to edit the metadata listed above in subparagraph C2.2.2.5. prior to filing the record except for data captured electronically from e-mail or other automated systems.

C2.2.2.7. RMAs shall provide the capability for authorized individuals (only) to add user defined profile data fields, for site-specific information such as project number, security classification, Privacy Act, etc. (36 CFR 1234.22, reference (n))

C2.2.2.8. RMAs shall provide the capability to output for viewing, saving, or printing the record profile information (metadata) identified in paragraph C2.2.2.5. above.

C2.2.2.9. RMAs shall provide the capability for only authorized individuals to limit the file codes available to a user or work group. The RMA shall ensure that only current and valid file codes are presented to the user for selection during filing.

C2.2.2.10. RMAs shall allow a record to be assigned to more than one file category when appropriate. (NARA — RM Requirements for Electronic Recordkeeping System, reference (o))

C2.2.2.11. RMAs shall provide the capability for only authorized individuals to change a file code assigned to a filed record.

C2.2.2.12. RMAs shall provide the capability to designate a record as a vital record. (36 CFR 1236.20, reference (k))

C2.2.2.13. RMAs shall provide the capability to update and cycle vital records. (36 CFR 1236.14, reference (p))

C2.2.2.14. RMAs shall provide only authorized individuals the capability to reverse the designation of a vital record once the designation has become obsolete.

C2.2.2.15. RMAs shall link supporting and related records and related information such as notes, marginalia, attachments, and electronic mail return receipts, as well as all profile data, to the record. (RMTF, reference (j))

C2.2.2.16. RMAs shall provide the capability to link original superseded records to their successor records. If the disposition of the superseded record is to destroy when replaced, the RMA shall identify that the record is eligible for destruction.

C2.2.2.17. RMAs shall manage and preserve any record regardless of its format or structure, so that it can be reproduced and viewed in the same manner as the original.

C2.2.2.18. RMAs shall automatically date a document when it is saved as a record, and preserve the date of receipt on records received. This date shall remain constant, without being changed when accessed, read, copied, or transferred. RMAs shall not permit this data to be edited.

C2.2.2.19. RMAs shall link the record metadata to the record so that it can be displayed when needed and transported with the record when a copy is made and transmitted to another location. (36 CFR 1234.32, reference (q))

C2.2.2.20. RMAs shall provide the capability for only authorized individuals to modify the metadata (values of the record profile attributes) of stored records that have not been specified as uneditable.

C2.2.3. Filing Electronic Mail Messages (E-Mail)

C2.2.3.1. RMAs shall treat electronic mail messages (including attachments) that have been filed as records, as any other record, and they shall be subject to all requirements of this document. (36 CFR 1222.32 and 36 CFR 1234.24, references (r) and (s))

C2.2.3.2. RMAs shall capture and automatically store the transmission and receipt data identified in Table C2.T1. below (if available from the e-mail system) as part of the record profile when an e-mail message is filed as a record. (36 CFR 1234.24, reference (s)) RMAs shall not allow editing of these metadata.

C2.2.3.3. RMAs shall store the attachments to an e-mail record and to associate and link the attachment with the e-mail record. (36 CFR 1234.24, reference (s))

C2.2.3.4. RMAs shall provide the capability to store distribution lists as required to ensure identification of the sender and recipients of messages that are records. (36 CFR 1234.24, reference (s))

TABLE C2.T1. Transmission/Receipt Data

Transmission/Receipt Data	Record Profile Mapping
The e-mail name and address of the sender.	RMAs shall automatically enter this data into the Author or Originator data field. (C2.2.7.1.8., below)
The e-mail name and address of all addressees (or distribution lists).	RMAs shall automatically enter this data into the Addressee data field of the record profile. (C2.2.7.1.3., below)
The e-mail name and address of all other recipients (or distribution lists).	RMAs shall automatically enter this data into the Other Recipients data field. (C2.2.7.1.10., below)
The date and time that the message was sent.	RMAs shall automatically enter this data into the Document Creation Date data field. (C2.2.7.1.7., below)
The subject of the message.	RMAs shall automatically enter this data into the Subject data field of the record profile. (C2.2.7.1.1., below)
For messages received, the date and time that the message was received.	RMAs shall automatically enter this data into the Document Creation Date data field. (C2.2.7.1.7., below)

C2.2.4. Storing Records

C2.2.4.1. RMAs shall provide or interface to a repository for storing electronic records and prevent unauthorized access to the repository. (44 U.S.C. 3105 and 36 CFR 1222.50, references (t) and (h)) If the repository is contained in an electronic database management system (DBMS), the query interface between the RMA and the DBMS shall comply with FIPS 127-2, "Database Language SQL," reference (u).

C2.2.4.2. RMAs shall not alter nor allow alteration of records they store. They shall preserve the format and content of the record as it was filed. (36 CFR 1222.50, 36 CFR 1234.22, and RMTF, references (h), (n), and (j))

C2.2.4.3. RMAs shall automatically date a document when it is saved as a record and preserve the date of receipt on records received. This date shall remain constant, without being changed when accessed, read, copied, or transferred. RMAs shall not permit this data to be edited.

C2.2.4.4. RMAs shall allow only authorized individuals to move/delete records from the repository. (36 CFR 1234.28 and 36 CFR 1222.50, references (v) and (h))

C2.2.5. Scheduling Records

C2.2.5.1. RMAs shall provide the capability to automatically track the disposition schedules of records, including those with retention periods of less than one year, as well as those with retention periods of one year or more. (RM Handbook, reference (w))

C2.2.5.2. RMAs shall, as a minimum, be capable of scheduling each of the following three types of disposition instructions: (RM Handbook, reference (w))

C2.2.5.2.1. Time Dispositions, where records are eligible for disposition immediately after completion of a fixed period of time.

C2.2.5.2.2. Event Dispositions, where records are eligible for disposition immediately after a specified event takes place.

C2.2.5.2.3. Time-Event Dispositions, where the retention periods of records are triggered after a specified event takes place.

C2.2.5.3. RMAs shall be capable of implementing cutoff instructions for scheduled and unscheduled records. (RM Handbook, reference (w))

C2.2.6. Screening Records

C2.2.6.1. RMAs shall provide for viewing, saving, and printing list(s) of records (regardless of media) within record categories based on disposition instruction code; record category or file code; and/or disposition event to identify records due for disposition processing. (RMTF, reference (j)) The information contained in the list(s) shall be user definable record profile attributes.

C2.2.6.2. RMAs shall provide the capability to identify records with event driven dispositions and provide authorized individuals with the capability to indicate when the specified event has occurred.

C2.2.6.3. RMAs shall provide the capability to identify records with time-event dispositions and provide authorized individuals with the capability to indicate when the specified event has occurred and when to activate applicable cutoff and retention instructions.

C2.2.6.4. RMAs shall identify files scheduled for cutoff, and present them only to the authorized individual for approval. RMAs shall not allow any additions or other alterations to files that have reached cutoff.

C2.2.6.5. RMAs shall identify records that have been frozen and provide authorized individuals with the capability to reactivate or change their assigned dispositions.

C2.2.6.6. RMAs shall provide for viewing, saving, and printing lists of records (regardless of media or location) that have no assigned disposition. (RMTF, reference (j))

C2.2.7. Retrieving Records

C2.2.7.1. RMAs shall allow searches using any combination of the following record profile data elements. (RMTF, reference (j))

C2.2.7.1.1.	Subject	(36 CFR 1234.22, reference (n))
C2.2.7.1.2.	Date Filed	(RMTF, reference (j))
C2.2.7.1.3.	Addressee(s)	(36 CFR 1234.22, reference (n))
C2.2.7.1.4.	Media Type	(RMTF, reference (j))
C2.2.7.1.5.	Format	(RMTF, reference (j))
C2.2.7.1.6.	Location of Record	(RMTF, reference (j))
C2.2.7.1.7.	Document Creation Date	(36 CFR 1234.22, reference (n))
C2.2.7.1.8.	Author or Originator	(36 CFR 1234.22, reference (n))
C2.2.7.1.9.	Originating Organization	(36 CFR 1234.22, reference (n))
C2.2.7.1.10.	Other Recipients (E-mail)	(36 CFR 1234.24, reference (s))
C2.2.7.1.11.	File Code	(36 CFR 1234.22, reference (n))
C2.2.7.1.12.	Disposition Instruction Code	(36 CFR 1234.22, reference (n))
C2.2.7.1.13.	Disposition Cutoff Date	(36 CFR 1234.22, reference (n))
C2.2.7.1.14.	Disposition Action Date	(36 CFR 1234.22, reference (n))
C2.2.7.1.15.	Disposition Action Code	(Transfer, Destroy, or Freeze)
C2.2.7.1.16.	Disposition Instruction Type	(Time, Event, Time-Event)
C2.2.7.1.17.	Vital Record Indicator	(36 CFR 1236.20, reference (k))
C2.2.7.1.18.	Record Identifier	(RMTF, reference (j))
C2.2.7.1.19.	User Defined Fields	(36 CFR 1234.22, reference (n))

C2.2.7.2. RMAs shall allow the user to specify whether or not an exact match of case is part of the search criteria.

C2.2.7.3. RMAs shall also allow for specifying partial matches for multiple word fields such as subject and date and shall allow designation of "wild card" fields or characters.

C2.2.7.4. RMAs shall allow searches using Boolean logic: and, or, greater than (>), less than (<), equal to (=), and not equal to (/=).

C2.2.7.5. RMAs shall present the user a list of records meeting retrieval criteria, or notify the user if there are no records meeting the retrieval criteria. The information contained in the list shall be user definable from the set of record profile attributes. (RMTF, reference (j))

C2.2.7.6. 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. (RMTF, reference (j))

C2.2.8. Transferring Records

C2.2.8.1. RMAs shall, using the disposition instruction for the record category, identify and present those records eligible for transfer. (44 U.S.C. 3103 and RMTF, references (b) and (j))

C2.2.8.2. RMAs shall, for records approved for transfer that are stored in the RMA, copy the pertinent records and associated profiles to a user-specified filename, path, or device. (36 CFR 1228.188, 36 CFR 1234.32, and RMTF, references (x), (q), and (j))

C2.2.8.3. RMAs shall, for records approved for transfer and that are not stored in the RMA, copy the associated profiles to a user-specified filename, path, or device.

C2.2.8.4. RMAs shall, for records approved for transfer, provide the capability for only authorized individuals to suspend the deletion of records and related profile until successful transfer has been confirmed. (44 U.S.C. 3105 and 36 CFR 1228.54, references (t), and (m))

C2.2.9. Destroying Records

C2.2.9.1. RMAs shall, using the disposition instruction for the record category, identify and present records that are eligible for destruction. (36 CFR 1228.58, 36 CFR 1234.32, and RMTF, references (y), (q), and (j))

C2.2.9.2. RMAs shall, for records approved for destruction and for records that have been transferred, present a second confirmation, within a dialog box, requiring authorized individuals to confirm the delete command, before the destruction operation of the records and/or profiles are executed. (44 U.S.C. 3105 and RMTF, references (t), and (j))

C2.2.9.3. RMAs shall delete records and/or profiles that are stored in its repository and have been approved for destruction, in a manner such that the records cannot be physically reconstructed. (36 CFR 1234.34, reference (z))

C2.2.9.4. RMAs shall restrict execution of the records destruction commands to authorized individuals. (44 U.S.C. 3105 and 36 CFR 1222.50, references (t), and (h))

C2.2.10. Access Control

C2.2.10.1. RMAs shall provide the capability to define different groups of users and access criteria. RMAs shall control access to records based on groups as well as individuals meeting the access criterion/criteria. (36 CFR 1234.28 and RMTF, references (v), and (j))

C2.2.10.2. RMAs shall support multiple-user access.

C2.2.10.3. RMAs shall control access to transfer and destroy functions based upon user account information. (36 CFR 1234.28 and RMTF, references (v), and (j))

C2.2.10.4. RMAs shall control access to audit functions based upon user account information.

C2.2.11. System Audits

C2.2.11.1. RMA audit utilities shall provide an account of records capture, retrieval, and preservation activities to assure the reliability and authenticity of a record. (RMTF, reference (j))

C2.2.11.2. RMA audit utilities shall provide a record of transfer and destruction activities 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. (RMTF, reference (j))

C2.2.11.3. RMAs shall provide the capability to store audit data as a record. (RMTF, reference (j))

C2.2.11.4. The following audit information shall be reported on demand: (RMTF, reference (j))

C2.2.11.4.1. Total Number of Records.
C2.2.11.4.2. Number of Records by Record File Code.
C2.2.11.4.3. Number of Accesses by File Code.

C2.2.11.5. The following audit information shall be logged for each delete operation: (RMTF, reference (j))

C2.2.11.5.1. Record Identifier.
C2.2.11.5.2. File Code.
C2.2.11.5.3. User Account Identifier.
C2.2.11.5.4. Date/Time.
C2.2.11.5.5. Authorizing Individual Identifier (if different from user Account Identifier).

C2.2.11.6. RMAs shall allow only authorized individuals to enable/disable the audit functions and to backup and remove audit files from the system.

C2.2.12. System Management Requirements

The following are functions typically provided by the operating system or a DBMS: (They 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.

C2.2.12.1. Backup of Stored Records. The RMA system shall provide the capability, as determined by the Agency, to automatically create backup or redundant copies of the records as well as their metadata. (36 CFR 1234.28 and RMTF, references (v), and (j))

C2.2.12.2. Storage of Backup Copies. The method used to backup RMA data base files shall provide copies of the data that can be stored off-line and at separate location(s) to safeguard against loss of records, record profiles, and other records management information due to system failure, operator error, disaster, or willful destruction. (36 CFR 1234.30, reference (aa))

C2.2.12.3. Recovery/Rollback Capability. Following any system failure, the backup and recovery procedures provided by the system shall provide the capability to complete updates (records, record profiles, and any other information required to access the records) to RMAs, ensure that these updates are reflected in RMA files, and ensure that any partial updates to RMA files are backed out. Also, any user whose updates are incompletely recovered, shall, upon next use of the application, be notified that a recovery has been executed. RMAs shall also provide the option to continue processing using all in-progress data not reflected in RMA files (36 CFR 1234.28 and RMTF, references (v), and (j))

C2.2.12.4. Rebuild Capability. The system shall provide the capability to rebuild forward from any backup copy, using the backup copy and all subsequent audit trails. This capability is typically used to recover from storage media contamination or failures. (RMTF, reference (j))

C2.2.12.5. 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 only authorized individuals of the need for corrective action in the event of critically low storage space. (RMTF, reference (j))

C2.2.13. Additional Baseline Requirements

The following are records management requirements that shall be implemented by the organization, but not necessarily by the RMA s:

C2.2.13.1. Electronic Calendars and Task Lists. Some electronic systems provide calendars and task lists for users. These may meet NARA's definition of a record (44 U.S.C. 3301, reference (bb). Calendars and task lists that meet the definition of records are to be managed as any other record. If the RMA being acquired does not have the capability to extract them 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.

C2.2.13.2. 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. above, the user organization shall implement processes or procedures to enable these records to be managed by the RMA. (36 CFR 1234.24, reference (s))

C2.2.13.3. Ability to Read and Process Records. Since RMAs are prohibited (paragraph C2.2.4.2., above) 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 maintaining the hardware and/or software used to create or capture the record; by maintaining hardware and/or software capable of viewing the record in its native format; by ensuring downward compatibility when hardware and/or software is updated, or by migrating the record to a new format before the old format becomes obsolete. Any migration shall be controlled to ensure continued reliability of the record. (36 CFR 1234.30, reference (aa))

C2.2.13.4. Classified and Other Sensitive Records. If required, the acquisition/using activity shall specify requirements and/or acquire additional capabilities for the management of records containing information classified in the interests of national security (see DoD 5200.28-STD and DoD 5200.1-R, references (cc) and (dd)); records that contain Privacy Act information (see DoD 5400.11-R, reference (ee); records exempt from release under the FOIA (see DoD 5400.7-R, reference (ff); or any other records that require special access control or handling. The using organization shall implement special procedures to comply with legal and regulatory requirements for those records. (36 CFR 1228.194, reference (gg))

C3. CHAPTER 3

NON-MANDATORY REQUIREMENTS

C3.1 REQUIREMENTS DEFINED BY THE ACQUISITION/USING ACTIVITY

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

C3.1.1. Data Base Management System (DBMS). The acquisition and/or using activity should determine if RMAs would interface with a user provided DBMS or a DBMS to be supplied by RMA vendors. If the DBMS is to be acquired separately, it should comply with FIPS 127-2, "Database Language SQL," reference (u).

C3.1.2. User Interface. The acquisition and/or using activity should define an industry standard graphical user interface for RMAs, such as Windows, Macintosh, X-Windows.

C3.1.3. Storage Availability. The acquisition and/or using activity should define the size of the storage space required for its organizational records with the related record profiles and associated audit files.

C3.1.4. Documentation. The acquisition and/or using activity should determine the type and format of desired documentation, such as user guide, technical manual, and installation procedures, to be provided by the vendor.

C3.1.5. System Performance. The acquisition and/or using activity should specify what is acceptable RMA system availability, reliability, response times, and downtimes that will satisfy the user's business requirements.

C3.1.6. Hardware Environment. The acquisition and/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 be executed.

C3.1.7. Operating System Environment. The acquisition and/or using activity should define the operating system environment (for example: UNIX, MS DOS, Windows 3.x, Windows 95, Windows NT, IBM OS/2, VMS, Macintosh) on which the RMA is to be executed.

C3.1.8. Network Environment. The acquisition and/or using activity should define the LAN, 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 executed.

C3.1.9. Protocols. The acquisition and/or using activity should identify the protocols, such as Transmission Control Protocol/Internet Protocol (TCP/IP), Simple Mail Transfer Protocol (SMTP), and X.400, that the RMA is to support.

C3.1.10. Electronic Mail Interface. The acquisition and/or using activity should specify the e-mail application(s) that the RMA is to interface with.

C3.1.11. Internet Interface. The acquisition and/or using activity should determine if and in what manner the RMA is to interface with the Internet.

C3.1.12. File Code Selection/Search Capability. The acquisition and/or using activity should specify the desired methods for assisting the user in the selection of the file code to be assigned to a record such as priority ordered lists or directed sear ches.

C3.1.13. End-User Orientation and Training. The acquisition and/or using activity should specify record manager and end-user training requirements.

C3.1.14. Government Information Locator Service. An organization may determine that RMAs should have the capability to implement the requirements of the Government Information Locator Service (GILS). (FIPS 192, reference (hh)) GILS was established to identify public information resources throughout the Federal Government, describe the information available in those resources, and provide assistance in obtaining the information. GILS may also serve as a tool to improve Agency electronic records management practices.

C3.2. OTHER USEFUL RMA FEATURES

Many RMA products provide the following time and labor saving functions either as standard or optional features to enhance the utility of the system: (The acquisition/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 categories, record category codes, disposition instructions, and disposition instruction codes. In addition, RMAs should provide the capability to detach part of the file schema, re-attach to any specified file; move files from one location to another within the schema; and delete a file and all of its sub-files.

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

C3.2.2.1. An Agency's pre-existing file plan.
C3.2.2.2. Disposition instructions and codes.
C3.2.2.3. Electronic records.

C3.2.2.4. Record profiles.

C3.2.3. Record Version. RMAs should provide the capability to store version(s) of a record in a RMA repository. These should be associated and linked.

C3.2.4. Retrieval of Latest Version. When the user selects a record for retrieval, RMAs should check for the latest version of the record and prompt the user that it is a later version, but allow the user the flexibility to retrieve any version.

C3.2.5. Interfaces to Other Software Applications. RMAs should interface to 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.

C3.2.6. Report Writer Capability. RMAs should provide the capability to generate reports on the information held within the RMAs repository based upon user-developed report templates or user query.

C3.2.7. On-Line Help. RMAs should have an on-line help capability for easy access to user operational information.

C3.2.8. Document Imaging Tools. RMAs should be capable of interfacing with document imaging and workflow software/hardware in order to be consistent with the DoD Automatic Document Conversion Master Plan.

C3.2.9. Fax Integration Tools. An organization may determine that there is a requirement for RMAs to interface with desktop or server-based fax products to capture fax records in their electronic format.

C3.2.10. Bar Code Systems. An organization may determine that there is a requirement to use a bar code system with RMAs. Bar code technology can be used to support the following records management tasks:

C3.2.10.1. File and correspondence tracking to positions, sections, or staff members.
C3.2.10.2. Creating, printing, and reading of labels for non-electronic records.
C3.2.10.3. Boxing of records for transfer.
C3.2.10.4. Box tracking for records holding facility operations.
C3.2.10.5. Workflow tracking.
C3.2.10.6. Posting changes in disposition.
C3.2.10.7. Record audit and census functions.

C3.2.11. Thesaurus. Many RMAs provide vocabulary control to group related records together through the use of an organizational thesaurus.

C3.2.12. Retrieval Assistance. RMAs should have additional search and retrieval features, such as full text search or other method(s) to assist the user in locating records.

C3.2.13. Workflow Features. An organization may determine that RMAs should have the capability to manage working and draft versions of documents and other potential record material as they are being developed.

C3.2.14. Records Management Forms. An organization may determine that RMAs should have the capability to generate completed standard records management forms such as:

C3.2.14.1. Standard Form 115 and 115-A, "Request for Records Disposition Authority."
C3.2.14.2. Standard Form 135 and 135A, "Records Transmittal and Receipt."
C3.2.14.3. Standard Form 258, "Request to Transfer, Approval, and Receipt of Records to the National Archives of the United States."
C3.2.14.4. National Archives Form 14012, "Database Record Layout."
C3.2.14.5. National Archives Form 14097, "Technical Description for Transfer of Electronic Records to the National Archives."

C3.2.15. Printed Labels. RMAs should provide the capability to produce hard copy codes or identifiers in the form of labels or other products as required.

C3.2.16. Logic Checks. RMAs should conduct logic checks to ensure consistency and assist with error checking for all required metadata elements.

C3.2.17. Viewer. RMAs should provide the capability to view each file in its stored format or its equivalent.

C3.2.18. Access Log. RMAs shall log the following audit information for each access:

C3.2.18.1. Record identifier.
C3.2.18.2. File code.
C3.2.18.3. User account identifier.