Department of Defense Records Management
Business Process Reengineering
Executive Level Report (Condensed)

Sponsors of BPR:

Honorable Emmett Paige, Jr.
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)

Ms. Cynthia Kendall
Deputy Assistant Secretary of Defense (Information Management)

Mr. Tom Bozek
Information Management, Functional Information Manager
Office of the Deputy Assistant Secretary of Defense (Information Management) (OASD(C3I))
Phone: (703) 604_1592 DSN: 664_1592
FAX: (703) 604_1492 DSN: 664_1492
E_mail: bozekt@c3icg2.c3i.osd.mil

Ms. Linda Bagby
Deputy Director C3I Policy
Office of the Deputy Assistant Secretary of Defense (Plans & Resources) (OASD(C3I))
Phone: (703) 604_1562 DSN: 664_1562
FAX: (703) 604_1492 DSN: 664_1492
E_mail: bagbyl@c3icg2.c3i.osd.mil

Executive Agent for FPI:

Colonel Greg Florey
Department of the Air Force, SAF/AAIQ
Phone: (703) 697_4501 DSN: 227_4501
FAX: (703) 693_1713 DSN: 223_1713
E_mail: florey@saf3.hq.af.mil

Project Manager:

Captain Daryll R. Prescott
Department of the Air Force, SAF/AAIX
Phone: (703) 614_0657 DSN: 224_0657
FAX: (703) 693_1713 DSN: 223_1713
E_mail: prescott@saf3.hq.af.mil

Table of Contents

Executive Summary. iv

1 Improvement Opportunities1_1

2 Functional TO_BE Model (IDEF0) (Year 2003) & Glossary2_1

2.1 TO_BE Model2_5
2.2 Glossary2_10

3 Information Model (IDEF1X) (Year 2003) & Glossary3_1

3.1 Overview of the Model3_1
3.2 Model3_3
3.3 Glossary3_6

4 Functional Support Requirements (Year 2003)4_1

5 Technical Review of Functional Requirements5_1

5.1 Draft Request for Proposal for Acquisition of Electronic Records Management Tools (Hardware/Software)5_1
5.2 Availability of Technology to Support Functional Requirements Matrix5_6

6 Review of NARA "Records Management Standards for E_mail"6_1

7 System, Security, and Routine Backup Requirements7_1

7.1 Policy Issues7_1
7.2 Discussion7_1

8 Distribution Lists and Records Retention (Electronic and Non_Electronic)8_1

9 Electronic Authentication, Encryption & Delivery, Return, and View Receipts9_1

10 Proposed Recommended Retention Schedule (Year 2003)10_1

Appendix A _ Executive Summaries

Appendix B _ Participant Lists

Appendix C _ References

Executive Summary

Representatives of the services and the Office of the Secretary of Defense (OSD), with the support of the Department of Defense (DoD) Corporate Information Management (CIM) initiative, are re_engineering records management to dramatically improve the process. The Assistant Secretary of Defense for Command, Control, Communication and Intelligence (ASDC3I) directs the CIM support through sponsorship by the Deputy Assistant Secretary of Defense for Information Management (DASD(IM)). The team is

employing standard DoD Business Process Re_engineering (BPR) methodology to identify better ways to manage records. The Records Management BPR team is proposing, by the year 2003, that DoD migrate to the TO_BE records management process. This method represents a single, agreed upon way to meet needs.

The scope of the BPR is to manage the life_cycle of information contained in records, regardless of medium. The viewpoint is that of the action officer or analyst at an office of record. In particular, the team is addressing the trend toward electronic records.

The Air Force, as Executive Agent for the BPR, is responsible for program management and oversight. Enthusiastic participation throughout the DoD from varying organizational levels has made this effort successful.

Completed events in the BPR effort include:

A scoping session of component/agency representatives. (August 1993)

Construction of four component AS_IS functional models by component/agency representatives. (September_October 1993)

Comparison of the four AS_IS models and construction of a DoD TO_BE functional model. (November and December 1993)

Construction of a DoD TO_BE information model. (January 1994)

Review of functional recommendations, technical issues, and available support tools by a multi_service/joint agency technical team. (November 1993_May 1994)

The BPR team developed improvement opportunity recommendations with six themes:

Develop standard DoD retention schedules.

Reduce the number of records retention periods.

Migrate toward a standard DoD coding system for records.

Develop standard DoD functional and automated system requirements for records management.

Incorporate records management requirements into Automated Information System development and redesign.

Develop standard DoD systems requirements for voice and E_mail records.

Remaining major scheduled BPR activities are:

Activity based costing to determine costs of present records systems and the possible economic feasibility to migrate into automated electronic records management systems.

A case study addressing the first three improvement opportunities.

Academic review by the Massachusetts Institute of Technology.

Industry benchmark study sponsored by Shell Oil Company.

A case study addressing the application of this effort into DoD identified migration and legacy systems.

The formal BPR effort is scheduled to conclude by August 1994. Current plans call for establishment of a transition project office to begin implementation of the recommendations.

1 Improvement Opportunities

Participants revised and refined improvement opportunities identified during the comparison matrix workshop. Working only on those opportunities dealing with policy and procedures, the participants initially identified twelve improvement opportunities. After two days of intensive group discussions and effort, that list was refined to six opportunities. Three of the original twelve opportunities were determined to be outside the scope of the current BPR work and four others were merged into the final six. In the merging process, one new improvement opportunity was developed. The final six improvement opportunities are:

Develop standard DoD retention schedules.

Reduce the number of records retention periods.

Migrate toward a standard DoD coding system for records.

Develop standard DoD functional and automated system requirements for records management. (Include public access to electronic records.)

Incorporate records management requirements into automated information systems development and redesign. (New).

Develop standard DoD systems requirements for voice and e_mail records.

The original twelve improvement opportunities are:

Develop a standard numbering system for records.

Develop a standard DoD retention schedule.

Define, in the standard DoD retention schedule, the minimum number of discrete retention periods needed to meet mission requirements efficiently.

Develop a standard DoD automated system.

Require the review and approval of automated support systems by records

managers to ensure compliance with the law.

Build Privacy Act and FOIA rules into information systems.

Promulgate improved policies for voice and E_Mail.

Provide electronic access/dissemination of electronic information (public access).

Implement a common DoD records schedule compatible with electronic records.

Simplify records schedules for electronic use (7 _ 9 retention periods).

Integrate records management functions with information resource management (IRM).

Request NARA issue up_to_date guidelines for permanent electronic storage.

The three improvement opportunities determined to be outside the scope of the current FPI work are:

Build Privacy Act and FOIA rules into information systems.

Integrate records management functions with IRM.

Request NARA issue up_to_date guidelines for permanent electronic storage.

The four improvement opportunities that were merged into the final six are:

Simplify records schedules for electronic use (7 _ 9 retention periods).

Define, in the standard DoD retention schedule, the minimum number of discrete retention periods needed to meet mission requirements efficiently.

Implement a common DoD records schedule compatible with electronic records.

Provide electronic access/dissemination of electronic information (public access).

The one new improvement opportunity that resulted from merging others is:

Incorporate records management requirements into automated information systems development and redesign.

2 Functional TO_BE Model (IDEF0) (Year 2003) & Glossary

The top level in an IDEF process model is the "context diagram." It describes

the most general activity (there is only one activity named at the top level of the model), inputs, controls, outputs and mechanisms in the model.

An activity is the transformation of inputs into outputs, performed by mechanisms under the constraints set by controls. The context diagram can be "read" as: "INFORMATION (the input) is transformed into RETRIEVABLE INFORMATION and DESTROYED RECORDS (the outputs) by RECORDS HANDLING TOOLS, HUMAN RESOURCES and FACILITIES (the mechanisms), under the guidance of LAWS, EXTERNAL REGULATIONS, IMPLEMENTATION GUIDELINES and PROCEDURES (the controls).

The TO_BE model has four processes decomposed as follows:

A1 _ CREATE RECORDS

A11 _ FILTER INFORMATION

A12 _ MAKE RECORDS

A13 _ ASSIGN DISPOSITION INSTRUCTIONS

A14 _ INDEX RECORDS

A2 _ MAINTAIN RECORDS

A21 _ STORE RECORDS

A22 _ SCREEN RECORDS

A23 _ RETRIEVE RECORDS

A3 _ TRANSFER RECORDS

A4 _ DESTROY RECORDS

2.1 TO_BE Model

2.2 Glossary

The following terms and definitions were developed by the participants during the TO_BE session. Terms in all capital letters (i.e., CREATE RECORDS) indicate a process. Terms in lower case (i.e Destroyed Records) indicate an input, output, control, or mechanism. The alphanumeric designations Ax (Ay) indicate where the terms appear on the IDEF0 model.

ASSIGN DISPOSITION INSTRUCTIONS
A1 (A13)
The process of matching retention schedules to records.

CREATE RECORDS
A0 (A1)
The process of collecting, organizing, and recording information on the appropriate media to document the agency's business, determining whether information is record or non_record material, categorizing by disposition schedule, and indexing for retrieval. A record may be made by internal processes of an agency.

DESTROY RECORDS
A0 (A4)
Change the characteristics of temporary records so the information is not retrievable.

Destroyed Records
A_0 / A0
Records which no longer exist.

Disposition
Not on model. A term which denotes transfer and/or destruction.

External Regulations
A_0 / A0 / A1 / A2
Guidance from the organizations of the Office of the President, Office of Management and Budget (OMB), National Archives Records Administration (NARA), General Services Administration (GSA), General Accounting Office (GAO), Department of Justice (DOJ), etc.

Facilities
A_0 / A0 / A1 / A2
Places where records are created and stored. This includes current files areas, holding/staging areas, and record centers.

FILTER INFORMATION
A1 (A11)
Process of sifting incoming information and documents to separate record and non_record material.

Human Resources
A_0 / A0 / A1 / A2
People.

INDEX RECORDS
A1 (A14)
Tagging records with unique identifiers for storage and retrieval.
Implementation Guidelines
A_0 / A0 / A1 / A2
Regulatory instruments initiated by the defense agencies such as regulations, letters, etc.

Information
A_0 / A0 / A1
Information is facts or data communicated or received. Upon receipt by the action officer it may become a record.

Laws

A_0 / A0 / A1 / A2
Legislation.

MAINTAIN RECORDS
A0 (A2)
Any action taken to administer and preserve a record during its life cycle.

MAKE RECORDS
A1 (A12)
Generating a new record, in any media, by the internal processes of an agency. This is the beginning of the life cycle of a record.

MANAGE RECORDS
A_0
Manage the life cycle of information, including the creation, maintenance (use, storage, retrieval), and disposition, regardless of media.

New Records
A1
A collection of record material (including original thought) organized as defined by the business processes of the office that has not been tagged with indices or disposition.

Non_Record Material
A0 / A1
Any information that the action officer is not required to manage as a record.

Procedures
A_0 / A0 / A1 / A2
Detailed methods for managing records that are prescribed at various levels in each Component (Army, Navy, Air Force, Defense Agencies).

Record Material
A1
Any information that the action officer is required to manage as a record.

Records
A0 / A1 / A2
Records includes all books, papers, maps, photographs, machine_readable materials, and other documentary materials, regardless of physical form or characteristics, made or received by an office in connection with the transaction of official business and preserved or appropriate for preservation by that office as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of that office or because of the value of data in the record.

Records Disposition Recommendations
A1
A proposal to change retention schedules.

Records Handling Tools
A_0 / A0 / A1 / A2
Hardware, software, and other devices used to manage records throughout their life cycle.

Records to Destroy
A0 / A2
Records eligible for destruction according to the retention schedule.

Records to Be Refiled
A2
Records that have been retrieved, used, and are being returned to records storage.

Records with Disposition Only
A1
Records which have been tagged with the appropriate retention instructions but have not yet been indexed.

Records with Index Only
A1
Records which have been tagged with unique identifiers but have not yet been tagged with appropriate retention instructions.

Requests for Information
A_0 / A0 / A2
Expressed needs or desires for information which is expected to be contained in Government records.

Retention Schedules
A0 / A1
The legal authority establishing the length of time a record must be kept before it is transferred or destroyed. (Permanent records are not authorized for destruction.)

Retrievable Information
A_0 / A0 / A2
Information, regardless of media, that can be found easily through the use of standardized approaches including cataloging and indexing techniques.

RETRIEVE RECORDS
A2 (A23)
To identify and/or remove a record from a storage system.

Retrieved Information
A0 / A2
Information, regardless of media, that can be found easily through the use of standardized approaches including cataloging and indexing techniques.

SCREEN RECORDS
A2 (A22)
Review for compliance with record "freezes," legal requirements, searches, declassification, disposition and quality control.

Selected Records
A2
Records identified as a result of a search using a given set of criteria.

STORE RECORDS
A2 (A21)

To retain records in an organized manner for purpose of (safeguarding and) preserving information throughout its life cycle and for ease of retrieval.

Stored Records
A2
Records organized for ease of retrieval and for preservation throughout their life cycle.

TRANSFER RECORDS
A0 (A3)
The movement of records from one organization to another, from office space to agency storage facilities, from one Federal agency to another, to a Federal Records Center, or for records requiring permanent preservation, to The National Archives.

Transferred Records
A0
Records moved from one organization to another, from office space to agency storage facilities, from one Federal agency to another, to a Federal Records Center, or, for records requiring permanent preservation, to The National Archives.

Transferable Records
A0 / A2
Records eligible for movement from one organization to another, from office space to agency storage facilities, from one Federal agency to another, to a Federal Records Center, or for records requiring permanent preservation, to The National Archives.

3 Information Model (IDEF1X) (Year 2003) & Glossary

3.1 Overview of the Model

The entity Record is the focal point of the model. Two codes uniquely identify each record: an identifier of the creating organization and a record identifier, which might be system generated. The model shows several non_key attributes which are required for records management. A record also contains other data related to the functional area that the record supports. These non_key attributes are outside the scope of this model. On this records management model, these functional attributes are represented by the attribute Record_Functional_Content.

A record's primary relationships are to Organization (in several relationships), to Disposition_Instruction though the associative entity Record_Category_Role, to Request For Information, to Addressee, to Distribution List, to Attachment, and to Sender.

Organization and Record have these relationships: originates, authenticates, and owns and/or maintains. Both entities are indirectly related to Request For Information that is satisfied by a Record and is received by an Organization.

Organization uniquely identifies the organizations that affect the management of records as creators, authenticators, owners, maintainers, and processors of requests for information.

Originates is a specific relationship. A record has only one recognized creator.

Authenticated_Record is an associative entity that resolves the non_specific relationship of authentication between Organization and Record. In some cases, a record is authenticated by more than one organization, e.g., memorandum of understanding. This entity also relates Organization_Position to show the position in the organization of the authenticator, e.g., commander, chief of staff, supply officer.

Owning/Maintaining_Organization_Record is an associative entity that resolves a non_specific relationship of owning or maintaining between Organization and Record. One organization could maintain a record owned by another organization, own a record that is maintained by another organization, or both own and maintain a record.

The Record_Schedule is a document which contains a listing of record categories. The listing is divided into categories. Each Record_Category describes a type of record (e.g., inspector general inspection, accident investigation, purchase order, budget request, personnel evaluation, weapons inventory). Each category is uniquely identified by the combination of the keys of its Record_Schedule and Records_Category.

The Role portrays a relative position of an organization in DoD or other Federal government and is used by functional proponents to specify the appropriate retention directions (Disposition Instruction) for a Record_Category. (Examples: Unit authorized a colonel commander. Special court martial authority. Wartime combat command headquarters authorized a 2_star commander.) A single organization may fill many different roles in the various functional areas.

Each instance of the associative entity Record_Category_Role has one and only one associated Disposition_Instruction. Because each Record has only one associated Record_Category_Role, each Record is matched to one and only one Disposition_Instruction.

The entity Disposition_Instruction consists of a unique disposition instruction code with associated narrative instruction (e.g., Destroy after two years; Destroy when no longer needed; Destroy after next comparable inspection).

The Request For Information entity seeks information contained in one or more records. Record_Request is an associative entity that resolves the non_specific relationship between Request For Information and Record.

Organization_Request For Information is an associative entity that resolves a non_specific relationship of receiving between Organization and Request_For_Information. (An organization can receive many requests for information; the same request can be received by or be sent to many organizations). Likewise Record_Request is an associative entity that resolves a non_specific relationship between a Request For Information and Record. (A request for information can apply to many records; a single record can be the object of many requests.)

Distribution List contains addressee information and may be used instead of or

in addition to specific Addressee references in the record. The Distribution List entity is related to both the Record and the Addressee entities through the associative entities Record_Distribution_List and Distribution_List_Addressee, respectively.

Sender is an entity that applies only to certain electronic communication_type records such as E_mail. Sender is shown on this model because it is proposed in NARA's draft E_mail standards.

Attachment is Information that is appended to a record. The attachment may be a record in itself. More than one attachment may be associated to a Record and the same information maybe associated with multiple records. Therefore the relation to Record is through the associative entity Record_Attachment.

3.3 Glossary

The following terms and definitions were developed (or adopted from previous works) by the participants during the IDEF1X TO_BE information modeling session.

Addressee
The person or organization to whom a correspondence type record is sent.

Attachment
Information that is appended to a record. The attachment may be a record in itself.

Attachment_ID
The attribute that uniquely identifies an attachment. This attribute will have varying forms dependent upon the nature of the attachment. If the attachment is a record in its own right the Attachment_ID would be RECORD_ID and Originating.ORGANIZATION_Code.

Authenticated_Record
Record approved by the proper authority.

Authenticating Organization_Code
The code used to designate an organization within the Federal Government that serves as an authenticating agency.

Delivered_Date/Time
The date and time that a record is delivered to the addressee's organization or electronic system. Examples: receipt information from acceptance of accountable mail and the date and time an E_mail system indicates a message was place in the addressee's mailbox.

Disposition_Instruction
The legal authority establishing the length of time a record must be kept before it is transferred, destroyed, or donated. (Permanent records are not authorized for destruction.)

Disposition_Instruction_Number
The number assigned to specific disposition instructions.

Disposition_Instruction_Text

The narrative description of the DISPOSITION_INSTRUCTION. (Examples: Destroy after two years. Destroy after next comparable inspection.)

Distribution_List
A collection of addressee information used to simply and to shorten communication type records. The record is addressed to the distribution list and the distribution system sends a copy to each addressee on the list.

Distribution_List_Addressee
An associative entity that links a distribution list with the addressees contained in the list.

Distribution_List_Code
The identifier used to uniquely identify a distribution list.

Information (from IDEF0 TO_BE model)
Information is facts or data communicated or received. Upon receipt by the action officer it may become a record.

Manage Records (from IDEF0 TO_BE model)
(scope of this model) Manage the life cycle of records, including the creation, maintenance (use, storage, retrieval), and disposition, regardless of media.

Organization
The organizational element that created, owns, or is otherwise related to a record.

Organization_Code
The code used to designate an organization within the Federal Government.

Organization_Position
A function or duty designator within a particular government entity.

Organization_Record_Association_Type
The code used to designate a particular association between a record and an organization (e.g., record maintainer, record owner, both maintainer and owner).

Organization_Record_Date
The date a specific organization_record_association was formalized.

Originating_Organization_Code
The code used to designate an organization within the Federal Government.

Owning/Maintaining_Organization_Code
The code used to designate an organization within the Federal Government that owns and/or maintains records.

Owning/Maintaining_Organization_Record
A record owned and/or maintained by a particular government entity.

Position_Title
The name of a particular function or duty within an organization.

Position_Title_Name
The name assigned to a position within the organization.

Received_Date
The date that a particular Request_For_Information is received at an organization.
Record (from IDEF0 TO_BE model)
Records include all books, papers, maps, photographs, machine_readable materials, and other documentary materials, regardless of physical form or characteristics, made or received by an office in connection with the transaction of business. Records are preserved or appropriate for preservation by that office: as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of that office; or because of the value of information in the record.

Record_Access Code
A tag on records to indicate who may see them.

Record_Addressee
The associative entity that resolves the non_specific relationship between record and addressee.

Record_Attachment
An associative entity that links a record with its attachments.

Record_Category
The description of a particular record within a series.

Record_Category_Code
The unique identifier for Record_Category.

Record_Date
The date assigned to a document.

Record_Distribution_List
An associative entity that links a record with its distribution list(s).

Record_Functional_Content
This attribute of record represents the functional information stored in the record, e.g., accounts payable, correspondence text and addressees, video tape, x_ray images. This information is the reason the record was created and is maintained.

Record_Functional_Information
A "place holder" attribute indicating the portion of the record that contains informational or historical value other than the attributes that uniquely identify the record or serve other records management purposes. Examples: the body of a letter, the photo portion of a patient's X_ray, the description of an accident in an accident report.

Record_ID
A sequentially_assigned, system_generated, unique number used to identify a particular record.

Record_Location
A tag on a record that indicates location.

Record_Media
The physical characteristic of the record.

Record_Request
An associative entity that specifically relates Request_For_Information from within or outside the organization that is linked to a Record that satisfies the request.

Record_Schedule
Publication of an organization stating policy and procedures for records management.

Record_Schedule_Number
The number assigned to a record management directive that contains a record's disposition instructions.

Record_Subject
What the record pertains to.

Request_For_Information
Expressed needs or desires for information that is expected to be contained in government records.

Request_For_Information_Identifier
A unique identifier used to identify a particular request for information.

Request_For_Information (from IDEF0 TO_BE model)
Expressed need or desire for information that is expected to be contained in government records.

Request_Subject
The subject associated with a particular request for information.

Requestor_Name
The formal name of the requestor that is associated with a particular request for information.

Retention_Schedule (from IDEF0 TO_BE model)
The legal authority establishing the length of time a record must be kept before it is transferred or destroyed. (Permanent records are not authorized for destruction.)

Role
Level in the DoD hierarchy of command as related to relative responsibility for information.

Role_Code
The code used to designate Role.

Role_Description
The text that establishes the criteria for designation of Role_Code.

Sender {E}
The person or office that transmits an e_mail message. This entity applies only to E_mail messages. Compare to entities AUTHENTICATED_RECORD, ORGANIZATION_POSITION, and POSITION_TITLE that identify the official title, but not the name, of the authenticator of paper correspondence and official message communications.

Viewed_Date/Time {E}
The date and time that an E_mail message is first "opened" by the addressee. Some E_mail systems provide this information. This attribute applies only to certain types of electronic records.

4 Functional Support Requirements (Year 2003)

During the session, the participants entered functional and system requirements for mechanisms to support the "MANAGE RECORDS" process. Participant functional and system requirements necessary to support the TO_BE process for the year 2003 are presented below. Unedited participant recommendations are contained in the session Source Data Report.

Any system which creates, maintains, transfers, or destroyed records will have the following capabilities. These requirements must be performed in support of the activity listed. All systems will be reviewed for Freedom of Information Act (FOIA) and Privacy Act considerations.

A1: CREATE RECORDS

1. Interface transparently with the operating environment and support tools such that certain functions, such as indexing, are performed transparently to the action officer.

2. Be compatible with existing paper records. Some paper records may still be in existence and possibly new types of non_electronic records may be created by the year 2003.

3. Automatically index all records created.

4. Automatically determine the proper disposition of each record created and store the disposition instructions with the record.

5. Provide automatic electronic date stamp or equivalent on created records.

6. Provide for the creation and storage of "working papers," both prior to and simultaneously with the addition of indexing and disposition instructions to the record before it can be stored.

7. Convert the storage medium of the record (i.e., hard disk to optical disk).

8. Feature common predetermined retrieval fields (i.e., subject, date, creator office) for ease of mass retrievals.

9. Provide a means to manually enter disposition instructions or override those the system selects.

A11: FILTER INFORMATION

1. Automatically filter out such items as E_Mail lunch invitations from actual information that should become a record.

2. Filter on standard data and information structures (i.e., E_Mail. Memorandums, Letters) to the maximum extent possible.

3. Convert from any format to the accepted standard (i.e., SGML, ASCII, etc).

A12: MAKE RECORDS

1. Generate standard reports (i.e. manpower documentation reports).

2. Add suspense times/events for the purposes of Freedom of Information or Privacy Act requirements.

3. Automatically track revisions to a record, document attachments, and addenda (i.e., provide an audit trail).

4. Incorporate margin notes on records without changing the actual record.

5. Integrate different information medium formats (i.e. optical disk, scanned paper, magnetic disk) to make a single record.

A13: ASSIGN DISPOSITION INSTRUCTIONS

1. Link records disposition to the coding/indexing scheme.

2. Assign disposition instructions automatically, but will allow for overriding the automatic selection through a selection from a displayed list.

A14: INDEX RECORDS

1. Create indexes based on characteristics such as disposition instructions, key words, subject, or full text.

2. Index automatically.

3. Allow for keyword search capabilities (subject, executive summary, full text, etc.).

A2: MAINTAIN RECORDS

1. Handle electronic copies, such as the creation and storage of information and reference copies. These copies will be handled as records themselves, but will have unique identifiers.

2. Include the capability to protect and distinguish access to classified and otherwise sensitive records.

3. Integrate indexing system with the paper indexing system such that retrievals are kept simple (i.e., multiple indexing systems not required).

4. Maintain an audit trail of record access, changes, etc.

5. Not allow changes to a record using the same record identifier (i.e. if a record is changed, a new record should be created and the old record kept in tact).

6. Provide a predetermined number of retrieval fields to simplify retrieval operations.

7. Recognize and utilize access restrictions such as clearance, need_to_know, etc.

A21: STORE RECORDS

1. Eliminate the possible loss of records due to system failures or operator errors through automated back_up procedures.

2. Store records in their native format (i.e., WordPerfect) or in an agreed standard.

3. Allow for both ease of retrieval and proper physical and electronic safeguarding of records.

4. Easily designate emergency records (Vital Records Program) that require duplicate storage.

A22: SCREEN RECORDS

1. Allow screening by either the action officer or the records manager.

2. Automatically display records for screening based on their disposition instructions. This capability will also incorporate features to handle event driven dispositions.

3. Incorporate features to ease screening for FOIA and Privacy Act requirements.

A23: RETRIEVE RECORDS

1. Retrieve records based on user level of access. Ensure that the records manager can also retrieve all records created within an agency.

2. Provide to the user the capability to retrieve by either the index or other predetermined fields. The system will give the user a list of records meeting retrieval criteria.

A3: TRANSFER RECORDS

1. Generate all required forms to transfer records, such as the Standard From (SF) 135. The forms and the records should be transferred electronically when possible.

2. Allow for the transformation of records into the proper medium for transfer to Federal Records Centers and the National Archives if electronic transfer is not feasible.

3. Verify the quality of records being transferred.

4. Maintain a detailed audit trail of transferred records including date, recipient, losing organization, and descriptions (identifier, file name, etc).

5. Automatically identify, according to disposition instructions, records requiring transfer.

A4: DESTROY RECORDS

1. Automatically identify records to be destroyed and notify the owner of the record or the records manager of the destruction requirement. Local policy will establish who to notify.

2. Build in safeguards to avoid accidental destruction of records. This will include a message which tells the user that the record hasn't reached its proper disposition period and queries the user to continue with the operation or cancel the operation. The system will have the capability to absolutely delete the record such that it is not retrievable, restorable, or reconstructible. Double checks for deletion/destruction are required.

3. Allow deletion only through the records management function of the system, based on access restrictions.

5 Technical Review of Functional Requirements

5.1 Draft Request for Proposal for Acquisition of Electronic Records Management Tools (Hardware/Software)

Users of this Strawman Request For Proposal (RFP) must review for their unique organization or functional requirements and modify this document as needed.

A review by the supporting offices for Records Management, System Support, and Legal is recommended to ensure that electronic records are: scheduled and managed properly, legal requirements are met, and correct backup, storage, and emergency recovery procedures are established.

ANNOTATION KEY

Brackets [ ] indicate the organization/functional proponent's specific or unique requirements.

Examples within the [ ] are for clarification. These are not mandatory items to be listed in the organization/functional requirement specifications.

Braces { } refer to activities of the Functional Model (IDEF0) in the DoD Records Management Functional Process Improvement (FPI) Report dated January 14, 1994.

STRAWMAN RFP

1 Create Records {A1_1 through A14_3}

1.1 The system shall seamlessly interface with the operating environment and supporting tools to the maximum extent possible. The system shall accomplish this by performing the following tasks [1., 2., 3., 4...].

1.2 The system shall accomplish the following functions without human intervention [1., 2., 3., 4...].

1.3 The system shall provide the following functions with some form of human verification [1., 2., 3., 4...].

1.4 Incoming information.

1.4.1 The system shall separate and distinguish between record from non_record material.

1.4.2 Incoming information determined to be a "record" __ the system shall identify the category of the record based on the record's structure type and/or information it contains.

1.4.3 The system shall use the following elements to make category identification and determination [1., 2., 3., 4...].

2 System compatibility for all records (electronic and non_electronic) {A1_2, A2_3}

2.1 The system should be able to track and manage all records _ electronic and non_electronic.

2.2 The system shall support functions for records in non_electronic media including type of record, assigning disposition instructions, indexing, and location.

2.3 The system shall provide the following search criteria for all records managed by the system [1., 2., 3., 4...].

3 Indexing and vital records management {A1_3, A1_8, A21_4, A23_2, A1_8}

3.1 The system shall automatically locate indexed records.

3.2 The system shall use the following elements to index and identify records [1. Originating organization, 2. Date of correspondence 3., 4...].

3.3 The system shall provide input capability for the following index items [1. Subject key words, 2. Other addresses, 3. Purpose, 4. Action office...].

3.4 The system shall create the following indexes automatically [1., 2., 3., 4...].

3.5 The system shall provide the capability to designate a record as belonging to [1. A vital record set, 2. Several vital record sets at one time, 3., 4...].

4 Disposition and storage instructions {A1_4, A13_1, A2_4, A3_5}

4.1 The system shall provide the capability to catalogue records.

4.2 The system shall automatically assign retention period and disposition instructions based on the category of records.

5 Individual working papers and date stamp {A1_5/6, A12_3, A12_4, A2_1, A2_5}

5.1 The system shall assign a unique key identifier for all records managed by the system.

5.2 The system shall distinguish between organizational records and individual workspace records.

5.3 The system shall provide that individual working space is independent of the organizational records space.

5.4 The system shall implement change control to document the history of record revisions.

5.5 The system shall provide the capability to annotate documents, leaving the original intact (e.g., like a sticky note).

5.6 The system shall not re_use record identifiers cleared by the disposition of records.

5.7 The system shall maintain a log of previously used record identifiers that are no longer available.

6 Convert storage medium {A11_3, A1_7, A12_5, A21_2, A3_2, A3_3}

6.1 The system shall [1. Store records in their native format, 2. Print records from their native format, 3. View records in their native format, 4...].

6.2 The system shall provide the capability to import and export records between the system storage environment and the following media [1. Paper, 2. Magnetic disk, 3. Optical disk, 4...].

6.3 The system shall convert system_stored records into the following standard formats [1. ASCII, 2. TIF, 3. SGML, 4...].
NOTE: Consideration should be made concerning data exchange with regard to physical media and data format.

6.4 The system shall be able to store multi_media information as a single record.

6.5 The system shall verify the quality of records being transferred by [1. Hashing, 2. Cyclical Redundancy Checks (CRC), 3., 4...].

7 Manual disposition {A1_9, A13_2}

7.1 The system shall allow designated personnel to manually supplement standard

record categories for special case records.

7.2 The system shall allow designated personnel to manually supplement retention periods and disposition instructions for special case records (e.g., pending NARA approval of new record types).

8 Reports generation {A12_2, A3_1, A3_4}

8.1 The system shall generate the following reports [1., 2., 3., 4...].

8.2 The system shall generate the following system utilization reports [1., 2., 3., 4...].

8.3 The system shall generate the information necessary to transfer records such as [1. Date, 2. Recipient, 3. Losing organization, 4...].

9 Suspense tracking {A12_2, A22_3}

9.1 The system shall add suspense times and events to allow tracking of suspense items [1. Who is suspended, 2. What organization, 3. Date of suspense, 4...].

10 Maintain Records {A22_1, A22_2}

10.1 The system shall screen and display records pending disposition or destruction.

10.2 The system shall notify the originator/custodian and/or the designated disposition authority of the records pending disposition or destruction [1. Within 30 days, 2. Two weeks, 3., 4...].

10.3 The system shall provide the capability for the originator/custodian of the records to view identified records and tag selected records for [1. Re_categorization, 2. Re_designation, 3. Movement to another..., 4...].

10.4 The system shall allow the originator/custodian of identified/tagged records that need disposition the capability to forward this information to the identified individual possessing disposition authority.

11 Records protection {A2_2, A2_7, A22_1, A22_3, A23_1}

11.1 The system shall distinguish different authorization levels to store and/or access records by [1. Categories of records, 2. Individual records, 3., Organizational records, 4...].

11.2 The system will provide personnel having disposition or retention authority safeguards to ensure that records are not accidentally disposed or destroyed.

12 Records backup, disaster prevention and recover {A21_1}

12.1 The system shall backup records at intervals such that minimum data and system files are not lost.

12.2 The systems record backup copy shall maintain records only to the extent necessary to recover the records in case of disaster.

12.3 The system shall provide that only one backup copy of records is maintained.

12.4 The system shall destroy each records backup every time a new backup is created.

12.5 The system shall provide that the management of records, records backup and system backup are mutually exclusive and independent of each other.

12.6 The system shall ensure that records backup is accomplished in such a manner to ensure that system files are not part of records backup.

12.7 The system shall ensure that records on backups that have passed their disposition are removed from the backup.

12.8 The system shall provide that no special feature be provided to save records that have passed their normal disposition when back_up files are updated or overwritten.

12.9 The system shall provide a backup to be maintained as a "security backup" to provide a means of ensuring retention and access in the event the original records and on_site backups are destroyed, inaccessible, or corrupted.

12.10 The system shall provide that system files backup and recovery is accomplished separately from records backup and recovery.

12.11 The system shall provide that systems management and records management are mutually exclusive and are accomplished independently of each other.

13 Destruction of records {A4}

13.1 The system shall provide access restriction capability to ensure that only properly identified personnel will dispose of or destroy records.

13.2 The system shall provide safeguards to ensure that only records identified for disposition or destruction are removed from the organizational or individual work spaces.

13.3 The system shall ensure that destroyed records are deleted from organizational records and all backups.

13.4 The system shall provide the capability to ensure that deleted records are not retrievable, restorable, or reconstructable by using the following destruction method [1., 2., 3., 4...].

13.5 The system shall provide that the level of deletion is accomplished using [1., 2., 3., 4...] standard of deletion.

14 Electronic Authentication and Encryption

5.2 Availability of Technology to Support Functional Requirements Matrix

The BPR technical team made judgment concerning whether technology is

available today or when technology will be available to accomplish the support requirements proposed by the TO_BE functional model workshop. (The support requirements are the items in the preceding sub_section.) Availability is defined as being reasonably procurable from multiple commercial or government sources at a reasonable cost ($100 to $300 per user).

The time line selection categories for availability are:

Now

In less than 5 years

In less than 10 years

Beyond 10 years

The results of the evaluation are in the following matrix.

A1_1
Certain Functions are Transparent to User
< 5 years

A1_2
Be Compatible with Paper Records
Now

A1_3
Automatically Index All Records Created
< 10 years

A1_4
Determine Disposition & Store Instructions
Now

A1_5
Date Stamp Electronic Records
Now

A1_6
Provide for "Working Papers"
Now

A1_7
Convert Storage Medium

Now

A1_8
Common Fields for Mass Retrievals
Now

A1_9
Manual Override of Disposition Instructions
Now

A11_1
Filter Out Non_Record Material
Now

A11_2
Filter on Standard Data/Information Structures
Now

A11_3
Convert Any Format to Accepted Format
Now

A12_1
Generate Standard Reports
Now

12_2
Add Suspense Information for PA/FOIA
Now

A12_3
Track Revisions to Record, Attachments, etc.
Now

A12_4
Incorporate Margin Notes
Now

A12_5
Integrate Media into Single Record
Now

A13_1

Link Disposition to Coding/Indexing Scheme
Now

A13_2
Assign Disposition Automatically with Override (A1:4&9)
Now

A14_1
Create Indexes from Visible Characteristics
Now

A14_2
Index Automatically
Now

A14_3
Keyword Search capability
Now

A2_1
Handle Electronic Copies
Now

A2_2
Protect Access to Sensitive records
Now

A2_3
Integrate Indexing with Paper Indexing System
Now

A2_4
Maintain Audit Trail
Now

A2_5
No Overwrite of Original
Now

A2_6
Predetermined Number of Retrieval Fields
Now

A2_7

Provide Access Restrictions
Now

A21_1
Automated Back_Up to Prevent Loss
Now

A21_2
Store as Produced or in Standard Form
Now

A21_3
Easy Retrieval and Safeguarding
Now

A21_4
Easily Designate Emergency Records
Now

A22_1
Screen by Either Action Officer or Records Manager
Now

A22_2
Automatically Display Based on Disposition Instructions
Now

A22_3
Ease PA/FOIA Screening
Now

A23_1
Retrieve Based on User Level of Access
Now

A23_2
Retrieve by Index or Other Set Fields
Now

A3_1
Generate and Send Transfer "Forms"
Now

A3_2

Allow Transfer to NARA_Approved Medium
Now

A3_3
Verify Quality at Transfer
Now

A3_4
Audit Trail of Transfer
Now

A3_5
Identify Transfer Records Per Disposition Instructions
Now

A4_1
Identify Records to Destroy and Notify Owner
Now

A4_2a
Prevent Accidental Destruction
Now

A4_2b
Destroy Absolutely
< 5 years

A4_3
Destruction Only Through RM Function with Access
Now

6 Review of NARA "Records Management Standards for E_mail"

The National Archives and Records Administration (NARA) is developing standards for management of Federal records created or received on electronic mail (E_mail) systems. These standards will be published as an appendix to regulations on electronic records in 36 CFR part 1234. NARA has asked Federal agencies to review and comment on the draft.

The technical team of the DoD Records Management Business Process Re_engineering (BPR) work group reviewed the NARA proposal and suggests extensive revisions in a response composed of a revised standard with annotations to explain the proposed changes.

The BPR Team agrees with NARA that many agencies are not applying

existing records management standards to electronic records and this situation must be corrected. As written however, the draft standard infers that an entirely new set of standards is required for E_mail. Records management policies should apply to all records regardless of medium. Instead of creating a new set of standards, NARA should apply the current standards with whatever modifications are necessary to meet emerging legal or functional requirements. The BPR Team's suggested alternative standard follows this philosophy.

The BPR Team's revised standard does not suggest linking disposition instructions to the medium of the record as does NARA's proposal. The BPR Team believes that most records in electronic format may be assigned disposition instructions in accordance with existing record schedules. The BPR Team agrees "that agencies cannot delete any records from E_mail systems or electronic records keeping systems until such time as NARA extends authorization to these categories of records" only with the understanding that "categories of records" are not defined by the medium of storage, but rather by the information in the records.

The BPR Team recommends that existing policies for retention of directories, distribution lists, and calendars also apply to E_mail directories and distribution lists and to electronic calendars. As written, the proposal infers these are entirely new classes of records that require new consideration.

The BPR Team proposes "that electronic records remaining live on an E_mail system after the record has been preserved on a records keeping system" are working papers or non_record material rather than "material suitable for destruction."

The BPR Team response to NARA is on the following pages. The format is:

Left Column:
Center
Column
Right Column

Original NARA's proposal on
"Records Management
Standards for E_mail"
Line
numbers
BPR Team review using
functional requirements from
functional and information
model reports

"Executive Level Report (ELR)
Chapter #" refers to chapter in
the (Condensed) that
discusses this issue.

Underlining indicates BPR Team recommended text revision.

No text means BPR Team has no comment at this time.

"Remove to end of paragraph" indicates that BPR Team recommends text after changes be removed.

Bold text indicates an annotation from the BPR Team.

The BPR Team responses, found in the following pages 1_29, are compared against the NARA Notice of Records Management Standards for E_mail. These pages are designed for removal from this document. An Electronic copy can be found at NARA.TXT

7 System, Security, and Routine Backup Requirements

7.1 Policy Issues

Specify the difference and use of each type of backup (system, security, routine).

Retention/disposition for back_up records should be incorporated.

Back_up should not be used as a records system.

System personnel and records managers need to coordinate efforts to ensure the organizational needs are met, systems maintenance and operations are acceptable, and records management requirements met.

7.2 Discussion

Electronic records are maintained in automated systems whose system managers periodically back_up files to ensure the information stored in records is not lost in the event of hardware, media, software failure, or through sabotage. These back_ups contain organizational records that are subject to Freedom of Information Act (FOIA) requests. The back_up schedules are prepared by the automated system managers based on what is needed to ensure continued system operation or recovery. Minimal or no coordination is being done between the system managers and records managers to ensure record retention instructions are instituted.

System related back_ups should not be used as the means for records retention. Integration of records retention schedules and back_up schedules is not feasible given the differing purposes of the two and the variance in retention schedules among records that may be stored in the same back_up.

Whatever procedure is used for records management, approved records schedules must be followed. Records must be transferred and destroyed in accordance with established instructions.

Back_up policy should specifically address system back_ups and data(records) back_ups as separate distinct activities.

System back_ups concentrate on the programs (e.g., operating systems and application software) necessary to make the system operate. Such back_ups may be kept for extensive periods, possibly until the software is superseded by a new version.

Data (or record) files may be kept for shorter periods of time, especially since they are backed up frequently. It is not economically feasible to locate and destroy those records whose retention period has ended before the life of the data file back_up occurs. Back_ups may be destroyed on a regular and frequent basis, however, if data files are also backed up frequently only non_ expired records will be maintained. For example, data files might be destroyed one week or one month after they are created because more recent back_ups exist.

The same policy of timely destruction of data back_ups may apply to off_site security back_ups.

The policies stated here should minimize the occurrence of past destruction date records "living on" in system and security back_ups while not imposing additional costs on organizations.

8 Distribution Lists and Records Retention (Electronic and Non_Electronic)

8.1 Policy Issues

Disposition/retention should be based on value not medium.

Disposition/retention should be consistent regardless of medium.

Lists should be maintained so that (1) the list is available and related to the document which used it, or (2) attached to the document or record.

Electronic distribution lists should match their non_electronic counterparts.

Electronic distribution lists should use organizational accounts which match their non_electronic counter_parts and not use personal accounts.

Structure the use of electronic media to be the same as non_electronic

media, i.e., require the use of organizational accounts which emulate in the electronic world what is accomplished with office addresses in the non_ electronic world.

Organizational accounts should be the same or as similar as possible to the organizational address used for non_electronic information.

8.2 Discussion

Records Management Requirements for Distribution Lists Associated with Electronic and Non_Electronic Records.

Distribution lists, whether electronic or non_electronic, should be retained as long as the longest retention period of the records to which they apply.

A record addressed using a distribution list is incomplete unless the distribution list in effect can be referenced when the record was released. The addressees cannot be determined without the distribution list.

Typically, current paper media policy is to keep distribution lists if they are included as a part of mail directives. Such directives are maintained by each organization. Also, paper_based distribution lists can usually be reconstructed from organizational charts and/or permanent orders (required to create an organizational change) which are also permanent records. The policy for records management in all media must be to retain distribution lists for as long as the longest retention period of the records created using that distribution list.

The distribution list challenge is particularly daunting for E_mail records because the lists are changed more frequently than are distribution lists for paper records. Also, unless special measures are taken, an update of an E_mail distribution list update overwrites the previous version. Complicating matters further is the ability of each user to create and modify their own lists as frequently as desired.

Identification of the sender and receiver of communications must be maintained for the entire retention period of the record.

One possible solution is for the E_mail system to show every addressee on all copies of the record.

Another option is to establish procedures and files for the retention of distribution lists. The system could automatically collect and store these for a predetermined period of time.

Another aid to retain addressee information is to implement naming conventions that assist in identifying the addressee. Aliases and system addressees that bear no relation to the addressee's name should be prohibited. For example, use "Joe=Smith%10_EMS%RAF_Alc@alcon.af.mil" instead of "ems230@alcon.af.mil." The first example contains enough plain English to identify a person in a unit at a base. In the paper world, mailing addressees follow a standard format beginning with a person or organization's name; E_mail addresses should too.

The job of retaining distribution lists is eased with a policy that allows only common, organizational mail boxes to be used to issue policy directives. Typically, documents requiring longer retention are produced from organizational mailboxes; personal E_mail and personal distribution lists may be destroyed sooner.

9 Electronic Authentication, Encryption & Delivery, Return, and View Receipts

9.1 Policy Issues

Electronic systems/e_mail applications should provide the capability of electronic authentication and encryption but these should be an "ON/OFF" capability.

Organizations should determine the need to utilize authentication or encryption.

All current systems which don't support these capabilities should migrate.

Procurement organizations should be made aware of this requirement if accepted as a standard.

Return receipt, delivery receipt, and view receipt capabilities should be available but these should be an "ON/OFF" capability.

Organizations should determine the appropriate use of receipts.

Organizations should determine the use of and need for encrypting organizational files.

Maintenance, retention, and disposition of password and encryption keys needs to be established.

Receipts and authentication when used must be maintained with the record.

9.2 Discussion

Identified migration and legacy systems should implement records management system requirements of this BPR in their next version changes.

Change procurement process so that organizations that purchase records management software when upgrading or migrating to local area networks.

Change procurement process for organizations and functionals to include review by their legal community to ensure that records requiring authentication and/or encryption are identified and the capability is purchased with the application.

Require the electronic authentication capability be available in electronic sys_ tems (specifically E_mail systems). This requirement should be available, but will NOT be used all the time.

Require the capability to encrypt text in electronic systems (specifically E_mail systems). Upon identification by the National Institute of Standards and Technology's (NIST) government standard, require all upgrades to electronic records management systems be compatible with the standard.

Require the maintenance of the public key and private key codes for organizational records. Recommended retention period should be the same period of the longest record which used the key.

Allow organizations or functional areas to procure applications which have authentication or encryption capabilities. Each organization or functional area should determine if these capabilities are required.

Require any records management E_mail, etc. application available for use within DoD to have available (either as part of the complete application or available as modules) electronic authentication, encryption, delivery, and return receipt information.

Policy should identify that password access and account access is reasonably secure and may be sufficient to secure records without authentication or encryption.

Adopt, for E_mail, the policy now in effect for records distributed by mail or other messenger service that calls for selective use of return receipt with delivery date and time. The capability for receipt and acknowledgement MUST be available in E_mail systems. Its use should not be mandatory, but rather applied on an as_required basis.

Develop position on electronic authentication and plan to change the DoD culture that now requires an ink signature to migrate toward electronic authentication.

Require any special capabilities (electronic authentication, encryption, delivery receipts, etc.) be captured in backup files (both security and regular backup files) as part of the record if they are used. It is felt that if it was important enough to encrypt or get a receipt, it is important enough to maintain as part of the record.

10 Proposed Recommended Retention Schedule (Year 2003)

Retention Period	Procedure
Keep until no longer	

needed ("Working
papers" in individual
system assigned work
area).

(Possibly one working
area in each "record
series.")
Record comes up "automatically" at the end of
one year from date of creation.

System options:
[KEEP IN WORK AREA] [FILE] [DESTROY]

If kept as a working paper, comes up
"automatically" again after one year.

System options:
[FILE IN DIFFERENT CATEGORY]
[DESTROY]

System offers capability to clean out or
categorize at any time.

2 Years
Records identified to originator/custodian
and/or records manager

5 years
Records identified to originator/custodian
and/or records manager

10 years
Records identified to originator/custodian
and/or records manager

25 years
Records identified to originator/custodian
and/or records manager

50 years
Records identified to originator/custodian
and/or records manager

75 years
Records identified to originator/custodian
and/or records manager

Permanent
Records identified to originator/custodian
and/or records manager

Appendix A _ Executive Summaries

Scoping Session

AS_IS Functional Modeling
Air Force
Army
Navy
OSD

Activity Based Costing Matrix

TO_BE Functional Modeling (IDEF0)

Technical Team Session 5

TO_BE Information Model (IDEF1X)

(Draft) Technical Team Session 6

Appendix B _ Participant Lists

Scoping Session

AS_IS Functional Modeling
Air Force
Army
Navy
OSD

Activity Based Costing Matrix

TO_BE Functional Modeling (IDEF0)

Technical Team Session 5

TO_BE Information Model (IDEF1X)

(Draft) Technical Team Session 6

Appendix C _ References

1. Department of Defense Records Management Functional Process Improvement Scoping Report, October 1, 1993.

2. Department of Defense Records Management Functional Process Improvement Air Force AS_IS Report, November 10, 1993.

3. Department of Defense Records Management Functional Process Improvement Army AS_IS Report, November 10, 1993.

4. Department of Defense Records Management Functional Process Improvement OSD AS_IS Report, November 10, 1993.

5. Department of Defense Records Management Functional Process Improvement Navy AS_IS Report, November 10, 1993.

6. Department of Defense Records Management Functional Process Improvement Comparison Matrix Workshop Report, November 26, 1993.

7. Department of Defense Records Management Functional Process Improvement TO_BE Report, January 14, 1994.

8. Department of Defense Records Management Functional Process Improvement TO_BE Information Model Report (IDEF1X), February 10 & 15, 1994, with Change 1 of April 27, 1994.

9. Department of Defense Records Management Functional Process Improvement Technical Team Meeting 5, February 23 _ 25, 1994.