National Archives and Records Administration (NARA)
Electronic Records Archives (ERA)

System Architecture and Design Document (SADD)
Summary
Non-CDRL Document
Version: 1.1.0

September 29, 2006

Status: Final

Document Number: NARA-2006-0325

Thomas S. Campbell, NARA CO, 301-837-1987

Mary Winstead, NARA COR, 301-837-3167

National Archives and Records Administration (NARA)
8601 Adelphi Road
College Park, MD 20740-6001

LOCKHEED MARTIN

Lockheed Martin Transportation and Security Solutions
7601 Ora Glen Drive
Greenbelt, MD 20770

Debra L. Jones, LMTSS Contract Administrator
301-623-4233

Contract Number: NAMA-04-C-0007

This page intentionally left blank.

Trademark Notice

Company, product, and service names that appear in this document may be trademarks or service marks of various companies other than Lockheed Martin Transportation and Security Solutions.

Change History

Table 1 – Change History

Change Contact	Date	Summary of Change
D. Earman	09/29/2006	Initial Issue

This page is intentionally left blank.

Preface

This document was prepared by Lockheed Martin Transportation and Security Solutions (LMTSS) for the National Archives and Records Administration (NARA) Electronic Records Archives Program Office per the Electronic Records Archives (ERA) contract number NAMA-04-C-0007.

This page is intentionally left blank.

TABLE OF CONTENTS

This page intentionally left blank.

LIST OF FIGURES

This page intentionally left blank.

LIST OF TABLES

1. INTRODUCTION

1.1 Purpose

The National Archives and Records Administration (NARA) is responsible to the American people as the custodian of a diverse and expanding array of evidence of America's culture and heritage, of the actions taken by public servants on behalf of American citizens, and of the rights of American citizens. The core of the NARA mission is that this essential evidence must be identified, preserved, and made available for as long as authentic records are needed—regardless of form.

The Electronic Records Archives (ERA) System is intended to preserve authentically any type of electronic record, created using any application on any computing platform delivered electronically and on any digital medium, from any entity in the Federal Government and any donor, and to provide discovery and delivery to anyone with an interest and legal right of access, now and for the life of the republic. The ERA System is also intended to support selected archival management tasks for non-electronic records, such as the scheduling and appraisal functions.

The delivered system will be an integrated system of Commercial-Off-The-Shelf (COTS) products to the maximum extent possible. The ERA System will subsume the functionality of other specified NARA legacy systems and will interface with external systems via the ERA System Interface specified in the ERA Interface Requirements Specification (IRS).

1.2 Scope

This System Architecture and Design Document (SADD) is the overall document for the ERA Program that provides description of the ERA System architecture and design. This document provides an understanding of the end-state architecture and design, and provides description of components to denote how the program will be heading toward this path.

It is useful to note that architectural and design decisions can have long-term repercussions. Thus, it is important that these decisions are clearly communicated and reviewed at incremental points within the system development life cycle. This document describes the decomposition of the ERA System from the System Requirements Specification (SyRS) requirements to the conceptual functional, data, and physical structures; the conceptual structures are then decomposed to the high-level software, data, and hardware design components. Key requirements and strategies are presented with this decomposition. In addition, the Lockheed Martin (LM) Team discusses the context of the ERA Architecture within the NARA Enterprise Architecture, the ERA System performance and availability models, the functional architecture of the ERA System, and how the architecture translates to design.

1.3 Document Organization

This document is structured consistent with the format and content provisions of the Lockheed Martin Data Item Description (DID).

The first part of this document presents the LM Team's ERA System Architecture followed by a discussion of the relationship of this architecture to the NARA Enterprise Architecture. The second part of the SADD presents the LM Team's ERA System Design. Appendices provide definitions to key terms used throughout the program, diagram notation, and a list of acronyms.

The SADD is organized in the following manner:

- Section 1, Introduction, provides administrative information and document structure.
- Section 2, System Architecture, describes the ERA System context; operational concept; driving requirements, key system concepts; the Service Oriented Architecture model; and the ERA System functional, physical, security and data architectures.
- Section 3, Relationship to NARA Enterprise Architecture, presents a mapping of the ERA System architecture to the NARA Enterprise Architecture.
- Section 4, Trade Study Methodology, reviews the LMTSS COTS product evaluation methodology.

- The Appendices in Volume 1 provide general reference material:
  - Appendix A provides a Glossary of Terms.
  - Appendix B provides a List of Abbreviations and Acronyms.
  - Appendix C provides a Tutorial on SADD Diagram Notation.

1.4 Intended Audience

This document is intended for the ERA Program Management Office (PMO), ERA stakeholders, and the LM Team.

1.5 Referenced Documents

1.5.1 Standards

- IEEE-Std-1471-2000, Institute of Electrical and Electronic Engineers (IEEE) Recommended Practice for Architectural Description of Software-Intensive Systems
- IEEE-Std-830-1998, IEEE Recommended Practice for Software Requirements Documentation
- Federal Information Processing Standards (FIPS) 140-2, Security Requirements for Cryptographic Modules, May 2001
- National Security Agency (NSA)/ National Institute of Standards and Technology (NIST) Configuration Documentation
- Director of Central Intelligence Directive, (DCID)-6/3 PL3, Protecting Sensitive Compartmented Information Within Information Systems, May, 2000
- Universal Description, Discovery and Integration (UDDI) 3.0
- Organization for the Advancement of Structured Information Standards (OASIS) Electronic Business Extensible Markup Language (ebXML) Registry 3.0
- Web Services Description Language (WSDL) 1.1
- OASIS Extensible Style Sheet Language Transformations (XSLT), Version 1.0
- Simple Object Access Protocol (SOAP) 1.1
- Lightweight Directory Access Protocol (LDAP)
- OASIS Security Assertions Markup Language (SAML)
- Relational data access: JDBC/XQJ/JDO/other and SQL
- File Data Access: Application Programming Language and Operational Software
- XML data access: XQJ and XQuery
- MADS, Metadata Authority Description Standard
- MODS, Metadata Object Description Standard
- MARC 21, Machine Readable Catalog

- Section 508 of the Rehabilitation Act of 1973, as amended 29 U.S.C. § 794 (d)
- CCSDS 650.0-B-1, *Reference Model for an Open Archival Information System (OAIS)*. Blue Book (Standard). Issue 1, January 2002
- CCSDS 651.0-B-1, *Producer-Archive Interface Methodology*, Blue Book (Standard). Issue 1, May 2004
- DoD 5015.2-STD, *Design Criteria Standards for Electronic Records Management Software Applications*, June 19, 2002
- ANSI/NISO Z39.19-2003, *Guidelines for the Construction, Format and Management of Monolingual Thesauri,* August 28, 2003
- Metadata Encoding and Transmission Standard (METS), version 1.4, January, 25, 2005, http://www.loc.gov/standards/mets/
- Machine-Readable Cataloging (MARC 21) Standards, March 1, 2005, http://www.loc.gov/cds/marcdoc.html
- Web Ontology Language (OWL), February 4, 2005, http://www.w3c.org/2004/OWL/
- OASIS WSRP, *Web Services for Remote Portlets*, September 3, 2003, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsrp
- SUN JSR 168, *Java Portlet Specification*, October 27, 2003, http://www.jcp.org/en/jsr/detail?id=168
- Unicode 4.0, http://www.unicode.org
- Extensible Markup Language (XML), http://www.w3.org/XML/
- MIL-STD-756, Reliability Prediction and Modeling
- MIL-STD-882, Department of Defense Standard Practice for System Safety
- MIL-STD-1629, Procedures for Performing a Failure Mode Effects and Criticality Analysis

1.5.2 NARA Documents

- ERA Requirements Document (RD v3.1), October 17, 2005
- ERA Statement of Objectives (SOO), NARA ERA RFP, Section J1, Amendment 001, December 24, 2003
- ERA Concept of Operations (CONOPS v4.0), July 27, 2004
- ERA Use Case Document (UCD v2.2), June 18, 2004
- ERA Target Release Paper (TAR v1.1), December 2, 2003
- NARA Business Process Re-engineering Flows, September 13, 2004
- NARA Business Process Re-engineering Flows, December 6, 2004
- NARA Enterprise Architecture Overview (Version 3.2), September 13, 2004
- NARA Data Architecture (Version 3.2), September 13, 2004
- ERA Domain Model (EDM v2.0), September 12, 2005
- ERA Load Analysis Report (LAR) v3.0, June 2, 2006
- FISMA, NARA 804 – *Information Technology Systems Security Handbook*, NIST SP 800-18, and DCID 6/3
- NARA Key Questions and Answers about Templates (Version 1.0), December 17, 2004

- NARA Information Quality Guidelines, http://archives.gov/about_us/information_quality/guidelines.html, April 3, 2005

1.5.3 Government Documents

- Service Component-Based Architectures, Version 2.0, June 2004

1.5.4 Lockheed Martin Documents

- ERA System Requirements Specification (SyRS), April 17, 2006
- ERA Interface Requirements Specification (IRS), April 17, 2006
- ERA Human Factors Specification, March 10, 2006
- ERA Interface Control Document (ICD) Non-Electronic Records Tracking Systems Interface, April 1, 2005
- ERA Interface Control Document (ICD) Transferring Entity Systems Interface
- ERA Security Risk Assessment Report
- ERA System Security Plan
- ERA Certification and Accreditation (C&A) Plan, May 19, 2006
- ERA Operations and Support Plan
- ERA System Engineering Management Plan (SEMP)
- ERA System Evolution Plan

1.5.5 Other Documents

- NCSC-TG-004-88, Glossary of Computer Security Terms, October 1988
- *Service Component-Based Architectures*, Version 2.0, Federal Chief Information Officers Council, June 2004
- Erl, Thomas, *Service Oriented Architecture - A Field Guide to Integrating XML and Web Services*, Prentice Hall, 2004
- Fowler, Martin, *UML Distilled A Brief Guide to the Standard Object Modeling Language*, Third Edition, Addison-Wesley, 2004
- Hunter, Cagle, Dix, Kovak, Pinnock, Rafter, *Beginning XML,* 2nd Edition, Wrox Press Ltd., 2001
- McComb, Dave, *Semantics in Business Systems: The Disciplines Underlying Web Services, Business Rules, and the Semantic Web*, Morgan Kaufmann Publishers, 2004
- Gamma, Erich; Helm, Richard; Johnson, Ralph; and Vlissides, John; *Design Patterns: Elements of Reusable Object-Oriented Software,* Addison Wesley Professional, 1995
- Buschmann, Frank; Meunier, Regine; Rohnert, Hans; Sommerlad, Peter; and Stal, Michael; *Pattern-Oriented Software Architecture: A System of Patterns,* Wiley Pbulishers, 1996

1.6 Approach

This document provides the overall approach to addressing system architecture and system design principles within the ERA Program. The use of the words "architecture" and "design" are often used interchangeably. In this document:

- System architecture is the conceptual, organizational structure of the ERA System, and
- System design is the collection of hardware and software components and their interfaces that provide the framework for developing the ERA System.

Based on this definition, this document describes ERA System concepts at the overall system architecture level. The goal is to provide an overall understanding of the system end-state and acknowledge that the system is being developed in increments. The approach is for the system architecture to be consistent throughout the entire life of the program. However, the system design will vary based on specific design conducted based on the incremental development life cycle.

The development and documenting of the ERA System architecture and design have been performed consistent with LM standard integrated engineering processes. The following sections discuss the methodologies employed within these processes, the benefits realized by these methodologies, and the modeling elements utilized in this document.

1.6.1 Methodology

The LM Team's engineering approach and the resulting architecture and design artifacts in this document leverage the best of structured analysis and object-oriented methodologies.

Application of a structured methodology ensures the complete conceptualization at the system-level by providing a high-level functional decomposition of the ERA System. The structured methodology is complemented by use of object-oriented methodology specifically as it relates to the Service Oriented Architecture (SOA) paradigm. The details of the SOA definitions and usage will be discussed later within this document.

Development of the ERA System software design follows an object-oriented approach providing the definition of the ERA System services, and a representative sample of system threads. Combining a structured analysis methodology for the system architecture with an object-oriented methodology for the system design balances the benefits of a more compact and abstract functional view with the more voluminous and concrete object view. The architecture and design included in this document reflects the LM Team's understanding of the requirements.

1.6.1.1 ERA System Architecture

The LM Team developed the ERA System architecture through iterative and parallel steps that yielded a system view that allowed multiple views. The goal of architectural modeling is to facilitate the ability to describe, understand and verify the conceptual integrity of system components (hardware, software, people, data and communications) and their relationships. The ERA System view was developed based on architectural modeling and defined the process to implement each task. The execution of the steps within each task was iterative. The result is the conceptual description of the ERA System allowing for multiple potential implementations. Tradeoffs occur during the design process to identify the "best" implementation.

The architecture definition produces: 1) the partitioning of the ERA System into components; 2) the allocation of function and data to components; and 3) the identification of connectivity between the components. Table 2 summarizes the ERA System architecture process:

Table 2 – Summary of System Architecture Process

Task and Objective	Steps	Products
Task: Analyze SyRS Requirements	• Identify drivers and constraints	• ERA System Architectural and Design Considerations
Objective: Gain insight into system partitioning possibilities	• Allocate SyRS requirements to major system functions	• ERA System-level Packages: – Ingest – Records Management – Preservation – Archival Storage – Dissemination – Local Services and Control – ERA Management
Task: Develop Functional Architecture	• Identify external interfaces	• ERA System Context Diagram
Objective: Develop and describe framework for system design	• Identify major system functions • Identify major data stores • Identify internal interfaces and data flows between major system functions	• ERA System Functional Architecture Diagrams • ERA Security Functional Architecture Diagrams • ERA System Domain Model
Task: Develop Physical Architecture	• Identify physical components	ERA System Physical Architecture Diagrams
Objective: Develop and describe framework for system hardware design	• Identify location of physical components • Identify interconnections of physical components	

1.6.1.2 ERA System Design

The system design describes the decomposition of the ERA System to hardware and software components, ultimately leading to hardware and software COTS product selections and the identification of software components to be developed. Similar to the ERA System architecture development, the execution of the ERA System design process within each task was iterative.

The LM Team developed the ERA System software design using an object-oriented methodology, initially defining the sub-package services and their associated methods, inputs and outputs by analyzing and allocating the SyRS requirements. A representative sample of system threads was documented via Unified Modeling Language (UML) sequence diagrams and this work also fed back into the definition of services and methods. The development of the hardware design followed a traditional, structured decomposition approach. Table 3 summarizes the ERA System design process:

Table 3 – Summary of ERA System Design Process

Task and Objective	Steps	Products
Task: Define Software Design **Objective:** Develop and describe software components for implementation	• Determine sub-package services, methods, inputs and outputs • Allocate requirements to services • Validate services/methods, interfaces and data	• ERA System-Level Packages[1] Service Description Tables • ERA Security Design • ERA System Operations Design • Sequence Diagrams • SyRS to Services Traceability Matrix • ERA System Data Models
Task: Define Hardware and Network Design **Objective:** Develop and describe hardware components for implementation	• Identify hardware component types • Allocate requirements to hardware components • Validate hardware components, configuration and interfaces	• ERA System Hardware Diagrams • ERA System Network Diagrams • ERA System Performance and Availability Models

1.6.1.3 Benefits

As mentioned earlier, combining a structured analysis methodology for the system architecture with an object-oriented methodology for the system design balances the benefits of a more compact and abstract functional view with the more voluminous and concrete object view. The benefits of this approach include:

Structured Analysis → Succinct ERA System Architecture

- Supports verification of system architecture at the conceptual level prior to delving into low-level details
- Supports discussions with a wide range of ERA stakeholders, including personnel more familiar with the ERA System business domain than with systems engineering notations

[1] A *package* is a grouping construct that allows one to take any construct in the UML and group its elements into higher-level units.

- Supports performance and availability modeling efforts
- Supports system-level test and integration planning
- Identifies and segregates persistent data (avoiding the inflexible inheritance issues of an object-oriented approach)
- Shows "state" concepts for complex interactions

Object-Oriented ⟶ Detailed ERA System Design

- Supports translation into the Service Oriented Architecture (SOA) model
- Allows loose coupling of design concepts and allows objects to be related to business activities
- Supports flexibility of the software design
- Leverages object-oriented design tool to ensure consistency of services and the data model

1.6.2 Software Modeling Elements

The ERA System architecture and design leverage standard functional structured analysis with refinements from UML to capture the service-oriented nature of the solution. Table 4 summarizes the modeling elements used in the LM Team's architecture and design processes, explains each element, provides the comparable structured analysis element for those more familiar with this approach and terminology, and points to the SADD section and associated architectural/design artifact using this element.

Table 4 – Summary of LM Software Design Elements

SADD Model Element	Purpose	Structural Equivalent	Document Section and Artifact
System-Level Package	System-level packages conceptually divide the system's function into manageable and cohesive pieces.	System Segment	Section 2.8 Functional flow diagrams illustrate the system-level packages.
Sub-Package	System-level packages can contain sub-packages, which further conceptually divide the system's function.	Configuration Item	Sections 2.8.4 - 2.8.11 Functional flow diagrams illustrate the sub-packages.
Service	Services provide the system function.	Computer Software Unit	Software Design Specifications
Method	Each service has one or more cohesive methods. Each method has inputs (parameters), outputs (results), and performs discrete processing.	Function	Software Design Specifications

SADD Model Element	Purpose	Structural Equivalent	Document Section and Artifact
Orchestration	Orchestrations invoke service methods in a specific order, based on a defined business process.	System Thread	Software Design Specifications
Data Class	Data classes represent persistent objects on which methods operate. All method inputs and outputs are modeled as Data Classes in the ERA Domain Model. Data Classes also represent the data exchanged with external interfaces.	Entity Relationship Diagram	Section 2.11 UML class diagrams illustrate the data classes.
Composite Application	A Composite Application comprises of portlets, the processes, and the requisite business logic that provides users with a complete set of business functions.	Front-end application with backend middleware	Section 2.7.3

This page is intentionally left blank.

2. SYSTEM ARCHITECTURE

2.1 System Purpose

The "ERA Requirements Document" (RD) describes the ERA System's purpose as:

> NARA ensures, for the citizen and all branches of the Government, ready access to essential evidence that documents the rights of citizens, the actions of Federal officials, and the national experience. The purpose of the ERA System is to enable NARA to realize its strategic vision: "ERA will authentically preserve and provide access to any kind of electronic record, free from dependence on any specific hardware or software, enabling NARA to carry out its mission into the future."
>
> Increasingly, this "essential evidence" takes the form of electronic records. Traditional methods of transfer, preservation, and access are not applicable to electronic records. Electronic records pose unique archival difficulties, including ease of deletion and the risk that advancing technology will render records and operating systems obsolete in a short period of time, making the records inaccessible. Compounding the problem is the diversity, complexity, and enormous volume of electronic records being generated, and the rapidly changing nature of the systems that are used to create them.
>
> The ERA solution must be dynamic (capable of responding to continuing change) and sound, ensuring that electronic records delivered to future generations of Americans are authentic decades in the future, as they were when first created.[2]

Thus, the ERA System serves two complementary purposes: 1) to provide services that enable NARA to carry out its mission to provide ready access to essential evidence; and 2) to authentically preserve and provide access to any kind of electronic record.

2.2 System Scope

The following statements define the ERA System scope at the broadest level:

- The ERA System will interface to external system classes as described within the external system context
- The ERA System will store and manage electronic records
- The ERA System will coordinate life cycle management transactions (such as appraisal, disposition agreements, transfers, accessions) for all records
- The ERA System will dispose of electronic records as stipulated by disposition agreements
- The ERA System will provide the capability to create, store, and search descriptions for all records
- The ERA System will authentically preserve any kind of electronic record

[2] ERA RFP# NAMA-03-R-0018, Section J-2, Amendment 001, p. J2-1

- The ERA System will provide the capability to create, store, and search arrangements for electronic records
- The ERA System will have the capability to provide products and/or services to users for a fee
- The ERA System will support collaboration between users
- The ERA System will have the capability to present and/or output all records, while enforcing appropriate access and release restrictions
- The ERA System will store both assets and electronic records that are unclassified, sensitive, and classified through Top Secret/Sensitive Compartmented Information (SCI)
- The ERA System will operate within the context of the Federal Enterprise Architecture and the NARA Enterprise Architecture

The following summarizes the functions that are outside the ERA System scope:

- The ERA System will interface to Financial Systems where financial transactions are processed
- The ERA System will interface with Non-Electronic Records Tracking Systems that track non-electronic records archival processing or location, e.g., movement of boxes, shelving, re-filing
- The ERA System will interface with Help Desk Systems that provide help desk support for systems other than the ERA System
- The ERA System will interface with Transferring Entity Systems that manage the Transferring Entities' records and records life cycle transactions prior to the transfer of these records to the ERA System
- While the ERA System will not convert non-electronic records, the ERA System will have the capability to ingest transferred electronic records converted from non-electronic formats

2.3 System Overview

This section provides an overall set of information to represent the system view of ERA as the program matures based on increments up to its Full Operational Capability (FOC). To address this need, we start by providing system context based on the NARA Enterprise Architecture. We introduce key infrastructure concepts needed to describe the system and provide the overall System Functional Architecture. This section provides the reader with the concept of system evolution based on codifed ERA System requirements. The progression of ERA requirements implemented based on Increments 1 through 5 is tracked based on the development life cycle. The next topic deals with ERA interfaces to external systems and its coordination with financial systems; record tracking systems, help desk systems and transferring entities.

2.3.1 Enterprise Architecture Context

The ERA System architecture is predicated on the Federal Enterprise Architecture Framework (FEAF) and the NARA Enterprise Architecture (EA). It follows guidance from the Federal CIO Council, Federal

Enterprise Architecture Program Management Office, the Industry Advisory Council Enterprise Architecture Shared Interest Group (SIG) and Service Component-Based Architectures. Figure 1 maps the NARA EA views to the ERA System architecture.

Figure 1 – NARA EA Views Mapped to ERA Service-Based Implementation

ERA_ENG_001b

Section 2.3.1.1 discusses the ERA System performance goals and the LM Team's approach to meeting these goals. Section 2.3.1.2 discusses how the ERA System supports NARA business goals. Section 2.7.1 presents the ERA Service view.

2.3.1.1 Performance View

ERA System-specific performance measures derive from the NARA ERA Performance Goal Specification (PGS), which is derived from NARA's Strategic Goals. The LM Team's ERA Service Oriented Architecture has been developed in the context of NARA's performance and business objectives as captured in the PGS and the RFP Section J Statement of Objectives (SOO). The LM Team has translated those objectives into a deployable solution that can successfully manage the predicted system loads, throughput, capacity, and service goals through a scalable, flexible, and evolvable architecture.

Using the metrics listed in the System Requirements Specification (SyRS) Tables 10-1, 10-2 and 10-3, the LM Team established the initial ERA System performance baseline. The LM Team analyzed the expected system loads in order to determine network bandwidth and storage requirements.

The LM Team will employ the LMTSS Technical Performance Measurement (TPM) methodology to assure continued success. The TPMs are product assessments that estimate, through engineering analyses, tests, and actual system performance, the values of essential performance parameters. TPMs are used to forecast the values to be achieved through planned project efforts, which are the values of essential performance parameters.

Using TPMs, the LM Team will also employ system models to drive the ERA System's evolution. The first step is the establishment of a baseline set of models that directly relate to the design. These models include the corresponding scalability of Instances, intra-site communications, expected receipt and transmission volumes of records, and other critical characteristics affecting system and enterprise-solution performance. The LM Performance Measurement Specification captures the initial baseline TPMs.

2.3.1.2 Business View

NARA Enterprise Architecture business imperatives[3] drive the ERA System goals:

- **NARA Business Imperative:** NARA must be able to accept, authenticate, store, preserve, and manage Federal, Congressional, Presidential, and other government records and donated material regardless of their form.
  - **ERA System Goal:** The ERA System will enable NARA to accept, authenticate, store, preserve, and manage Federal, Congressional, Presidential, and other government electronic records and donated electronic records. ERA will support processes for non-electronic records.
- **NARA Business Imperative:** Within the constraints of security and privacy, NARA must be able to provide access to the electronic records it keeps to the public, regardless of geographical location of the records.
  - **ERA System Goal:** The ERA System will provide access via a Web browser and the public Internet for Unclassified and Sensitive But Unclassified (U/SBU) records.
- **NARA Business Imperative:** Access must be standardized, secure, reliable, and protect the privacy of information in the records in NARA's custody.
  - **ERA System Goal:** The ERA System will ensure identity, integrity, confidentiality, and non-repudiation.
- **NARA Business Imperative:** NARA must improve its working relationships with all agency customers, and NARA must continue to participate in cross-agency service delivery within the context of strategic Federal E-Government initiatives as prescribed by the FEA.
  - **ERA System Goal:** The ERA System will provide tools so that NARA can work collaboratively with other government agencies.

The ERA System software architecture is comprised of seven (7) system-level packages. Together, these packages meet the Archival Records Services business needs of NARA (see Table 5). Figure 2 summarizes the ERA System business services.

[3] NARA Enterprise Architecture Overview, Version 3.2, pg 4-5

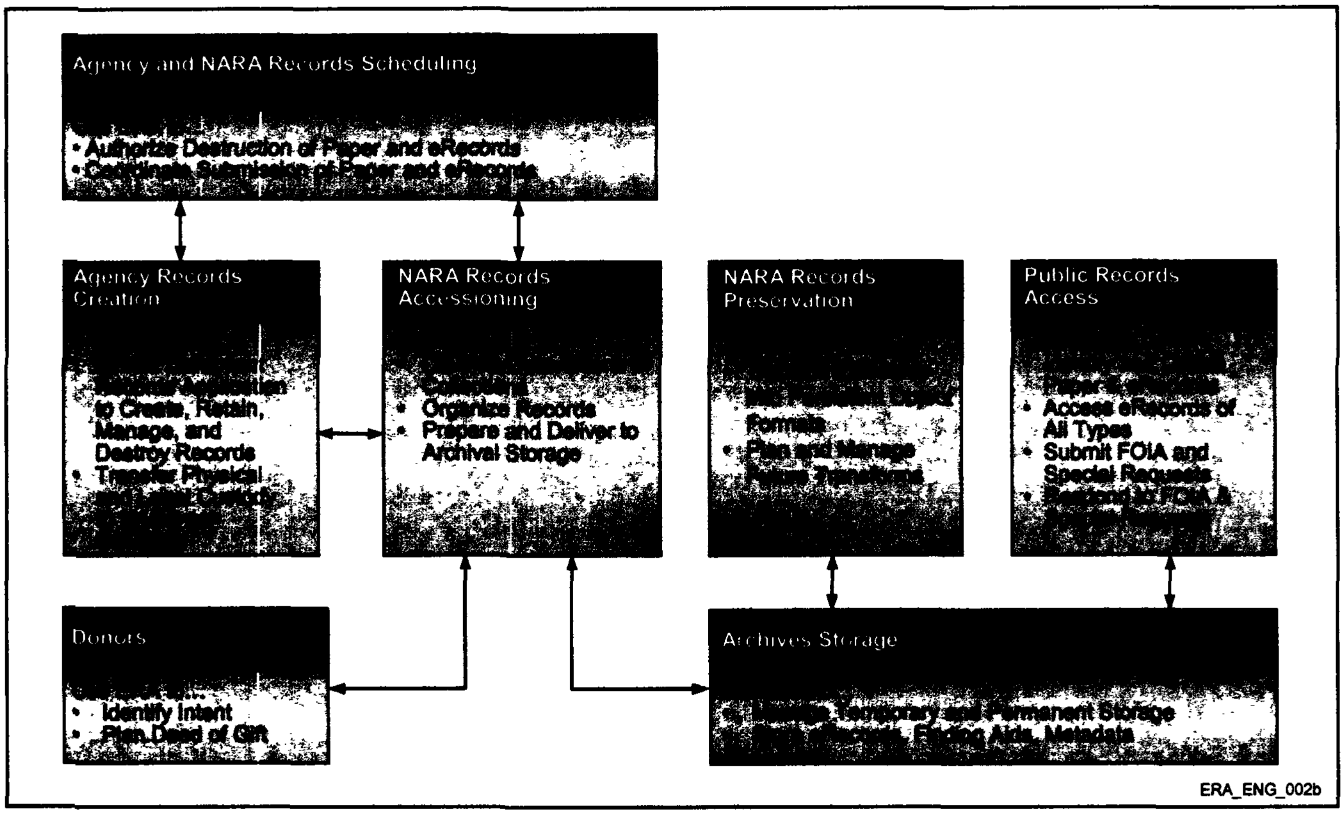
Table 5 – ERA System-Level Packages Derived from NARA Business Functions

	ERA System-Level Packages[4]						
Archival Records Services[5]	**Ingest**	**Records Mgmt**	**Preservation**	**Archival Storage**	**Dissemination**	**LS&C**	**ERA Mgmt**
Federal Agency and Presidential Records Management	X	X	X	X	X		
Appraisal		X	X				
Implementation of Disposition		X	X	X			
Acquisition of Donated Historical Materials	X	X	X	X	X		
Documentary Materials Storage		X		X			
Accession	X	X		X			
Process		X	X	X	X	X	X
Preservation			X	X			
Access				X	X		
Public Programs					X		

[4] The ERA system-level packages are described in Section 2.8.

[5] NARA business functions from the NARA Enterprise Architecture

Figure 2 – ERA System Business Services


Agency and NARA Records Scheduling
• Authorize Destruction of Paper and eRecords
• Coordinate Submission of Paper and eRecords
Agency Records Creation
to Create, Retain, Manage, and Destroy Records
• Transfer Physical
NARA Records Accessioning
• Organize Records
• Prepare and Deliver to Archival Storage
NARA Records Preservation
Formats
• Plan and Manage
Public Records Access
• Access eRecords of All Types
• Submit FOIA and Special Requests
• Respond to FOIA &
Donors
• Identify Intent
• Plan Deed of Gift
Archives Storage
Temporary and Permanent Storage
Finding Aids, Metadata
ERA_ENG_002b

2.3.2 Infrastructure Concepts

The following section defines overall infrastructure concepts that are key to the ERA System.

2.3.2.1 Instances

The LM Team's architecture is centered on the concept of an Instance. Each Instance provides a fully functioning self-contained archives system. From a physical viewpoint, Instances can be independently deployed to any number of Facilities, and any Facility may contain multiple Instances.

The software and hardware physically deployed to each Instance can be scaled to meet the Instance's particular profile by:

- Omitting one or more system-level packages (e.g., Ingest) entirely
- Scaling the processing resources provisioned to execute a particular service
- Scaling the storage resources allocated to the Instance

Regardless of scaling, each Instance is deployed with the same configuration-managed software baseline; the architecture does not require custom software configurations for specific Instances or Facilities, other than normal site configuration information (e.g., IP address).

2.3.2.2 Federations

The LM Team's architecture allows for the deployment of multiple Instances to multiple Facilities of any size and any data classification. To meet NARA's requirements for a national archive, these Instances may be *federated* through a Wide Area Network (WAN).

A Federation is a collection of Instances at the same security classification level and compartment that can communicate electronically via a WAN with one another. ERA System services ensure that federated Instances appear and operate as one cohesive archive. In other words, the particular Instance within a Federation that satisfies a request is completely transparent to the user (or external system).

Federations are collected together for system management purposes, and a representative depiction of the ERA Federation of Instances is illustrated in Figure 4 – ERA Federation of Instances.

2.3.2.3 ERA Management

Each collection of Federations has a primary and a backup ERA Management system-level package, which provides the hardware/software for monitoring and management services for the collection of Federations. The ERA Management network will typically be physically separate from the Federation network and will be installed at a Systems Operations Center (SOC).

2.3.2.4 Facilities

A Facility is a physical location. A Facility can contain one to many Instances, zero to many SOCs, and zero to many Secure Compartmented Information Facilities (SCIFs). Inventory management services track inventory levels at facilities.

The final configuration of Facilities and Instances will be determined by balancing total cost of ownership, security access, and NARA policy and guidelines.

2.3.2.5 System Operations Center (SOC)

The SOC provides ERA System support by providing ERA Management functionality such as centralized monitoring and management services. Another primary function of the SOC is to communicate with the development Facility to receive software releases and distribute them to the ERA Instances. To provide high availability and reliability, there is one SOC and one backup SOC for each security classification level. The backup SOC is physically located at a remote Facility to ensure availability in the event an Instance loses the connection to the primary SOC location.

All U/SBU ERA Management functionality can be accessed remotely via the public network infrastructure (assuming proper security authorization is granted), providing a great deal of deployment flexibility. The physical configuration follows the safeguards and procedures required by the classification level it manages.

The ERA System physical architecture leverages the same security and network infrastructure stack, cluster server hardware and software, and working storage devices as archival Instances. The SOC, like the Instances, is also configured with redundant hardware to guarantee accessibility in the event of a system failure. Additional bandwidth, processors or servers can be added to accommodate future growth, if required.

2.3.2.6 Secure Compartmented Information Facility (SCIF)

A SCIF is a facility that complies with a set of physical security standards governing the construction and protection of facilities for storing, processing and discussing SCI that requires extraordinary security safeguards. The SCIF security requirements are specified in DCID 6/9. LM is not responsible for the facility. NARA will provide one for the SCI federations, if LM is to be accredited.

2.3.3 System Functional Architecture

This section presents the overall functional architecture of the ERA System. This set of information and representative diagrams provide a high-level system interface description that depicts the first-level of system processes. This first level of decomposition presents system-level packages, external interfaces, data flows, and major data stores. The next level of detail for each system process is separately presented within Section 2.8, which is labeled as System Functional Design. This section provides more detail as to how the ERA System addresses the operational concepts from the archival life cycle and implements it within the ERA System.

Figure 3 provides an illustration of the ERA System Functional Architecture from a notional perspective that delineates all of the system-level packages and external system entities.

descriptions, and arrangements. In addition, access review, redaction, selected archival management tasks for non-electronic records, such as the scheduling and appraisal functions are also included within the Records Management service.

- Preservation – This system-level package includes the services necessary to manage the preservation of the electronic records to ensure their continued existence, accessibility, and authenticity over time. The Preservation system-level service also provides the management functionality for preservation assessments, Preservation and Service Level plans, authenticity assessment and digital adaptation of electronic records.
- Archival Storage – This system-level package includes the functionality to abstract the details of mass storage from the rest of the system. This abstraction allows this service to be appropriately scaled as well as allow new technology to be introduced independent of the other system-level services according to NARA's business requirements.
- Dissemination – This system-level package includes the functionality to manage search and access requests for assets within the ERA System. Users have the capability to generate search criteria, execute searches, view search results and select assets for output or presentation. The architecture provides a framework to enable the use of multiple search engines offering a rich choice of searching capabilities across assets and their contents.
- Local Services and Control (LS&C) – This system-level package includes the functional infrastructure for the ERA Instance including a user interface portal, user workflow, security services, external interfaces to NARA and other Government systems as well as the interfaces between ERA Instances.

Note that all external interfaces are depicted as flowing through LS&C.

The ERA System contains a centralized monitoring and management capability called ERA Management. The ERA Management H/W and S/W are located at an ERA site. The Systems Operations Center (SOC) provides the system and security administrators with access to the ERA management Virtual Local Area Network. Each SOC manages one or more Federations of Instances based on the classification of the information contained in the Federation. The ERA Management system-level service provides ERA Help Desk functionality, Configuration Management (CM), security services, and administration of a Federation of Instances.

The ERA System interfaces to various external systems through a series of standard interfaces. These standard interfaces are listed below:

- Financial Systems
- Non-Electronic Records Tracking Systems
- Transferring Entity Systems
- NARANET
- Help Desk
- Public User Interface

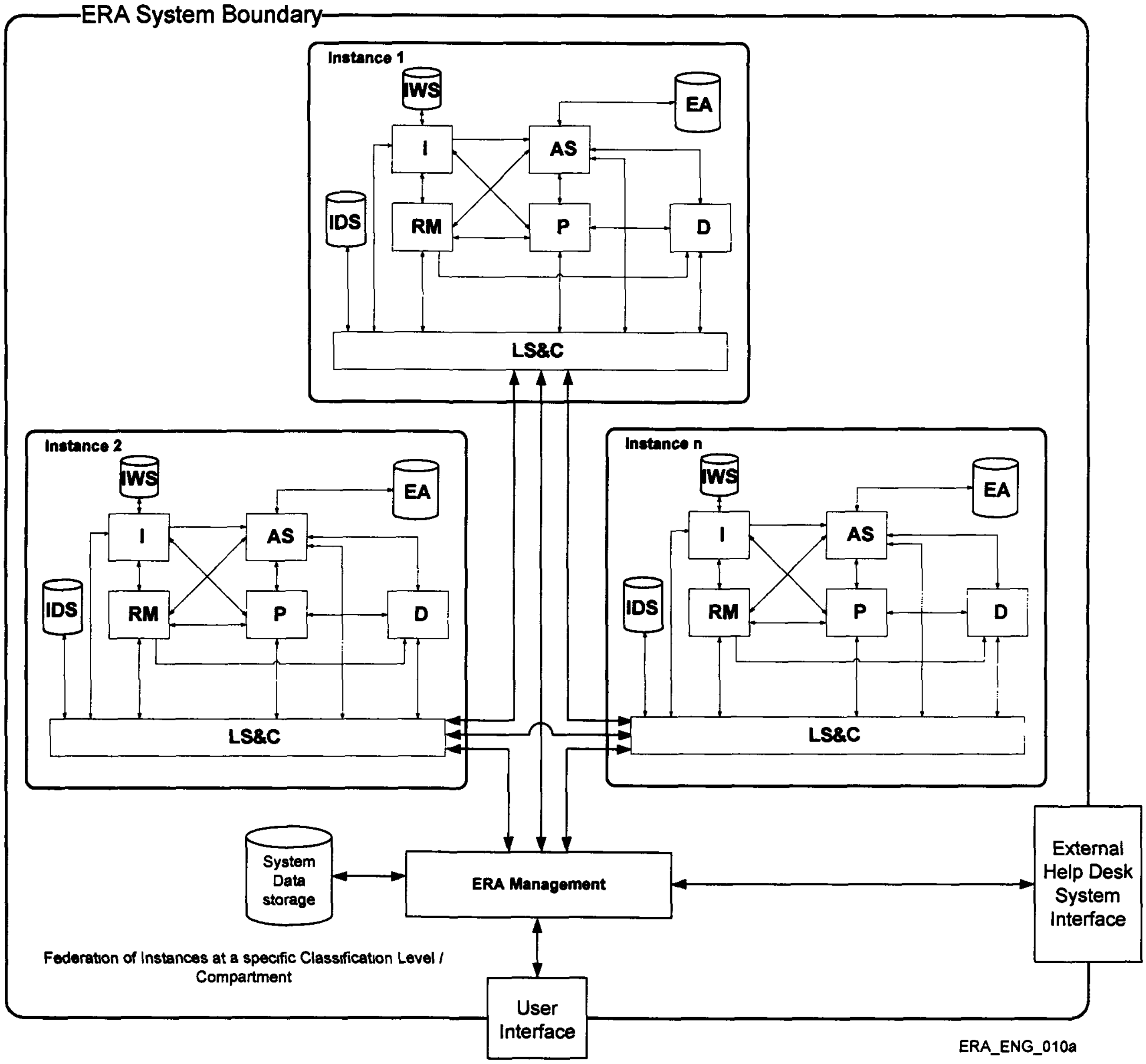
Also shown are the three primary data stores for each Instance:

1. **Ingest Working Storage** - Contains transfers that remain until they are verified and placed into the Electronic Archives
2. **Electronic Archives** - Contains all assets (i.e., disposition agreements, records, templates, descriptions, authority sources, arrangements, etc.)

3. **Instance Data Storage** - Contains a performance cache of all business assets, operational data and the ERA asset catalog

This diagram provides a representative illustration of how a federated ERA System can be put together. The diagram describes a collection of Instances at the same security classification level and compartment that can communicate electronically via a WAN with one another.

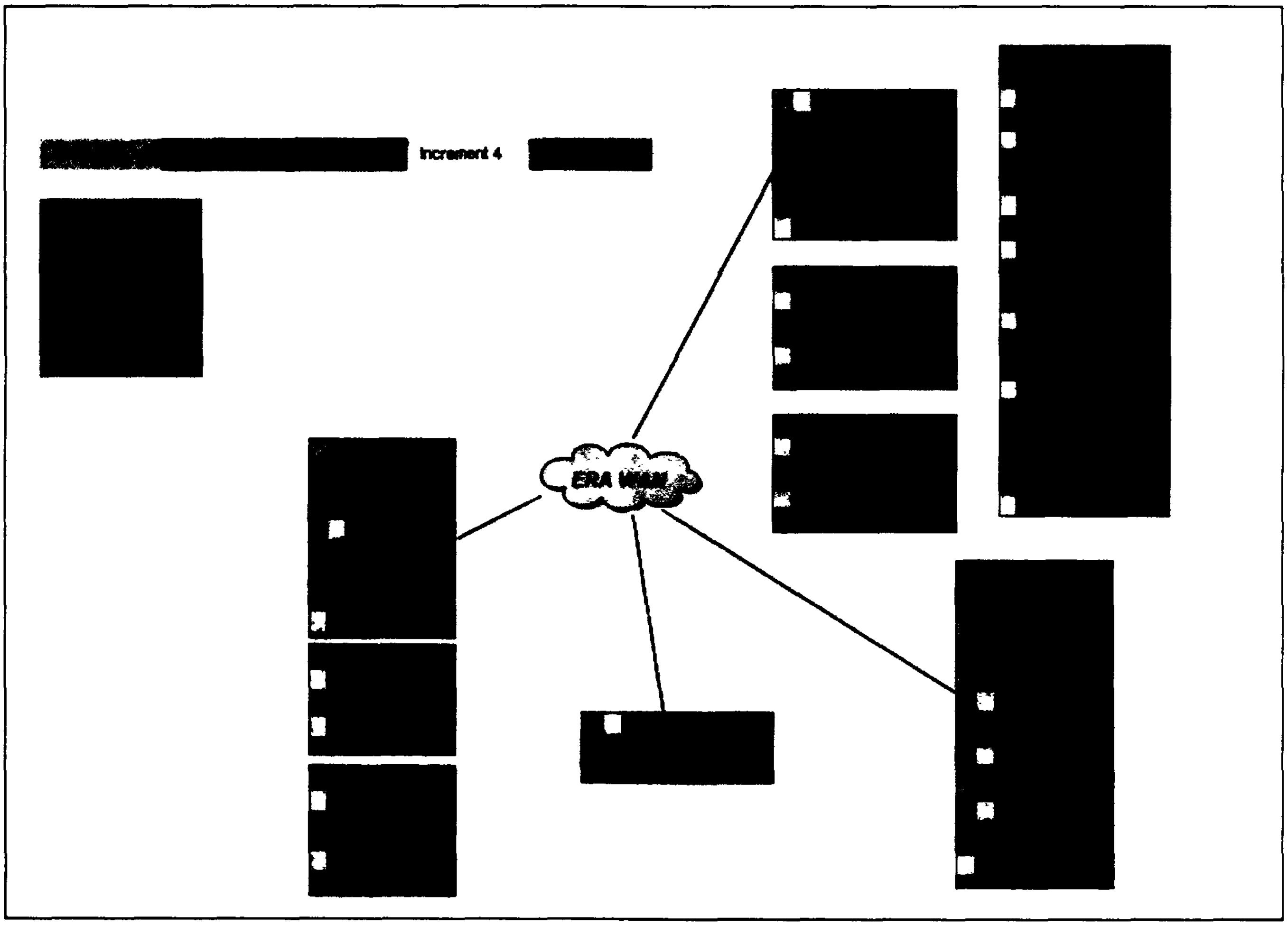
Figure 4 – ERA Federation of Instances



The next illustration presents the baseline facilities implementation that takes into account the level of security compartmentalization that is necessary as the ERA System is deployed to Full Operational

Capability. Figure 5 presents the current understanding of ERA Instances based on the latest ERA Increment 2 through 5 Lockheed Martin baseline proposal to NARA. It provides facility choices at two different facilities: Rocket Center, West Virginia and Stennis MSRC, Mississippi. It provides the growth of Unclassified/Sensitive But Unclassified (U/SBU) Instances as is necessary for Increments 2 through 6. A number of lab facilities have been identified that includes: customer acceptance test lab, system integration test lab, software integration test lab, and development lab. Instances with higher classification have also been identified that includes air-gapped secret, top-secret and SCI Instances. This baseline configuration of ERA System Instances may change over time, however, the intent for archives deployment will remain the same.

Figure 5 - ERA System Instances at Full Operational Capability



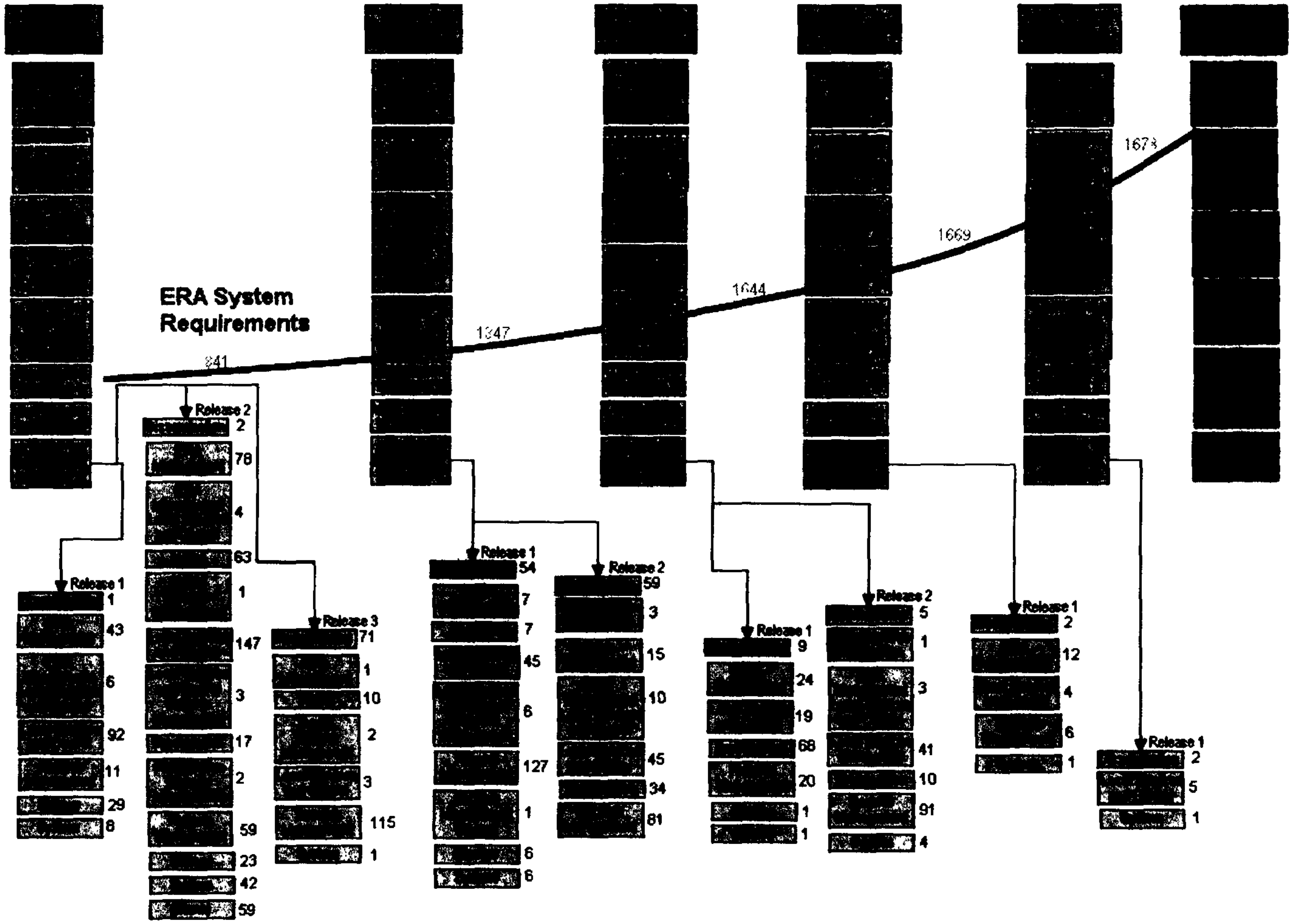
[redacted]

2.3.4 Progression of ERA System Requirements

This section provides the reader with a pictorial view as to how ERA System requirements are being added based on Increments, and how the system grows as a result of them. Figure 6 provides progression of A-Level system requirements and how these requirements have been allocated based on Increments.

The ERA System functional architecture in Figure 3 provides each of the high-level functions performed by the ERA System. This denotes the six system level packages within the ERA System Boundary. Figure 6 characterizes A-Level requirements based on the six system level packages and provides requirements totals that have been allocated to increments and releases. This allocation is also useful from the perspective of work breakdown structure from the ERA Program perspective.

Figure 6 – Progression of System Requirements



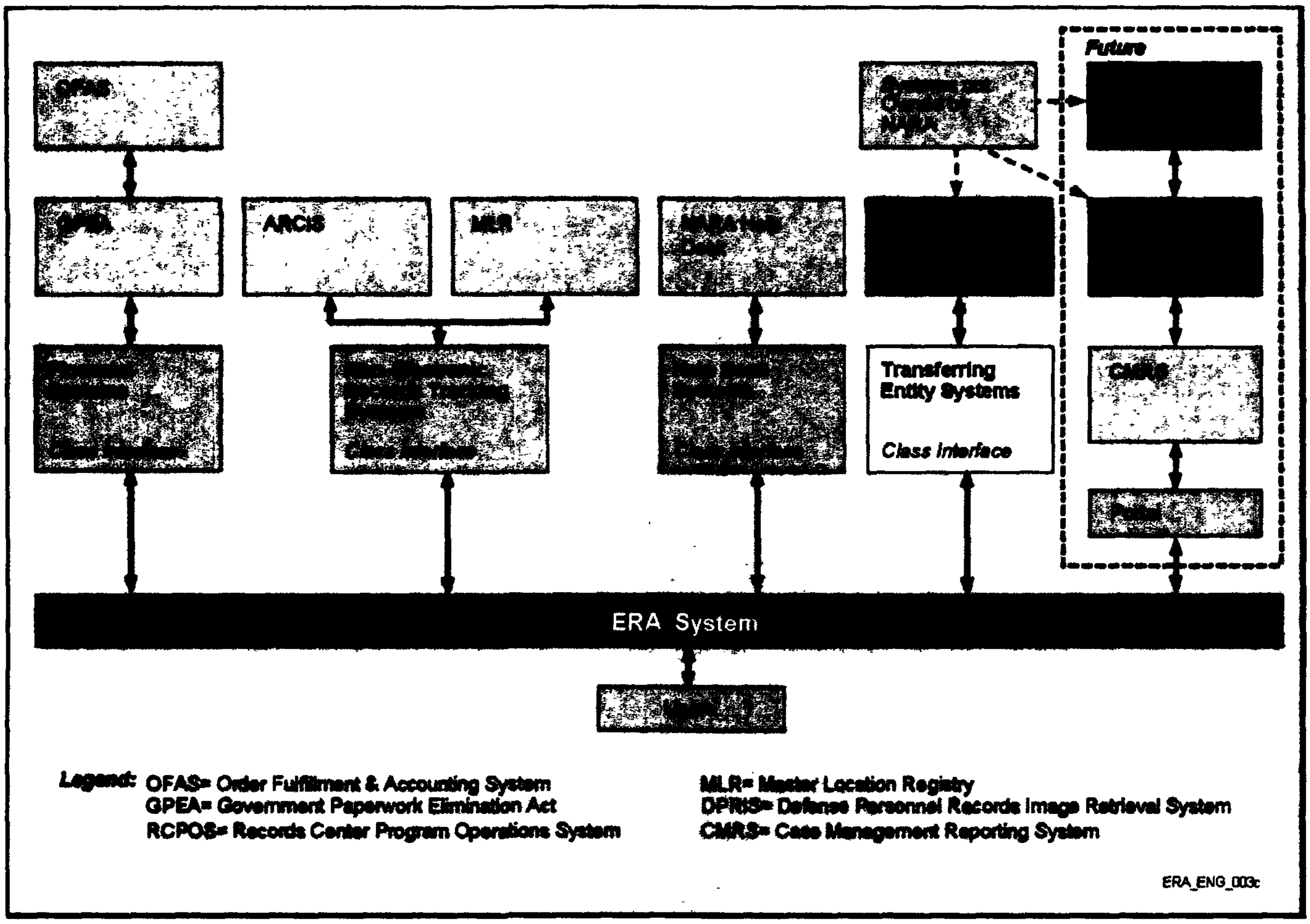
2.3.5 Interfaces to External Systems

The ERA System must interface with certain types (or classes) of external systems. The systems fall outside the ERA System Boundary. The systems to be interfacing the ERA System were primarily designed as stand-alone, single purpose, self-contained applications and may not easily and efficiently support interfacing with the ERA System. ERA Increment 1 is currently coordinating with NARA organizations to identify legacy systems and systems that will interface with the ERA System. At this time, several of the existing external systems are being considered for redesign, replacement by other systems, or combination with other systems prior to ERA Initial Operating Capability (IOC).

Based on the characterization that there will be near-term volatility in the interfacing of external systems to the ERA System, the ERA PMO has defined generic, abstract classes of external systems. The ERA System will interface to these abstract interface classes, rather than to specific external systems directly. Similarly, external systems will interface to the abstract interface classes, rather than to the ERA System directly. By decoupling the ERA System from direct external system interfaces, the external system owners gain the freedom to change their systems independently from the ERA System, as long as they adhere to the abstract interface class contract.

Figure 7 illustrates the four different types of external system interfaces, and their relationship to the ERA System.

Figure 7 – ERA System External Interfaces


Future
OFAS
GPEA
ARCIS
MLR
Transferring Entity Systems
Class Interface
CMRS
ERA System
Legend: OFAS= Order Fulfilment & Accounting System
GPEA= Government Paperwork Elimination Act
RCPOS= Records Center Program Operations System
MLR= Master Location Registry
DPRIS= Defense Personnel Records Image Retrieval System
CMRS= Case Management Reporting System
ERA_ENG_003c

The four abstract classes of external systems are:

- **Financial Systems:** The ERA System will have the capability to provide products and/or services to users for a fee, which will require a financial transaction. The ERA System will interface with external financial systems (such as GPEA) to provide this capability;
- **Non-Electronic Records Tracking Systems:** The ERA System will coordinate life cycle management transactions (such as appraisal, disposition agreements, transfers, accessions) for all records, including non-electronic records. The ERA System will interface with external systems (such as RCPOS and MLR) to track the location and disposition non-electronic records, to provide disposition instructions to these systems, and to confirm that the instructions have been implemented;
- **Help Desk Systems:** The ERA System will provide help desk support for problems within its system scope. The ERA System will interface to help desks for external systems (e.g., the NARA Help Desk) outside its scope to exchange and track help desk tickets; and

- **Transferring Entity Systems:** The ERA System will provide the capability to transfer records and records life cycle information from external systems. The ERA System will interface with Transferring Entity systems to provide this capability.

The ERA System will provide:

- Security functions that protect the messages and data on the interface and verify that only appropriate external system connections are allowed
- Management of the availability of the system interface and ERA System service availability
- Enforcement of a message protocol that identifies the system providing the message and the destination, and vice versa
- Management of the performance and required resources of the interface and assurance that the external system will not interfere with the ERA System service response times specified in the ERA System Requirements Specification

There is another class of external systems: Administrative Reporting Systems. The ERA System will not need to interface directly with this class of system; instead, Administrative Reporting Systems will satisfy their requirements using the ERA System's reporting capabilities.

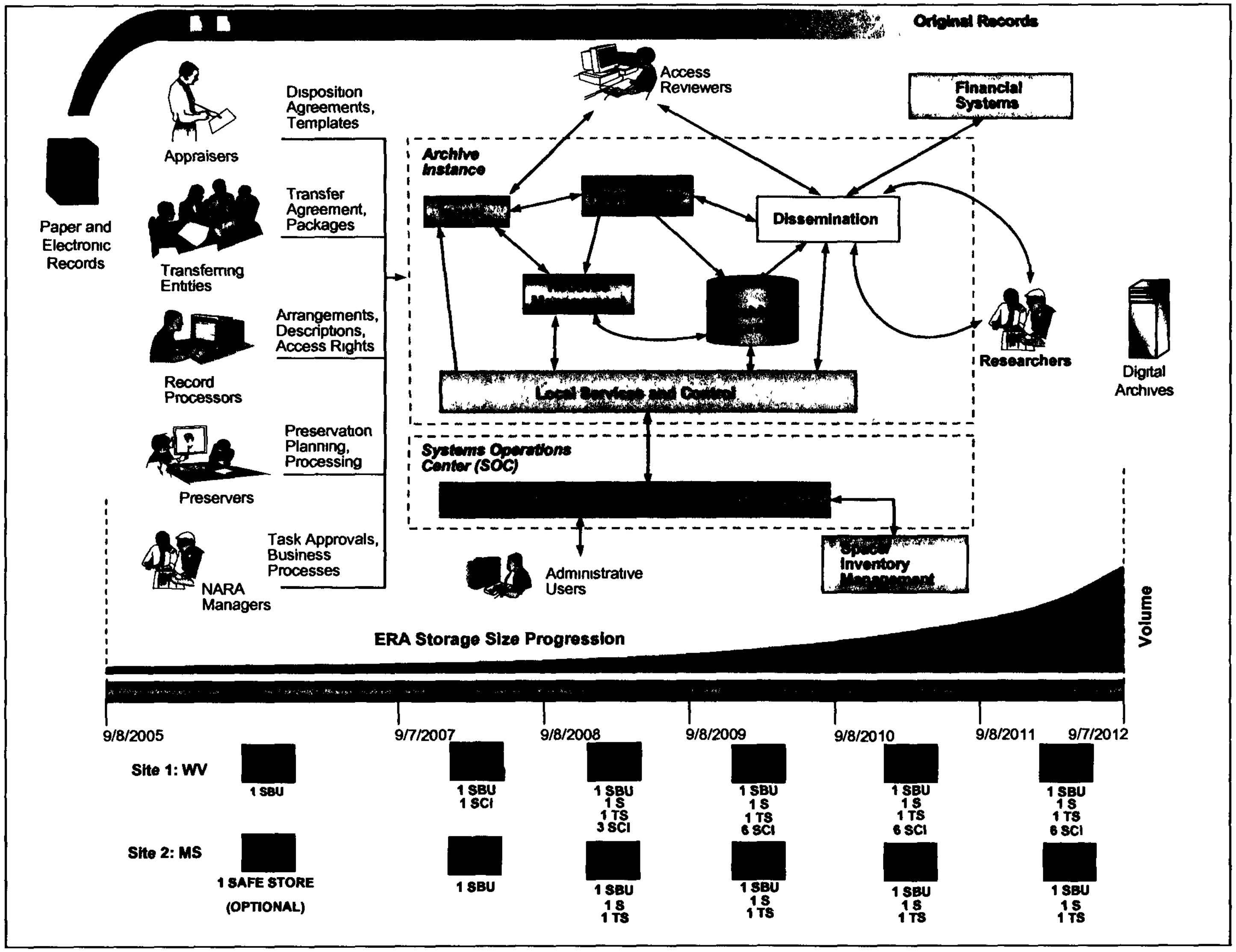
2.4 Operational Concept

This section provides a set of information that explains the operational concept of the overall ERA System. This includes a high-level depiction of the process, a set of examples of user level operations such as the use of workbenches, the use of a notional records life cycle, system support, test and training activities.

2.4.1 High-Level Operational Concept

This section provides an illustrated depiction of the ERA System shown in Figure 8 from the user and public's perspective. It denotes the ERA System operations, business workflow and the transition from human archival activities to automated system processes. The diagram also provides a pictorial understanding of the growth of the system over time through development increments until Full Operational Capability (FOC). The growth of overall storage necessary for the system is illustrated along with the configuration of facility Instances up till full operational capability. The Instance data storage is also pictorially depicted as the ERA System is deployed based on Options: Option 1, Option 2, Option 3, Option 4, Option 5, and Option 6.

Figure 8 - ERA High Level Operational Concept



2.4.2 User Level Operations

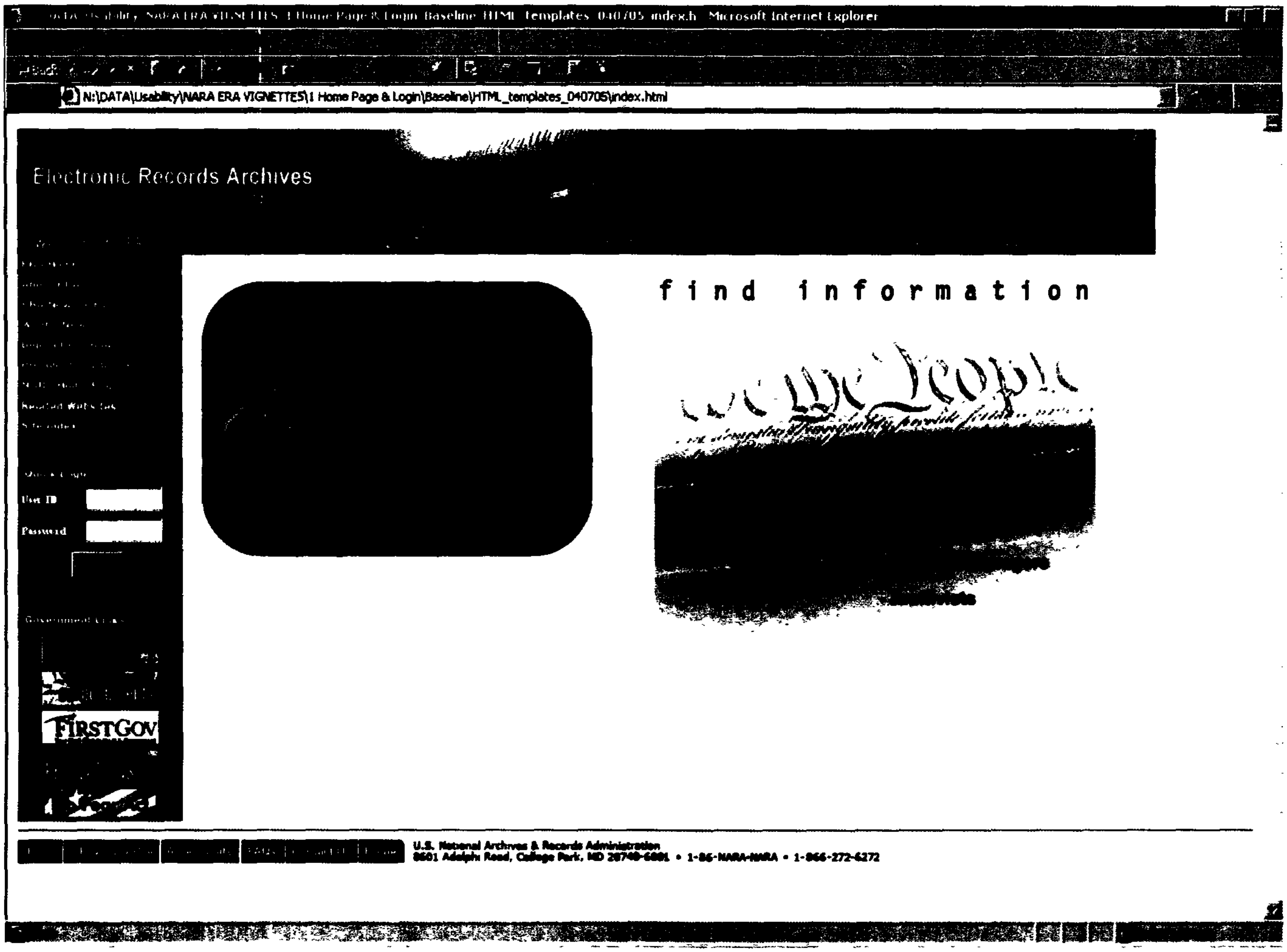
This section provides an example set of ERA System user level operations based on the current analysis and design stage of the ERA Program. This section provides an overview of the front-end application portal that includes web-based design, user registration, and business workflow components.

The ERA System intends to employ a web-based configurable "workbench" concept to provide its primary user-facing operational platform. Users log into the ERA System via a Web-based portal, and are presented with a configurable workbench that is tailored for the role(s) to which the user is authorized. The ERA System provides the capability to create user roles and to map business processes to these roles; a workbench provides users with access to the business processes their role or roles require. Workbench capabilities include user-interface components, workflow components, and other services required to complete specific operational tasks.

2.4.2.1 ERA Homepage

The "home page" for ERA is the general public user's webpage. It serves as the initial point of access to information and assets, and includes a link for registered users to login and access their role-based workbenches. Figure 9 shows an example homepage, which includes a variety of navigational methods (e.g., menus, text links, etc.), and a base set of public-facing tools. As the design of this default homepage matures, public-facing tools presented might include: general notices, news and events (see also Figure 10 – Example Informational Page), and "top 10" lists of popular collections or new releases.

Figure 9 – Example ERA Homepage



N:\DATA\Usability\NARA ERA VIGNETTES\1 Home Page & Login\Baseline\HTML_templates_040705\index.html

Electronic Records Archives

find information

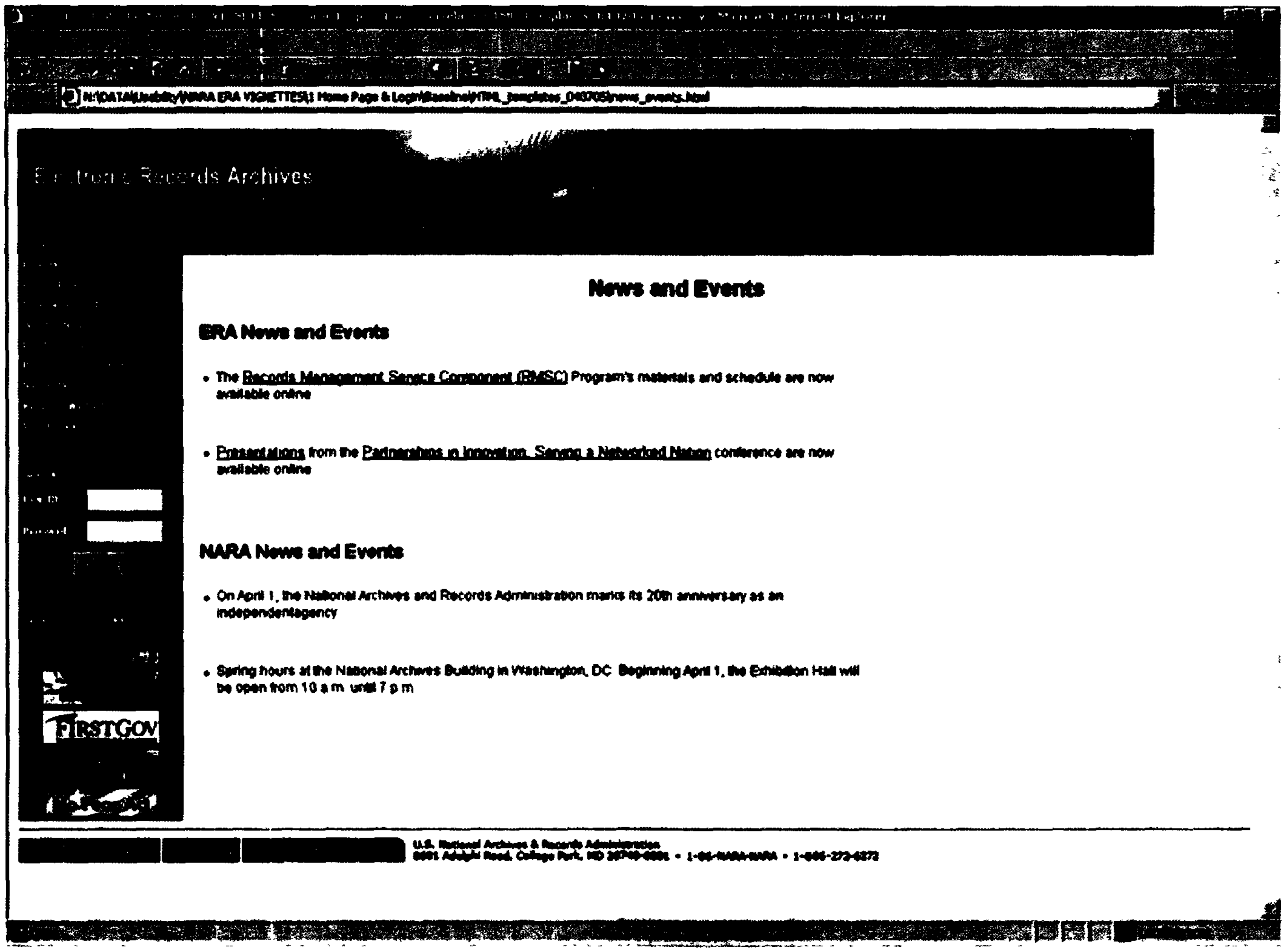
User ID

Password

U.S. National Archives & Records Administration
8601 Adelphi Road, College Park, MD 20740-6001 • 1-86-NARA-NARA • 1-866-272-6272

home.png

Figure 10 – Example Informational Page



N:\DATA\Usability\NARA ERA VIGNETTES\1 Home Page & Login\Baseline\HTML_templates_040705\news_events.html

Electronic Records Archives

News and Events

ERA News and Events

- The Records Management Service Component (RMSC) Program's materials and schedule are now available online
- Presentations from the Partnerships in Innovation, Serving a Networked Nation conference are now available online

NARA News and Events

- On April 1, the National Archives and Records Administration marks its 20th anniversary as an independentagency
- Spring hours at the National Archives Building in Washington, DC Beginning April 1, the Exhibition Hall will be open from 10 a.m. until 7 p.m.

U.S. National Archives & Records Administration
8601 Adelphi Road, College Park, MD 20740-6001 • 1-86-NARA-NARA • 1-866-272-6272

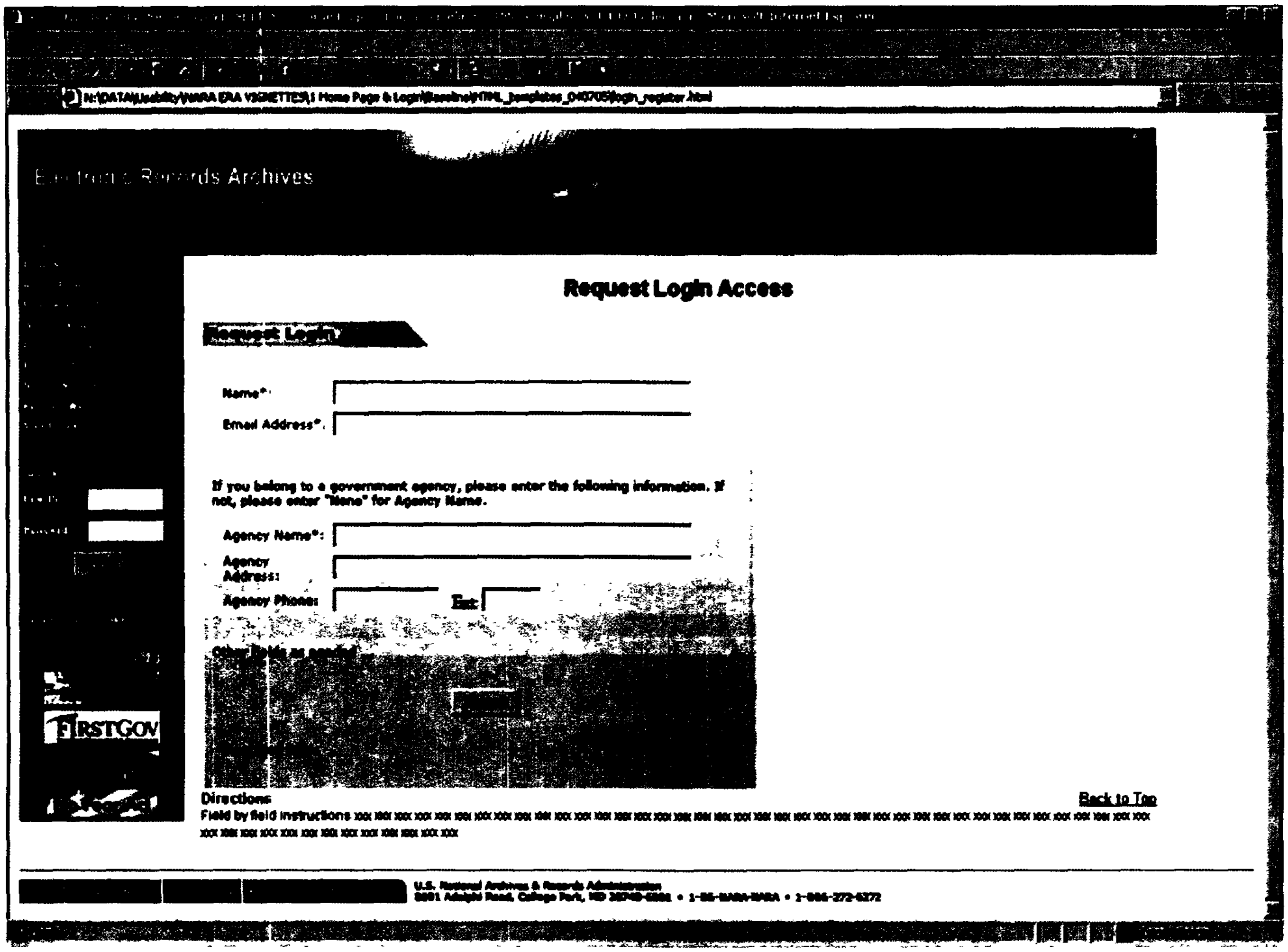
notices.png

2.4.2.2 User Registration and Login

Users can register and receive additional ERA capabilities. General public users will be able to subscribe to areas of interest, save searches, and customize their personal workbench. Government users from NARA, other Agencies, or approved entities (e.g., universities that NARA has relationship with) will be able to request additional access privileges. Approval of these access requests is delegated to community owners. For example, the Director of Records Management at an agency will approve or reject access requests to that agency's records management collaboration tools.

The Request Account, Request Access (Figure 11), and Login tools enable this functionality.

Figure 11 – Example User Registration Request Page



N:\DATA\Usability\NARA ERA VIGNETTES\1 Home Page & Login\Baseline\HTML_templates_040705\login_register.html

Electronic Records Archives

Request Login Access

Request Login

Name*:

Email Address*:

If you belong to a government agency, please enter the following information. If not, please enter "None" for Agency Name.

Agency Name*:

Agency Address:

Agency Phone: Ext:

Other fields as needed

Directions

Field by field instructions xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx xxx

Back to Top

U.S. National Archives & Records Administration
8601 Adelphi Road, College Park, MD 20740-6001 • 1-86-NARA-NARA • 1-866-272-6272

registration.png

2.4.2.3 Role Based Workbenches

The ERA portal is structured into a set of Workbenches. After logon, registered users are presented with their role-based workbenches. For example, the NARA manager of a team of archivists would see the archivist workbench and the NARA manager workbench, as well as the researcher workbench. General public researchers would only see the default workbench with researcher-focused tools, and would not have access to the other workbenches, or even to the tools (presented as portlets) that are not specific to their allowed workbench. The workbenches include tools and notices that are relevant to the user's role, and restrict users from access to functionality to which they are not authorized.

The user roles specified in the NARA Concept of Operations map to a baseline set of workbenches. Table 6 lists the related workbenches, and the major business processes supported within each workbench. Because the ERA System user interface is based on a portal framework, it is flexible and configurable - enabling the creation or modification of workbenches as the new roles are identified. That is, the portal architecture is extensible to the creation of additional workbenches, such as an Agency Records Manager.

Table 6 – Sample ERA System Workbenches

Sample Workbenches	Business Processes
Transferring Entity	Creates or receives records, and prepares and transfers records to NARA. This class of users primarily consists of records creators, but the name was chosen to indicate the predominate interaction with the system.
Appraiser	Assesses the records with respect to informational value, artifactual value, evidential value, associational value, administrative value, and monetary value and recommends which records should be accessioned into NARA's assets and which should be disposed of by the Transferring Entity when no longer needed by the Transferring Entity.
Records Processor	Manages transfers of records, identifies arrangements and creates archival descriptions of records, carries out other processes needed to ensure the availability of records, and is responsible for the disposal of temporary records.
Preserver	Plans the system approach for maintaining the authentic context, content, and structure of electronic records over time for viewing, use, and downloading. The preserver plans processing activities that ensure the ability to provide long-term access to electronic records through implementation of the Preservation and Service Level Plan.
Access Reviewer	Reviews security classified or otherwise potentially access restricted information to determine if the information can be made available to a consumer, facilitating redaction of potentially access restricted information in electronic records. The Access Reviewer reviews records in NARA custody and sets access restrictions.
Consumer	Uses the system to search for and access records, submit FOIA requests, request assistance via mediated searches, communicate with NARA, and invoke system services
Administrative User	Directly supports the overall operations and integrity of the ERA System and its use, and manages system activities such as determining user access rights, monitoring system performance, and scheduling reports.
NARA Manager	Reviews system recommendations and makes decisions on when and how specific records life cycle activities occur, and who will perform the work. The manager has ultimate responsibility for the completion of tasks and the quality of the products.

ERA_ENG_154a

2.4.2.4 Example Workbench

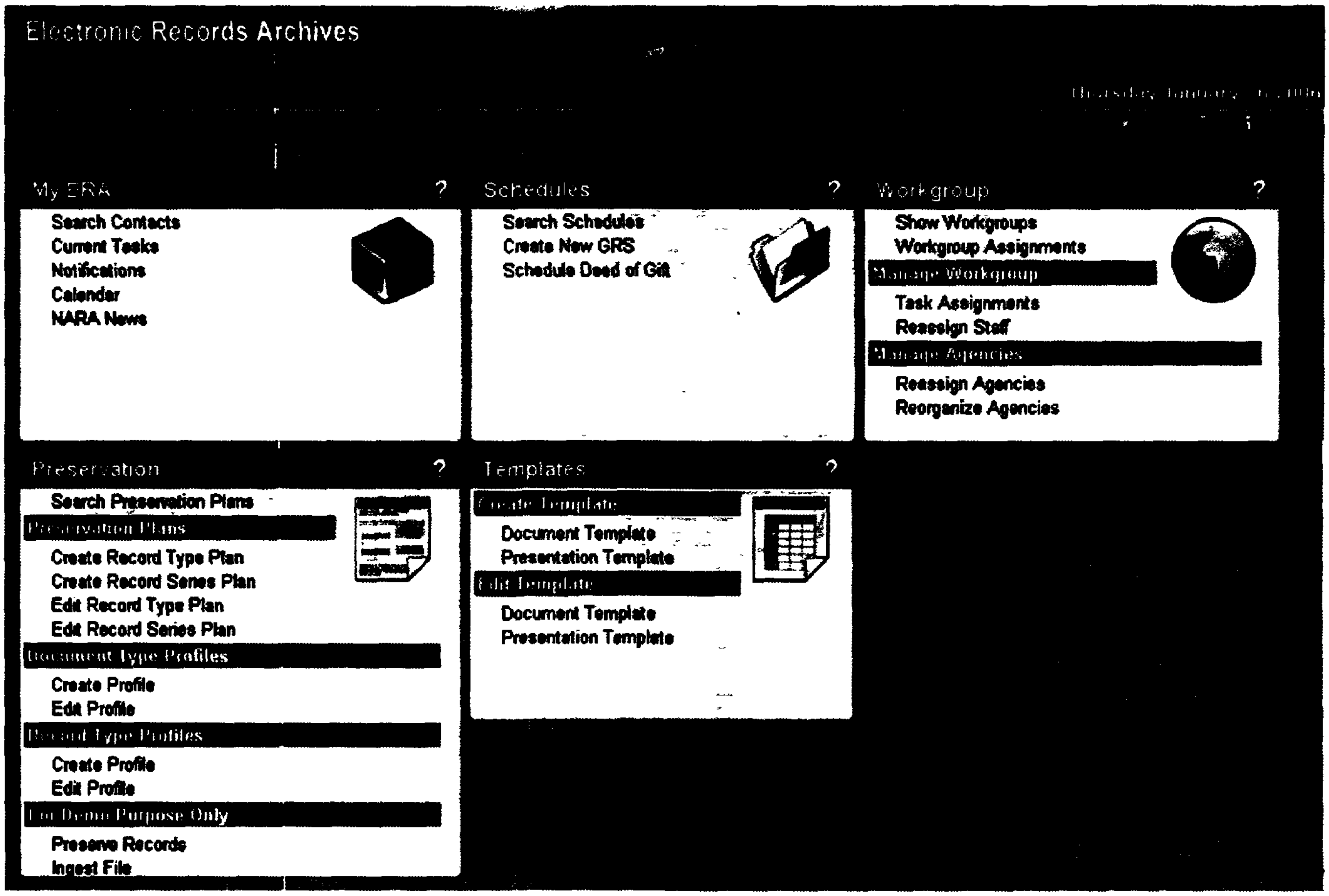
Figure 12 and Figure 13 provide examples of a role-based workbench. The layout of the workbench includes:

- Generic tabs, which provide access to general-purpose tools common to all workbenches.

- Workbench-specific tabs, which provide access to the many pages that might be included in a user's workbench. This would include tabs for all roles to which the user is authorized.
- Main body portlets, which provide the initial layer of business functionality. These portlets could include:
  - Links to specific tools (Figure 12)
  - User-specific tasks and notices (Figure 13)
  - Miniature Web forms for request submittal

To access a specific component of business functionality, the user selects the appropriate tab, and then clicks on the action within the portlet.

Figure 12 – Example NARA Manager Workbench



Electronic Records Archives

Thursday January [illegible]

My ERA ?

Search Contacts
Current Tasks
Notifications
Calendar
NARA News

Schedules ?

Search Schedules
Create New GRS
Schedule Deed of Gift

Workgroup ?

Show Workgroups
Workgroup Assignments

Manage Workgroup

Task Assignments
Reassign Staff

Manage Agencies

Reassign Agencies
Reorganize Agencies

Preservation ?

Search Preservation Plans

Preservation Plans

Create Record Type Plan
Create Record Series Plan
Edit Record Type Plan
Edit Record Series Plan

Document Type Profiles

Create Profile
Edit Profile

Record Type Profiles

Create Profile
Edit Profile

For Demo Purpose Only

Preserve Records
Ingest File

Templates ?

Create Template

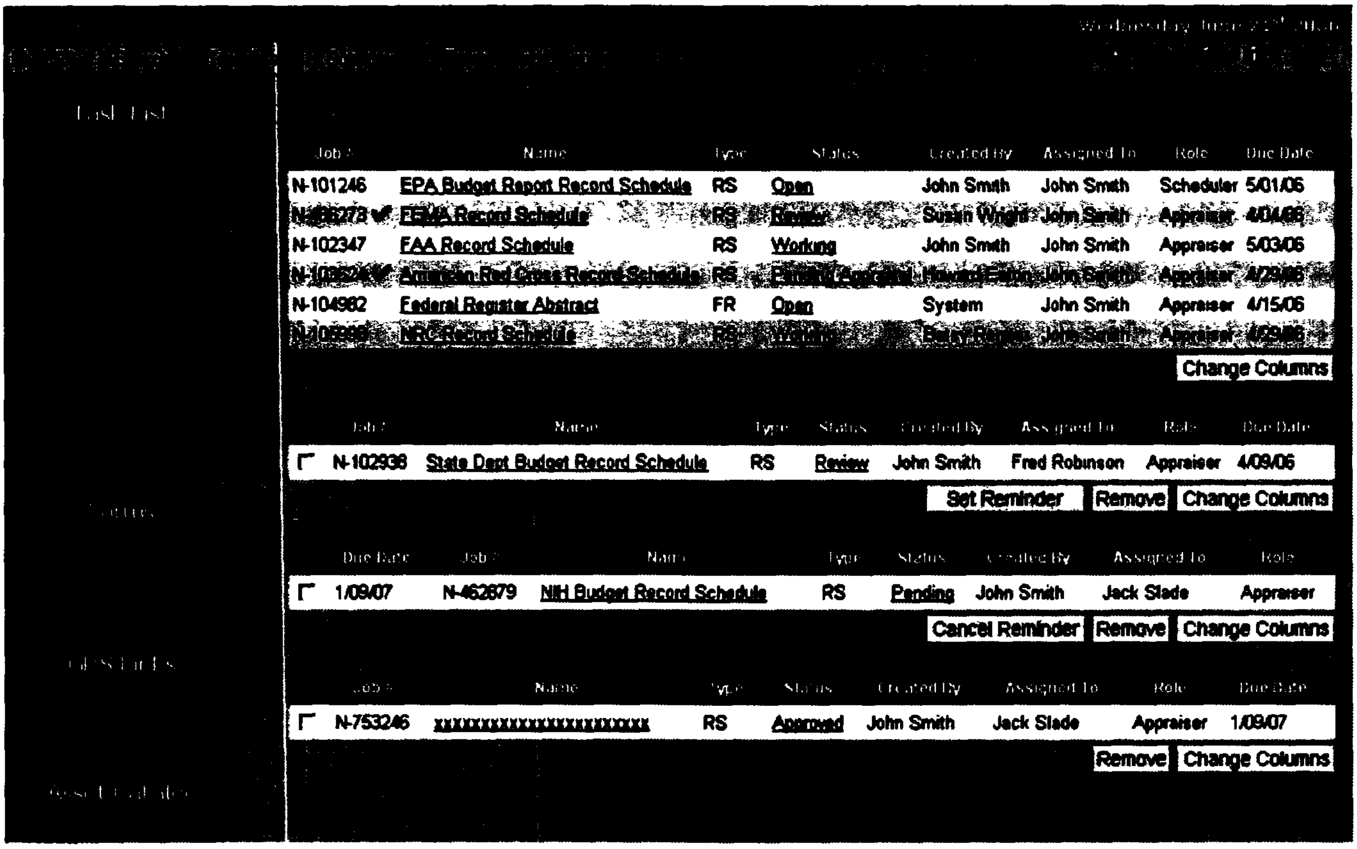
Document Template
Presentation Template

Edit Template

Document Template
Presentation Template

elters.gif

Figure 13 – Task "Inbox" Within a Workbench



Task List

Job #	Name	Type	Status	Created By	Assigned To	Role	Due Date
N-101246	EPA Budget Report Record Schedule	RS	Open	John Smith	John Smith	Scheduler	5/01/06
N-[illegible] ✓	FEMA Record Schedule	RS	Review	Susan Wright	John Smith	Appraiser	4/04/06
N-102347	FAA Record Schedule	RS	Working	John Smith	John Smith	Appraiser	5/03/06
N-[illegible] ✓	American Red Cross Record Schedule	RS	Pending Appraisal	Howard Eaton	John Smith	Appraiser	4/29/06
N-104982	Federal Register Abstract	FR	Open	System	John Smith	Appraiser	4/15/06
N-[illegible]	NRC Record Schedule	RS	Working	[illegible]	John Smith	Appraiser	4/29/06

Change Columns

	Job #	Name	Type	Status	Created By	Assigned To	Role	Due Date
☐	N-102938	State Dept Budget Record Schedule	RS	Review	John Smith	Fred Robinson	Appraiser	4/09/06

Set Reminder Remove Change Columns

	Due Date	Job #	Name	Type	Status	Created By	Assigned To	Role
☐	1/09/07	N-462879	NIH Budget Record Schedule	RS	Pending	John Smith	Jack Slade	Appraiser

Cancel Reminder Remove Change Columns

	Job #	Name	Type	Status	Created By	Assigned To	Role	Due Date
☐	N-753246	xxxxxxxxxxxxxxxxxxxxxxx	RS	Approved	John Smith	Jack Slade	Appraiser	1/09/07

Remove Change Columns

2.4.2.5 *Task Performance*

It would be impractical to expect a user fill out a complicated Web form by providing them only a small, portlet-sized portion of the screen. When the user selects to perform such a task, they are afforded the maximum real estate possible by making this item as the only item occupying the main body of the portal layout. Upon submittal, the portlet invokes its associated processing, including validating user input, manipulating data and assets, and persisting data. If the submitted form has errors, it is returned to the user for correction, with the errors clearly identified.

Some tasks require more than one user session to complete. For example, developing a NARA Standard Description may require some research that is spread over several days. For these tasks, the system allows the user to save partially complete work, and return to it at a later time to complete – with the previous input included in the new session.

Upon completion of this user task, the workflow manager passes control to the next step in the business process. The workflow manager invokes system services to perform automated steps, and queues tasks for human performed steps. The user (which may be the same person) for that step then has this item added to his/her available set of tasks. The event log for this workflow creates a system-generated audit trail for each process Instance.

2.4.3 Notional Record Life Cycle

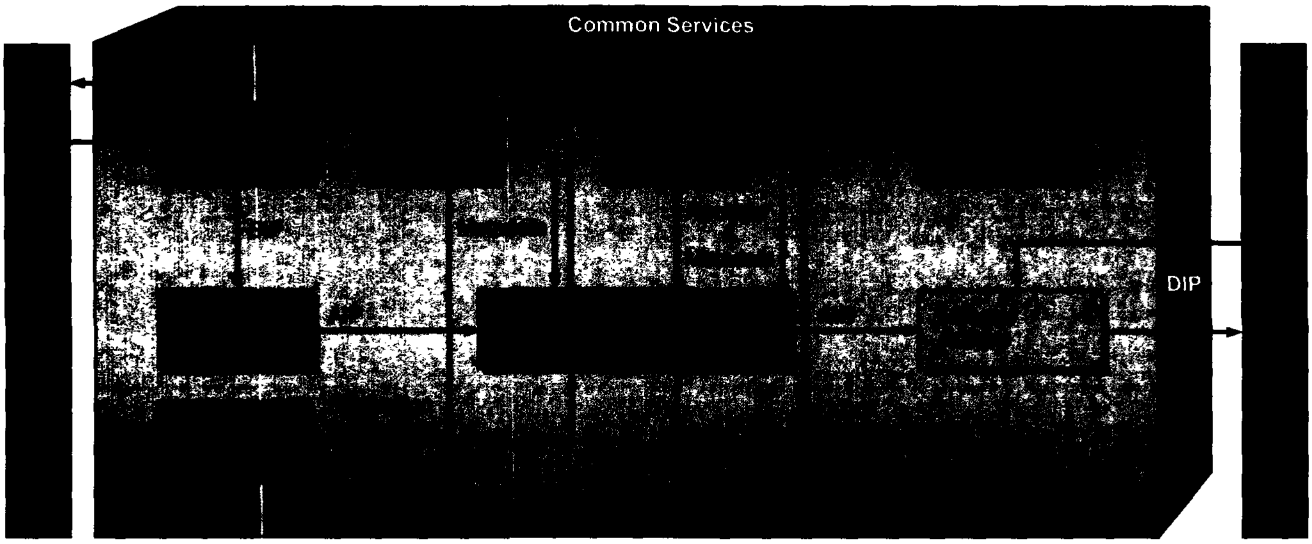
Now it is important to step back and provide the context as to what provides the basis for the ERA System. Figure 14 illustrates the notional life cycle of records as they move through the ERA System. This figure and text description of the steps uses the following terms and roles from the Open Archival Information System (OAIS) reference model[6]:

- **Producer:** Persons or client systems, which provide the information to be preserved. In the ERA System documentation, the Producer role is named "Transferring Entity".
- **Submission Information Package (SIP):** An Information Package that is delivered by the Producer to the OAIS for use in the construction of one or more Archival Information Packages (AIPs).
- **Metadata:** Data about other data; in this context, metadata is data about the records and their life cycle.
- **Archival Information Package (AIP):** An Information Package, consisting of the content information and the associated metadata, which is preserved within an OAIS.
- **Dissemination Information Package (DIP):** The Information Package, derived from one or more AIPs, received by the Consumer in response to a request to the OAIS.
- **Consumer:** Persons or client systems, which interact with OAIS services to find preserved information of interest and to access that information in detail.

The figure and text also overlay the notional records life cycle onto the three principal phases of archiving, as identified by the Society of American Archivists: Identify, Preserve, and Make Available.

[6] CCSDS 650.0-B-1, Reference Model for an Open Archival Information System (OAIS). Blue Book (Standard). Issue 1, January 2002

Figure 14 – Notional Records Life Cycle



Legend:	OAIS Functions	ERA System-Level Packages	Service Oriented Architecture
■	1- Ingest	Ingest	Business Application Services
■	2- Archival Storage	Archival Storage	
■	3- Data Management	Records Management	
▨	4- Access	Dissemination	
■	5- Preservation	Preservation	
■	6- Common Services	Local Services & Control ERA Management	Common Infrastructure Services

ERA_ENG_081c

Identify:

- Producers and archivists develop a Disposition Agreement to cover records. This Disposition Agreement contains disposition item description and disposition item instruction.
- Producers submit records to the ERA System in a SIP. The transfer occurs under a pre-defined Disposition Agreement and Transfer Agreement.
- The ERA System validates the transferred SIP by scanning for viruses, ensuring the security access restrictions are appropriate, and checking the records against templates.
- The ERA System informs the Producer of any potential problems.
- The ERA System extracts metadata (including descriptive data), creates an AIP, and places the AIP into Archival Storage.
- At any time after the AIP has been placed into Archival Storage, archivists may perform Archival Processing, which includes developing arrangement, description, finding aids, and other metadata. These tasks will be assigned to archivists based on NARA policy, business rules, and management discretion. Archival processing supplements the Preservation Description Information metadata in the archives.

Preserve:

- At any time after the AIP has been placed into Archival Storage, archivists may perform Preservation Processing, which includes transforming the records to authentically preserve them. NARA policy, business rules, Preservation and Service Plans, and management discretion will drive these tasks. Preservation processing supplements the Preservation Description Information metadata in the archives, and produces new (transformed) record versions.

Make Available:

- At any time after the AIP has been placed into Archival Storage, archivists may perform Access Review and Redaction, which includes performing mediated searches, verifying the classification of records, and coordinating redaction of records where necessary. These tasks will be driven by NARA policy, business rules, and access requests. Access Review and Redaction supplement the Preservation Description Information metadata in the archives, and produces new redacted record versions.
- At any time after the AIP has been placed into Archival Storage, Consumers may search the archives to find records of interest.

Figure 14 correlates the OAIS functional entities to the ERA System-level Packages. There is a direct correspondence between the OAIS functional model and the ERA System functional model. For more details on the ERA System functional model, see Section 2.8.

As a clarification on access and retrieval from archival storage, a mediated search engine is also known as a directory search engine that searches for information by categories. It first searches for a broad subject heading and then searches for more specific topics that fall within those categories.

The OAIS functions are represented as services in the LM Service Oriented Architecture model. The primary OAIS functions correspond to the ERA System's Business Application services while the OAIS common services correspond to the ERA System's Common Infrastructure services. For more details on the ERA System Service View model, see Section 2.7.

2.4.4 System Support

The primary mechanism for ERA System support is the single point of control provided by the SOC. The SOC is a centralized organizational element that is staffed with technicians who have the tools, skills, training, authority and permissions to monitor, diagnose and correct system problems. The SOC staff utilizes enterprise system management tools, which are hosted in the ERA Management element, to monitor the health and performance of the ERA System, perform normal system maintenance, contain and resolve system problems, and support electronic software deployment.

Augmenting the SOC, the ERA Help Desk serves as the entry point for user assistance requests and as the hub to communicate the status of known system issues to the user population. ERA Help Desk personnel manage user requests and problem reports via telephone, and Help Desk management tools.

Some elements of the ERA System architecture and design are driven by the operational concept for the Test program. To support the test approach and activities efficiently and effectively, functional services and capabilities must be designed into the system early in the project life cycle. The main system design features influenced by the Test program's operational needs include simulation; performance testing/monitoring; and data recording, reduction and analysis. Each of these areas is discussed further in the context of two aspects of the operational concept for Test: pre-deployment testing and post-deployment testing at an operational facility.

2.4.4.1 External Interface Testing

Connections to external systems are unlikely to be available until installation at the sites. The operational concept for testing external interfaces includes emulation of these interfaces during system testing. The system will provide functions necessary for test and training purposes to generate and receive messages following the Interface Control Document (ICD) formats and specified system behavior. The emulator will generate responses to messages received from the system during test. These services will also be used to support the training operational concept as described in Section 2.4.5.

When testing is required in the field, the system will permit test messages and data to be sent through the system such that the test data and any temporary artifacts created during processing can be easily detected and deleted. Test data is flagged as such to easily distinguish it from operational data.

2.4.4.2 Performance Testing/Monitoring

An important aspect of testing is to verify that performance and stability requirements are met or exceeded. The concept is that test plans and cases are written and executed to focus on performance, separate from the test cases that focus on functional requirements. Initially, performance is projected through modeling. Later, as system development progresses, performance is measured and periodically re-measured with the actual, developed system. The performance models are updated throughout the system life cycle, incorporating design changes, measurement data, and knowledge gained from the integration and test phases. See Performance Modeling and Prediction Report for more detail about performance modeling.

Features of the ERA System to support performance testing include an ability to automate generation of performance load data, measure system response times and internal processing times, and to enable/disable various performance measuring hooks. This is necessary because the very presence of performance monitoring may affect system performance.

In the field, performance monitoring is an important operational element of the SOC. One of the primary purposes of the SOC is to provide enterprise-wide monitoring of a number of system performance parameters such as CPU usage, memory usage, and storage usage so system performance issues may be avoided or addressed in a timely manner. Test of performance using the operational system, if/when necessary, would be performed at off-peak hours for minimal disruption of service.

2.4.4.3 Data Recording, Reduction and Analysis

During test phases, some requirements can be verified only by analyzing system-generated artifacts such as event logs. The ability to define which data and data elements are recorded and to enable/disable specific types of data recording is a key aspect to support this test concept. For a system as large and with as much data as the ERA System, automated tools to support the consolidation/reduction of data and report generation assist in more efficient, less error-prone analysis of system behavior. These support functions may be implemented as a built-in part of the system development or as tools applied to the system or a combination of the two approaches. Any ERA

Program developed tools used in the formal Test program go through a rigorous certification process to ensure correct behavior and output of the tools.

Data recording, reduction and analysis features may also be used to help with debugging problems and for monitoring/analyzing the system during operation at the sites.

2.4.5 Training

System acceptance by ERA users is a critical success factor for the ERA System implementation. System training is an essential element of User Adoption. The LM Team recognizes that training must accommodate the learning styles of the various ERA System users and that training content should be as convenient as possible to the end user. As such, in addition to the online help tools that will be available in the system, the LM Team has developed training requirements that address both classroom and computer-based training. For both types of training there are considerations in the areas of hardware and software, training content development, and training delivery.

2.4.5.1 Classroom Training

The LM Team plans to use a single ERA Instance from the development facility for classroom training and testing, as a cost-effective way to meet both requirements. This Instance will be available for classroom training and will mirror the production Instance so that training is consistent with the operational environment. The LM Team will use previously developed user-interface testing scripts as the basis for designing scenarios for classroom training. The test/training Instance will include data check pointing functions so that the data will revert back to its original state and will be available for the next class needing to complete the training scenarios. Training materials will include annotated system screenshots. Classroom training will be available for NARA archivists, NARA Managers, and Transferring Entity records managers.

2.4.5.2 Computer Based Training (CBT)

CBT will be available to ERA users 24 hours per day, seven days per week via the Internet and NARANET. Consequently, users will be able to access training during or after work hours at a time that is most convenient for them. The CBT will be simulation-based as opposed to the real system interaction that is found in a classroom-training environment. Separate software packages will be needed to capture screenshots for the simulations, develop demonstrations and pop-up windows, and to code the CBT.

Simulations will be based on test scripts and will be updated and synchronized with the ERA System, as new releases/updates are made available to users. In addition, there will be a link to CBT in the ERA System's online help. Finally, CBT will include email confirmation of completed CBT courses to employee management or to a NARA training coordinator.

CBT Training will be available for NARA archivists, and NARA and Transferring Entity records managers; user training will also be available.

2.5 Driving Requirements

The key ERA System requirements are reviewed in the following subsection. These requirements apply to the entire system, and drive the system's architecture and design. In addition, lower level driving requirements associated with specific system-level packages are described in the corresponding sections of this document.

Each driving requirement includes a description the requirement, and any principles, constraints, and assumptions based on that requirement.

2.5.1 Authenticity

"The purpose of the ERA System is to enable NARA to realize its strategic vision: 'ERA will *authentically* preserve and provide access to any kind of electronic record, free from dependence on any specific hardware or software, enabling NARA to carry out its mission into the future.' The ERA System solution must be dynamic (capable of responding to continuing change) and sound, ensuring that electronic records delivered to future generations of Americans are *authentic* decades in the future, as they were when first created."[7]

To achieve NARA's vision, it is not enough just to preserve electronic records. Now and into the future, NARA must be able to attest to the authenticity of the preserved records in order to protect the rights and interests of its various constituents. If records cannot be certified as authentic, public trust in the National Archives will erode. An authentic record "is a record that is what it purports to be and is free from tampering or corruption."[8]

The authenticity of a preserved electronic record can be certified only if the archives can show that none of the specific authenticity requirements applicable to the record were violated. This is the challenge facing the ERA System.

- **Principle:** Preserving authentic electronic records is a fundamental mission of the ERA System.
- **Implication:** The ERA System architecture and design must include a comprehensive intellectual and technical approach to preserving authenticity. This approach is documented the LM Team's "Implementing Authenticity of Records', May 25 2006, non-CDRL Technical Paper.

- **Assumption:** Authenticity is a judgment that involves levels of certitude rather than a binary yes/no decision.
  - **Implication:** Prior to ingest of a particular body of records, NARA will develop a Preservation and Service Plan that either accepts or modifies the default authenticity requirements. Throughout the rest of the records' life cycle after ingest, the ERA System will be able to produce copies of the digital record (and associated metadata) that can be used to judge the continuing authenticity of the records. Although ultimately only an archivist may judge authenticity, the ERA System's large volume of records will require automated methods to check specific features of the records, which give an indication of authenticity. Human assessment also may be applied to sampled records as part of a quality control process.
- **Assumption:** Preserving accurate bit streams is necessary but not sufficient for preserving authentic records. Authenticity applies to records and aggregates of records, not to bit streams. Authenticity is a determination about conceptual objects, not logical or physical objects.

[7] ERA Requirements Document (RD), pg J2-1

[8] "The Long-term Preservation of Authentic Electronic Records: Findings of the InterPARES Project", available at http://interpares.org/book/index.cfm

- **Implication:** NARA will receive reliable electronic records from federal agencies or donors. The ERA System will preserve unaltered the original bit stream received. The bit stream in itself does not constitute the authentic record; the ERA System's approach to maintaining the conceptual record may involve transforming the information to a different bit stream while preserving the essential characteristics of the records that make them authentic.
- **Implication:** The ERA System will offer Consumers the option to access both the original bit stream, and any transformations.

- **Assumption:** Authenticity is a policy decision and one likely to be tested by the courts.
  - **Implication:** The ERA System will be flexible enough to permit NARA to implement different policies for authenticity now and in the future. As part of the templates for records, NARA will develop default authenticity requirements for different types of records. These templates can be modified over time to reflect new requirements.

2.5.2 Persistent Archives

NARA and the nation will be entrusting the ERA System with the care of "essential evidence". The ERA System must manage this essential evidence in a way that is independent of a particular set of hardware and software technologies. In fact, continual evolutions of the system punctuated by new technology replacements can be expected multiple times during the long life of permanent records.

- **Principle:** The LM Team will ensure that all assets and identification of assets are self-describing so that they can be understood and accessed by different hardware and software technologies.
  - **Implication:** The LM Team will carefully design the structure of the assets specifically to be independent of any particular set of hardware and software. All relationships and metadata will be externalized and persisted in a way so that the retrieval process is self-describing and essential characteristics can be reconstructed from the assets themselves.
  - **Implication:** The evolution planning and preservation planning processes will monitor "disruptive" technologies, and the ERA System will authentically preserve its assets over time.
- **Constraint:** Even with an ideal self-describing format, future generations might require some guidance on understanding the structure of assets within the Electronic Records Archives.
  - **Implication:** The LM Team will base its persistent archives design on widely accepted standards (such as Unicode and XML), and will archive documentation on the design of the archives itself.

2.5.3 Evolvability

In addition to authentically preserving its assets over time, the ERA System itself will evolve. NARA's objectives and requirements for the ERA System include accessing and managing its documentary materials (records) independent of the hardware or software on which such assets were created.

- **Principle:** From NARA's Enterprise Architecture, "We [NARA] will acquire systems that are flexible and adaptable to change."[9]

[9] NARA Enterprise Architecture Overview (Version 3.2), September 13, 2004

- **Rationale:** From NARA's Enterprise Architecture: "NARA is adopting business strategies that are more heavily dependent upon information systems and technology, and likely to change and evolve over time. This makes it important to acquire systems with flexible architectures that can facilitate the quick delivery of new or enhanced information-based products or services."
- **Implication**: The LM Team's Service Oriented Architecture for the ERA System provides the necessary flexibility to assure that new or enhanced technologies can be introduced while maintaining the requisite operational stability and assured performance characteristics.
- **Implication**: The ERA System architecture and design must be developed in the context of a comprehensive approach to system evolution. This approach is documented in the LM Team's *System Evolution Plan.*

Technology evolution has multiple phases that must be continually and repeatedly addressed. Initially, the current deployed technology profile at a given time must be assessed. Evaluations address aspects such as pending obsolescence, variability of life cycle costs, failure probabilities and other risks, as well as continued compliance with strategic objectives (which themselves may also evolve over time). At the same time, the available (but not used) and emerging technology profiles (roadmaps for products and standards) will be evaluated and updated to assess maturity levels, potential risk mitigations/additions, potential cost reductions/increases, and the potential product strategic directions that may impact the ERA System baselines. These assessments of present and future technologies feed a structured review process where particular ERA System architectural support elements are evaluated for replacement. Each of these evaluations will address the plans and operational effects of transitions at each of the impacted functional sites, as well as contingency plans if obstacles are encountered with the subject technology insertion.

Ultimately, technology evolution and insertion must be beneficial, either for improved alignment to strategic goals or increased mitigation of risk or it will be delayed and re-evaluated.

2.5.4 Simplicity

The ERA System's architecture and design must be comprehensible to a non-technical audience so that archivists, consumers, and other records stakeholders can see and understand how the system ensures authenticity. In addition, the simpler the system, the easier it will be to evolve and replace portions of it over time.

- **Principle:** The LM Team will maintain simplicity in the ERA System architecture and design.
  - **Implication:** The architecture must clearly and cleanly partition the system into functional packages that resonate with a non-technical audience. The design components (both hardware and software) must flow down from the architecture partitions in a linear and traceable manner.
  - **Implication:** The requirements must clearly trace into the architecture and design, so that the ERA System stakeholders who created the requirements can see how the system realizes their vision.
  - **Implication:** The architecture and design will use layers of abstraction to "tell the story" of how all the pieces fit together in a comprehensible manner.

2.5.5 Flexibility

The ERA System will manage the nation's "essential evidence" for the Life of the Republic. To accomplish this mission, the ERA System will provide flexibility and policy neutrality. This flexibility has three dimensions: 1) at any point, different NARA communities will require tailored business processes to meet their particular needs; 2) over time, NARA's policies and business processes will change; and 3) there is a strong relationship between NARA's policies and business processes, and the data required to support them.

- **Principle:** The ERA System will provide the flexibility to tailor its business processes to meet diverse and changing needs.
  - **Implication:** The ERA System design provides core functionality through a collection of independent *services*. A *service* provides functions that are well defined, self-contained, and do not depend upon the context or state of other services. This design approach allows new services to be added to the system incrementally over time as new requirements are identified.
  - **Implication:** The business process functionality provided by a service is invoked through workflow *orchestrations*. Orchestrations invoke service methods in a specific order, based upon a defined business process. This approach allows new orchestrations to be added and existing orchestrations to be modified to match changing business policy, processes, and procedures.
  - **Implication:** Orchestrations will call on a flexible business rules engine to guide key decision-making. Authorized users of the ERA System will have the capability to change the business rules and parameters to reflect policy decisions. These changes will automatically flow through to the orchestrations that rely on the business rules.
- **Constraint:** Flexibility comes with a development price, in terms of time, design, implementation, and testing.
  - **Implication:** The ERA System design focuses on making high priority portions of the system the most flexible, based on customer input on the likelihood of change.
- **Constraint:** While the ERA System architecture and design can be policy neutral, the deployment and operation of the ERA System will require many concrete policy decisions.
  - **Implication:** NARA's business and configuration management policies will influence ERA System to support the system's development, test and deployment phases.
  - **Implication:** Business rules developed by the NARA Business Practices IPT during Increment 1 will provide input to the ERA System processes.
- **Constraint:** Much of the ERA System's data is enterprise-wide data for NARA, and therefore needs to be coordinated with NARA's Enterprise Data Architecture.
  - **Implication:** LM will work with NARA to configuration manage the changes to the NARA Enterprise Data Architecture that impact the ERA System to support the system's development, test, and deployment phases.

2.5.6 Extensibility

The ERA System architecture will be extensible in many dimensions, including ingesting a wide variety of records, incorporating new technologies, and providing enterprise-wide services.

A key dimension is that the ERA System will ingest and manage electronic records, regardless of their form. The variety of electronic records types and data types across the Federal Government is vast and continually changing as new systems and software applications are developed. Conducting a comprehensive inventory of the electronic records types and data types across the Federal Government is a nearly impossible task (particularly with data types), and would be out-of-date before the inventory was ever completed.

Thus, the ERA System will provide extensible capabilities to handle new records types and data types over time. This extensibility requirement applies to operations performed on the electronic records, including: gathering descriptive data from the record's contents, performing preservation processing on an electronic record, assessing the authenticity of an electronic record, presenting an electronic record to a consumer; and redacting an electronic record.

- **Principle:** The ERA System will include extensibility in its design to handle new record types and data types for electronic records.
  - **Implication:** The ERA System design includes a service-based framework for each of the operations that require knowledge about the electronic record.
- **Constraint:** Support for new record types and data types will be planned, designed, developed, tested, and deployed.
  - **Implication:** The development plan for each new release of the ERA System will prioritize extensible services to deploy.

ERA will provide other capabilities to extend to other areas as well. For example, the ERA System will provide an extensible way to add new search engines, an extensible way to add new template editing facilities, an extensible way to add new storage devices, etc.

- **Principle:** The ERA System architecture must loosely couple[10] the service components provided in the ERA System to maintain extensibility.
  - **Rationale:** Tightly coupled services complicate adding new or replacement services over time by requiring the coupled interactions between the services to be re-engineered.
  - **Implication:** Where practical, the coupling between the ERA System's services will occur through the highly flexible mediation/Orchestration layer.

The ERA System's Common Infrastructure services, (portal services, directory services, mediation services, etc.), could be extended to provide enterprise-wide services to help realize NARA's Enterprise Architecture.

- **Principle:** The ERA System's Common Infrastructure services will be extensible to provide enterprise-wide services.
  - **Implication:** The LM Team will design the Common Infrastructure services with the view that they might be extended to the enterprise some day.

Finally, the ERA System will be extensible to foreign languages.

- **Principle:** The ERA System must provide the capability for foreign language extensibility without requiring major system redesign.

[10] From the NARA EA Glossary: Coupling is "the degree of interaction between two software modules. Software modules can be loosely-coupled or tightly-coupled."

- **Implication:** The LM Team will use Unicode throughout the design to ensure future language extensibility.

2.5.7 Scalability

The ERA System will be scaleable upwards to support continued growth of Ingest volume, and increased user demand. The pattern of both Ingest volume and user demand will include “spikes”, or short periods where the load on the system is extremely high due to external events. Because the ERA System is among the first truly large-scale production electronic archives, limited industry data exists to support the prediction of processing load, storage capacities, and user demands on the system. Sensitivity analyses will support the examination of order of magnitude changes to predicted inputs. The ERA System will be scaleable downwards as well to support the smaller needs for certain kinds of Instances, including those for classified records.

- **Principle:** The ERA System will scale upwards to support continued Ingest volume.
  - **Implication:** The ERA System architecture is built on a concept of “Instances”, each of which is a self-contained, fully functioning electronic archives. A “federated” network of ERA Instances can be expanded essentially indefinitely to handle an exceedingly large number of concurrent users and a storage capacity exceeding one exabyte.
  - **Implication:** The ERA System allows increasing the capacity of storage provisioned for an Instance.
- **Principle:** The ERA System will scale upwards to support higher user demand.
  - **Implication:** The ERA System allows increasing the number of processors (including servers and blades) provisioned for an Instance.
  - **Implication:** The ERA System allows increasing the power of processors provisioned for an Instance.
  - **Implication:** The ERA System allows increasing bandwidth provisioned for a Federation of Instances.
- **Principle:** The ERA System will scale downwards to cost-effectively meet the needs for smaller Instances, including those for classified records.
  - **Implication:** The ERA System allows a subset of services to be deployed to an Instance (which saves costs of deploying the COTS hardware and software required to support the omitted services).
  - **Implication:** The ERA System allows decreasing the capacity of storage, number of processors, power of processors, and bandwidth provisioned for an Instance.
  - **Implication:** The ERA System supports as many (or few) tiers for hierarchical storage as necessary.

2.5.8 Availability and Performance

The ERA System must provide high availability and high performance, because NARA will be dependent upon the ERA System to carry out its business mission, and Consumers will depend on the ERA System to access essential evidence.

- **Principle:** The ERA System must fulfill specified availability requirements.
  - **Implication:** The ERA System has no single point of failure.
  - **Implication:** Availability modeling and failure mode analyses will be used to ensure that the availability requirements are met.
  - **Implication:** The ERA System automatically performs load balancing and fail-over across Federated Instances.
  - **Implication:** The ERA System includes operational and system support for disaster recovery.
- **Principle:** The ERA System must fulfill specified performance requirements.
  - **Implication:** Performance modeling will be used to predict performance characteristics of the system before it is implemented.
  - **Implication:** The LM Team will continue to refine and calibrate performance models to improve system design.
  - **Implication:** The LM Team will gather and monitor operational performance metrics to ensure the system performs within parameters during operational use.
  - **Implication:** The ERA System architecture includes support for degraded performance levels.
- **Assumption:** To meet the performance and availability goals, all aspects of the ERA System will require analysis, testing and configuration management.
  - **Implication:** Orchestrations, while having the capability to flexibly change over time to support new processes, requirements, and policies, will still require testing and configuration management before deployment.

2.5.9 Security

The ERA System will provide ready access to all records, while enforcing access and release restrictions. The ERA System will store both assets and electronic records that range from unclassified up through Top Secret/Sensitive Compartmented Information (SCI).

- **Principle:** The LM Team's architecture and design will ensure security through a defense-in-depth approach.
  - **Rationale:** Defense-in-depth is a multi-faceted security approach that implements both technical and non-technical layers of security to protect valuable resources. Defensive countermeasures are used to reinforce each other, protecting information and resources while allowing response activities to be undertaken quickly and efficiently. In this manner, a single security technique or mechanism is not relied upon to protect valuable resources, resulting in a higher degree of security.
  - **Implications:** Security for the ERA System is a combination of technology mechanisms, processes, facilities and personnel, all properly administered. The ERA System design uses, insofar as practical, independent control measures to counter the ERA System security risks. Besides the mechanisms that prevent unauthorized access, a number of mechanisms and processes are in place to provide additional capabilities to detect, limit, repair and respond to security incidents.

2.5.10 Usability

For the ERA Program to succeed, ERA stakeholders must accept and adopt the ERA System as their means of managing electronic records.

- **Principle:** The LM Team will develop a system that enables end users to accomplish their tasks in an operationally-acceptable manner that leaves them satisfied and positive about their experience.
  - **Implication:** The ERA System user interface design will follow documented Web design and usability guidelines, published in the ERA Human Factors Specification, which are based on a government standard published by the Department of Health and Human Services (HHS) and NARA standards.
  - **Implication:** The ERA System user interface will be tested and refined with users in the LM Human Factors Lab.
  - **Implication:** Performance is a key characteristic of user satisfaction; the ERA System will consistently provide the required response times to users per the SyRS.
  - **Implication:** The LM Team will evaluate price versus performance parameters for other performance-related TPMs.

2.6 Software Design Concepts

The following section present software design concepts that are important in understanding the ERA System.

2.6.1 Design Patterns

The LM Team's design makes extensive use of standard design patterns throughout.

- A design pattern provides a scheme for refining the subsystems or components of a software system, or the relationships between them. It describes commonly recurring structure of communicating components that solves a general design problem within a particular context[11]

Design patterns are invaluable tools for implementing "best practices" and "lessons learned" for solving known engineering problems. They first became popular within the software design community with the acceptance of the book *Design Patterns: Elements of Reusable Object-Oriented Software* by Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides.

Each design pattern focuses on a particular object-oriented design problem or issue. The pattern describes when it applies, whether or not it can be applied in view of other design constraints, and the consequences and trade-offs of its use. Although design patterns describe object-oriented designs, they are based on practical solutions that have been implemented in mainstream object-oriented programming languages.

The following design patterns have been used in the LM Team design:

- Framework

[11] *Pattern-Oriented Software Architecture: A System of Patterns* by Frank Buschmann, Regine Meunier, Hans Rohnert, Peter Sommerlad, and Michael Stal.

  - Defines an abstract set of interactions based on protocols, which allow processes that support the protocol to be "plugged in" to the framework and to extend the software to provide new capabilities.
- Façade
  - Provides a unified interface to a set of interfaces in a subsystem. Façade defines a higher-level interface that makes the subsystem easier to use. This can be used to simplify a number of complicated object interactions into a single interface.
- Adaptor
  - Allows objects with incompatible interfaces to work together. This is sometimes called a *wrapper* because an adaptor wraps the implementation of another object in the desired interface.
- Mediator
  - An object that encapsulates how a set of objects interacts. A mediator promotes loose coupling by keeping objects from referring to each other explicitly, and permits their interactions to vary independently.
- Observer
  - Defines a one-to-many dependency between objects so that when one object changes state, all its dependents are notified and updated automatically. Used mostly for managing dynamic relationships among objects.
- MVC
  - Model View Controller (MVC) is the concept of encapsulating some data together with its processing (the model) and isolating it from the manipulation (the controller) and presentation (the view). A *model*, therefore is an object representing data or even activity, e.g. a database table. A *view* is some form of visualization of the state of the model. A *controller* offers facilities to change the state of the model.

2.6.2 Templates

Templates play a large part in NARA's vision of the ERA System both as a means to manage and schedule records, and to preserve electronic records. Templates also provide a key characteristic of a "self-describing archives" in the sense that templates capture and externalize specifications on how the system operates. Templates provide flexibility and extensibility to the architecture and provide a mechanism for the system to evolve and adapt to changing organizational needs. The ERA Program Management Office (ERA PMO) has defined templates as:

- A [template is a] set of specifications about a type of electronic document, record, donated material, or an aggregate of such electronic documentary materials[12]

The LM Team calls templates that conform to this definition *Record Templates*. Record Templates specify characteristics from the archival domain. For example, a particular kind of Record Template might specify the expected content (such as a subject field and a date field) in a record type (such as a memorandum).

[12] NARA "Key Questions and Answers about Templates (Version 1.0)" White Paper, Page 1

The LM Team has extended the use of templates to cover the ERA System domain as well, through *System Templates*. The book *Semantics in Business Systems* provides a reasonable (albeit elliptic) working definition of system templates:

- A [template is a] pre-existing outline that allows for the generation of new data conforming to the pattern of the template.[13]

System templates specify characteristics from the System Engineering domain. For example, a particular kind of System Template might specify the fields required for an electronic form, as well as their constraints and presentation.

The definitions of both Archival Templates and System Templates are quite abstract, in the sense that many different kinds of things could be specified about records in Archival Templates, and many different kinds of things could be described by an outline in System Templates. This high level of abstraction has led to confusion about templates, because the single unqualified term "templates" can potentially mean so many different things to different people in different contexts.

The ERA System requirements cover templates at this same abstract level: the requirements call for a generic template registry, which supports generic template management facilities (including a hierarchy of templates). The LM Team's architecture meets these requirements at this abstract level, as documented in Section 2.8.6. This architecture allows NARA to define new kinds of templates over time, and manage them within the system.

The system design requires the LM Team to provide concrete details based on these abstractions. Specific design elements will produce or consume specific kinds of templates to achieve specific results. Section 2.6.2 enumerates and describes the types of templates, and how the system will use them. This enumeration is only exhaustive in the sense that it represents the types of templates currently designed into the system; as mentioned, the architecture supports adding new types of templates over time, and the LM Team plans to refine its template list through the Preliminary Design Review (PDR) and Critical Design Review (CDR) design phases.

Providing user-friendly tools to create and modify templates is of critical importance, because Archival Templates capture complex and important semantic meaning about the records within the archives, and System Templates control the operations of the archives. The LM Team believes that general-purpose abstract template tools cannot meet this requirement. The more generic the tools, the less tailored they are to the specific requirements of a specific template. Given the wide variety of template types, and the wide knowledge and expertise of the different kinds of users who might maintain templates, a general-purpose template editor will be sub-optimal. Instead, the LM Team intends to use the framework pattern to allow a series of template editing tools to be plugged into the ERA System, to support different kinds of templates in highly tailored ways and to allow extensibility over time. Section 2.6.2 describes this approach in more detail.

While there are relationships between forms, reports and templates, they are distinctly different elements and meet different needs. A *form* is a construct, whether it is electronic or otherwise, to collect information from an individual or group of individuals. The information from the form is entered into the system for the system to use or to store for future reference. A *report* is information from the system to an individual, a group of individuals, another system, another part within the same system, or a file that documents the state of the information at some point in time. In the case of both the form and report, templates govern the information to be addressed, how that information is presented to the

[13] *Semantics in Business Systems: The Disciplines Underlying Web Services, Business Rules, and the Semantic Web*, Dave McComb, page 369

user, and how the information is used by the system. Hence, a template or set of templates would establish the set of information requested from a user in the development of a disposition agreement; implement constraints on the information values; define how the information request is presented to the user; and contain rules that direct the operation of the system based on information that the user entered in the displayed form. Through this concept, managers can change system performance through modifications to existing templates or through the creation of new templates. Similarly, in the case of reports, there is a template or set of templates that define and implement the instructions for a report's content, format, timing, and destination.

2.7 Service Oriented Architecture Model

The LM Team's approach to the ERA System implementation uses a Service Oriented Architecture (SOA). In an SOA, business functionality is delivered by a set of loosely coupled services that communicate via request/response interfaces or by message passing.

In ERA System's SOA, a mediation layer provides communications to the services within an ERA Instance. The mediation layer also communicates across ERA Instances (within a classification level) to other mediation layers for federated operations, such as federated search and retrieval, via message queuing and message passing. Business processes are implemented in the mediation layer as a composition of services through orchestrations.

Features of an SOA include:

- Business functionality is encapsulated in independent modules (i.e., services), which provide a single business function. These services are "black-boxes", where the consuming business process does not need to know about the internal implementation. The modules are loosely coupled, with a request/response or message-passing interface.
- An integration layer mediates access to back-end applications for data.
- Business processes are orchestrated to create a "composite application".
- An SOA ensures documented and testable system interface. Each Service has a defined and public interface, typically expressed in the Web Service Description Language (WSDL), which lists all of the services methods, with their inputs and outputs. The Services can be tested independently, and the business processes which orchestrate the Services can also be tested.

The LM Team's SOA for the ERA System ensures loose-coupling of services and processes by employing asynchronous messaging using event handlers, messaging, and message queues. The loose coupling of services is the key parameter to enabling an evolvable, scalable, and extensible ERA System solution. The internal implementation of each service can be modified as user load grows, as new requirements emerge, or as technology changes, without affecting the remainder of the ERA System solution – as long as the service-based interface remains unchanged.

2.7.1 Services

Services have five basic tenets:

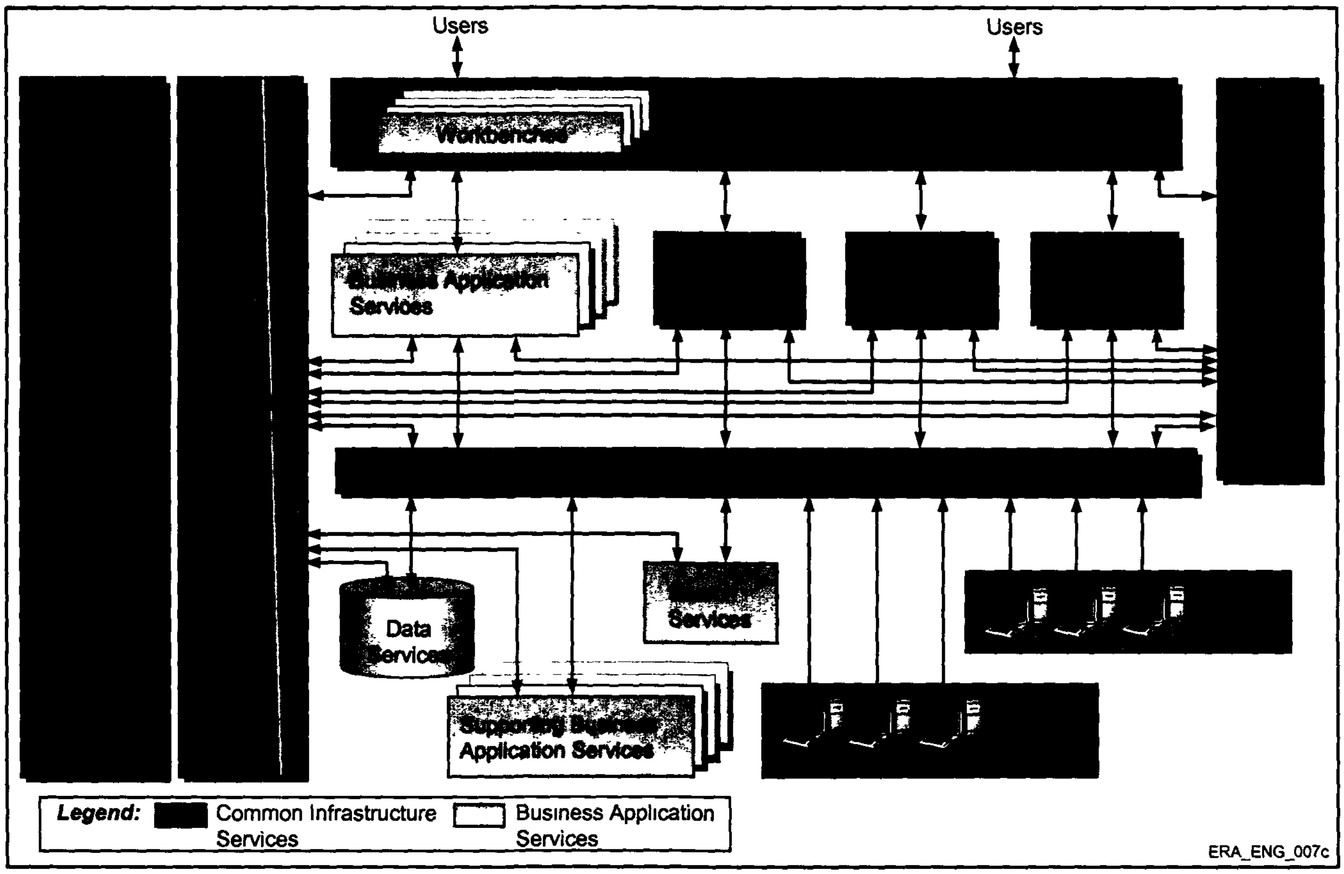
- Well defined, with explicit boundaries
- Autonomous, not depending on the state of any other service
- Share schema and contract, not class

- Expose (or "publish") an interface for invoking the service based on the contract (in other words, provide an Application Programming Interface, or API)
- Use policy as the basis for service compatibility

An SOA is based on the underlying services, their connections, and orchestrations. An SOA includes Common Infrastructure Services that are common to most enterprises, and are typically delivered through the configuration of COTS products. An SOA also includes Business Application Services, which may include custom-developed applications and components.

Figure 15 presents a view of the Common Infrastructure services and the Business services, based on the Defense Information Systems Agency's (DISA) Net-Centric Enterprise Services (NCES) model.[14]

Figure 15 – Service Oriented Architecture View


Users
Users
Workbenches
Business Application Services
Data Services
Services
Supporting Business Application Services
Legend: ■ Common Infrastructure Services □ Business Application Services
ERA_ENG_007c

Common Infrastructure services are designated separately within Figure 15 and include services that are leveraged across many business processes:

- Security Services (including authentication, identification, authorization, and audit logging)
- Portal Services
- Collaboration Services (including Enterprise Content Management)

[14] DISA NCES home page, http://www.disa.mil/main/prodsol/cs_nces.html

- Messaging Services
- Data Services (including file and database management)
- Enterprise Service Bus Services (including Business Process Management)

The Common Infrastructure services in the Services View correspond to the ERA Management and Local Services and Control System-level Packages in the ERA System Functional Architecture. The LM Team has architected the common infrastructure services in such a way that they can be extended to provide enterprise-wide services for NARA. For example, the ERA Portal Services could be extended to provide a single common portal that includes the ERA System and other NARA legacy systems.

Users and external systems view only those ERA System services that have been made visible to them – the Portal service and the Enterprise Service Bus, respectively. These ERA System services authenticate and authorize these interactions by invoking the Security Services.

Figure 15 shows the Enterprise System Management Services and Security Services spanning the model because they truly pervade the model. For example, all service requests are authenticated and authorized through the Security Services, and all services provide health and status information to Enterprise System Management Services.

Business Application services are designated separately within Figure 15 and are specific to the ERA System business environment. Business Application Services are user-facing business processes, and connect to portal services to provide the user-interface. Supporting Business Application Services perform automated system tasks. The Business Application services correspond to the Ingest, Records Management, Preservation, and Dissemination System-Level Packages in the ERA System Functional Architecture. Search services are called out in Figure 15 to conform with the DISA NCES model, though in ERA System's service view, search services are just another Supporting Business Application Service. Business Application services typically include a user interface, logic to perform a specific business function, and connections to a persistent data store. They implement a step in a business process, such as:

- User tasks (with Web forms), input validation, data read/write
- System tasks, automated by COTS or custom code (Supporting Business Application Service Components)

Services communicate with the mediation layer and thereby to persistent data stores through connections. These connections are used to invoke a service and to receive its response. Connections have evolved from proprietary interfaces through a plethora of standards-based interfaces to Web-services interfaces. It is the emergence of these Web-services interfaces that makes the full implementation of an SOA practical.

2.7.2 Orchestrations

The business functionality provided by a service is invoked through workflow *Orchestrations*. Orchestrations invoke service methods in a specific order, based upon a defined business process. This approach allows new Orchestrations to be added and existing orchestrations to be modified to match changing business policy, processes, and procedures. The ERA System will include a set of Orchestrations that are based upon how NARA has defined its business processes at a certain time. The system includes support for creating, modifying, deploying, and decommissioning Orchestrations, so that the ERA System can flexibly adapt to changing NARA policy.

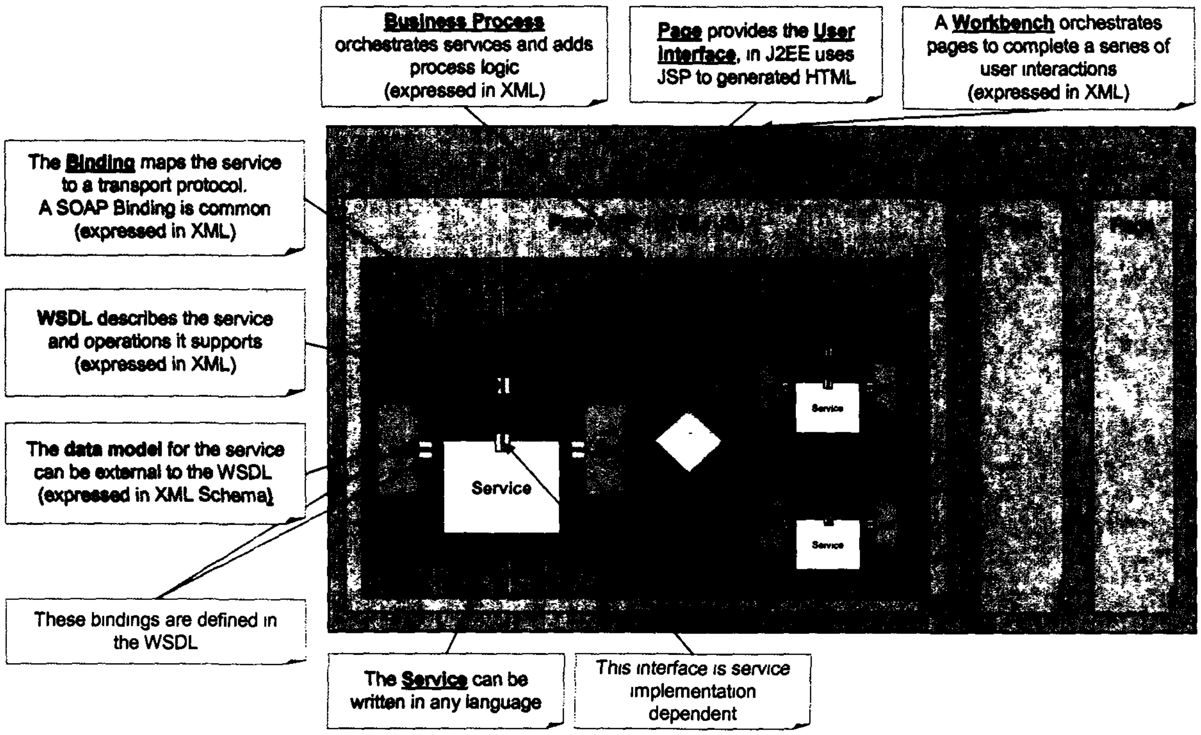
Business processes are orchestrated in the Mediation Layer, and invoke available services and controls for: user steps, system steps, message queues, read/write to persistent data store, and other orchestrations.

Orchestrations encode a logical process flow, and can include: workflow entries, sequential steps, decisions, branches/joins, iterations, publish/subscribe, error handling, workflow exits, and other orchestrations. Orchestration steps in a Web environment often produce and consume Web pages.

Error handling can include invalid authorization, timeouts, invalid messages, assured delivery of messages, check pointing, transaction failures, and rollback and compensation.

Figure 16 illustrates that business services, business process, and the portal interact to create business functionality. (This example uses Java 2 Platform, Enterprise Edition (J2EE); .NET and other technologies provide the same framework.) The portal presents a set of tools on the user's workbench. Underlying these tools are sets of Web pages and Web forms that are specific to that user's task. In performing that task, these Web pages invoke underlying system services to, for example, access persistent data stores, access queues, or perform input validation. These Web forms, system services, and persistent data stores can be implemented in any technology, such as J2EE or .NET, as long as their interfaces adhere to standards such as Extensible Markup Language/Simple Object Access Protocol (XML/SOAP) and are described using a standard such as Web Services Description Language (WSDL).

Figure 16 – Orchestrations Invoke Services and Controls to Codify a Business Process


Business Process orchestrates services and adds process logic (expressed in XML)
Page provides the User Interface, in J2EE uses JSP to generated HTML
A Workbench orchestrates pages to complete a series of user interactions (expressed in XML)
The Binding maps the service to a transport protocol. A SOAP Binding is common (expressed in XML)
WSDL describes the service and operations it supports (expressed in XML)
The data model for the service can be external to the WSDL (expressed in XML Schema)
These bindings are defined in the WSDL
Service
Service
Service
The Service can be written in any language
This interface is service implementation dependent

ERA_ENG_153b

Orchestrations are configurable based on NARA Policy. In the LM Team's approach, a new or reconfigured Orchestration can be deployed independent of any other Orchestration, and independent of the consumed services. The detailed process for deployment will follow the governance policies, including configuration management and release approval, to which NARA and the LM Team agree.

2.7.3 SOA for Portals

The workbenches described in Section 2.4.2 User Level Operations uses a Web-portal framework, which allows new components to be integrated into the operational platform over time as new business process requirements arise and are met, and new workbenches to be created as new user roles are defined. The components encapsulate[15] and provide specific features from COTS products, which allow the NARA-defined business processes to drive the overall design. This encapsulation contributes to the key requirement of hardware and software independence.

[15] In object-oriented and service-oriented designs, "encapsulation" is the inclusion of everything needed to perform a specific process within a "black box". The encapsulated object "publishes" interfaces, which precisely define the service's inputs and outputs. Other services adhere to these published interfaces without having to be concerned with how the service accomplishes its processing.

The Web-portal framework provides the following benefits:

- Enables ubiquitous access by users with no special client-side software
- Facilitates ease of maintenance with server-side deployment
- Provides a configurable user workbench capability "out of the box" (with pluggable "portlets" providing different business functions)
- Supports full compatibility with SOA – the user interface needs of SOA are driving Portal standards (WSRP, JSR 168)
- Integrates with many COTS products that include pre-built portlets available to fulfill related requirements (e.g., Enterprise Content Management, Collaboration, and Business Rules Management)
- Promotes a consistent user-interface across user classes and lines of business
- Allows specialized "branding" for NARA stakeholders such as Federal Records Centers and Presidential Libraries

Workflow drives many of the operational tasks presented in the workbenches. The ERA System architecture ensures that each step in the life cycle of a record archived by NARA is completed by the proper professionals, increasing assurance that the authenticity of each record is maintained. A workflow manager identifies the NARA-defined tasks and roles for each record at each stage in the life cycle. Users have access to the complete set of tasks requiring their attention at the selected security classification level. Tasks act on records and collections, or perform other ERA activities. The user can partially or fully complete tasks, performing multiple tasks in parallel. At the completion of a task, the record or collection that is being acted upon advances to the next workflow step that has been defined to the workflow manager. The user (which may be the same person) for that step then has this item added to his/her available set of tasks. This creates a system-generated audit trail for all tasks.

Reports show the size of the backlog of tasks, indicating the overall status of work within the ERA System. Managers have the ability to assign and reassign tasks to different users or groups of users.

The LM Team recognizes that not all data types, and not all tasks, are suited for the Web. For example, there are many specialized formats (such as Geospatial Information System formats) that may require specialized client-side (non-Web) software. Similarly, redaction is typically performed with specialized client-side software. The LM Team's design uses service adapters to integrate client-side software with the mediation layer.

2.7.3.1 User Interface Architecture

The user interface architecture is based on a Portal Framework. The implications of using a portal, the architecture of the portal, and how a user interacts with the portal and its component applications are discussed in this section.

The ERA System portal is structured into a set of Workbenches. Unregistered general public users can access only the default workbench. Registered users are presented with the role-based workbenches to which they are authorized. These role-based workbenches include tools and notices that are relevant to the user's role, and restrict users from access to functionality to which they are not authorized.

2.7.3.1.1 Portal

The term *portal* refers not only to the user interface and navigation, but also to the supporting architecture for integration with the underlying applications and services. The LM Team's architecture for the ERA Portal:

- Provides a user friendly interface with a consistent look and feel
- Supports dynamic interaction with users by providing an information rich and context-sensitive environment
- Provides an environment where users can perform different business functions that are created dynamically by invoking business service components
- Provides session management, including single sign-on among the portlets and their underlying business service components
- Enables implementing different business functions within a single architecture
- Implements loose coupling, but high integration, within all of its components
- Implements and enforces NARA's security policies
- Supports decentralization of administration of content, users, and privileges

2.7.3.1.2 Navigation and Taxonomies

Implementing the ERA System user interface within a portal framework has implications for user navigation of the ERA System. The navigation "style" within a portal typically uses tabs for pages, left hand context-sensitive navigation, and includes an array of "portlets" within the main body of each page. Maintaining these navigation panes across all subordinate layers of the portal provides a consistent look and feel, and provides a consistent mechanism for user navigation.

The ERA System portal contains a wide selection of tools, notices, and content, in addition to access to the electronic archives themselves. In providing navigation schemes to access these capabilities, it is important to provide comprehensive and understandable taxonomies, which systematically organize the large volume if information. Best practices for portals include providing multi-dimensional taxonomies, to match the way the many classes of users do their word. For example, depending on the user and what they are trying to locate, useful navigation paths to ERA tools and communities might be via the organization chart of NARA, or might be a cut across the organizational boundaries based on business functionality (e.g., HR, Finance, Services for Citizens). Taxonomies for navigating the electronic archives themselves include the organization of US Government and the organization of the constituent agencies, original order of a set of records, date order of a set of records, defined collections, authority sources, and conceptual topics (e.g., immigration, cold war, or terrorism).

2.7.3.1.3 Tools and Portlets

Tools that provide the user interface business functionality are manifested as portlets. Portlets include hooks to back-end services and processes. This architecture allows that any backend application can be "wrapped" with an interface, and that interface can be fronted by a portlet. Thus, new services, legacy applications, and Enterprise applications can be exposed in the portal.

The portal framework also provides a security container. All portlets inherit security, including user session information such as user identity, from the container. This enables single sign-on across the portlets, and to the back-end applications and services.

The portal provides a suite of core tools that are used across different workbenches. Core asynchronous collaboration, content management, and business process management (workflow) capabilities are provided by many COTS portal products. For the various role-based workbenches, these core capabilities will have a "façade" interface so that the user experience is in context with their role and tasks.

Users can personalize their workbench by adding tools, removing optional tools, and rearrange the layout of a page or pages. This personalization data are persisted within the ERA System, and will remain in effect across the user's sessions.

2.7.3.2 Composite Applications

The tools in a user's workbench, which provide the user interface to business functionality, are manifested as portlets. These portlets include hooks to back-end services and processes. The portlets, the processes, and the requisite business logic together comprise a Composite Application.

Composite applications provide the end users with a complete set of business functions to perform business tasks such as managing a Disposition Agreement, processing a FOIA request, or submitting and statusing an order. A composite application allows for having several interactions between the application and the end user. Composite applications may interact with the Core Services and Business Application Services directly, or, for more complex applications, may interact through the Business Process Management service to orchestrate and mediate Service invocations.

2.7.4 Governance

An SOA needs governance covering roles, responsibilities, and ownership, and a federated mechanism for service management. Specific areas to be included in a comprehensive governance policy are:

- Authoritative ownership of data
- Service registry
- Service prioritization
- Security policies
- Service level agreement management

Service management is more than a set of tools; it also includes the policies and procedures that the tools implement. Configuration Management control within Service Management, including test and deployment control gates, assures proper operation before promoting new controls, orchestrations, and services into a production environment.

2.7.5 Security within SOA

Orchestrations are security-aware, and can require authentication and authorization to execute services, assets, queues, and messages. Security services can be invoked at two layers: the communications layer, and the message layer. A communications layer for a request/response type interface, such as HTTP, can include authentication and authorization as part of the interface. For message-passing interfaces, security can be imbedded inside each message. Based on defined access policies, a user or service may be authorized access only to certain queues, certain message types, and certain specific messages. The structure of the relationship between users to roles is extensible to support on-going definition of new roles and capabilities in the system.

Refer to Section 2.10 for discussions of the ERA System security architecture and design.

2.8 System Functional Design

The following section provides the next level of detail that stems from the System Functional Architecture discussed in Section 2.3.3. This section is labeled as system functional design since it provides the overall design of the system-level packages identified within the high-level system functional architecture.

The design provides the rationale for system partition based on the archival life cycle to segment it into seven different system packages: Ingest, Records Management, Preservation, Archival Storage, Dissemination, Local Services & Control (LS&C) and ERA Management. There is then a mapping of ERA System requirements to the OAIS archival reference model.

Each of the individual system packages are then defined that includes a summary of key requirements, an illustrated depiction of the functional architecture, and terms and concepts to support the system package.

2.8.1 Rationale for Partitions

These seven system-level packages reflect the result of an engineering effort to select the best conceptual and physical partitioning of the ERA System. The LM Team evaluated several partitioning alternatives based upon the following key system engineering principles:

- **Simplicity:** The ERA System's architecture and design must be comprehensible to a non-technical audience so that archivists, records managers, consumers, and other stakeholders can see and understand how the system ensures authenticity.
- **Cohesion:** Cohesion is the measurement of the extent to which related aspects of a system are kept together, and unrelated aspects are kept out. Systems with high cohesion are simpler and more extensible over time.
- **Loose Coupling**: Coupling is a measure of the extent to which interdependencies exist among system elements. Loose coupling is a kind of coupling in which the interconnections among parts of a system are reduced, making the resulting system easier to understand, modify, test, and enhance in the future (evolvable).
- **Layering:** Layering is a form of cohesion in which the facilities for providing or accessing a set of services through a standard software API or hardware interface are logically kept together. There must also be a strict hierarchy in which higher-level layers can access only lower-level layers. In other words, the system is effectively divided into layers.
- **Domain Isolation***:* Domain isolation creates a layer of security to achieve logical isolation of the network traffic that moves between computers or networks. If an attacker manages to gain physical access to an internal network and attempts to access a server that contains valued data assets, domain isolation can block access simply because the computer that the attacker is using is not a trusted device, even if the attacker used a valid user account and password.

At the start of the System Design phase, the LM Team re-evaluated the conceptual system partitions from the original LM ERA proposal. The originally-proposed partitions were comprised of the Ingest, Storage, Dissemination, Local Services and Control, and ERA Management partitions. The LM Team determined that the original Ingest partition was overloaded and non-cohesive, in the sense that it bundled non-related aspects of the system together that violated the above-stated guiding principles. For example, ingest processes and preservation processes are decidedly distinct and should not be commingled within the same functional partition. This analysis led the LM Team to thoroughly re-examine the system partitions.

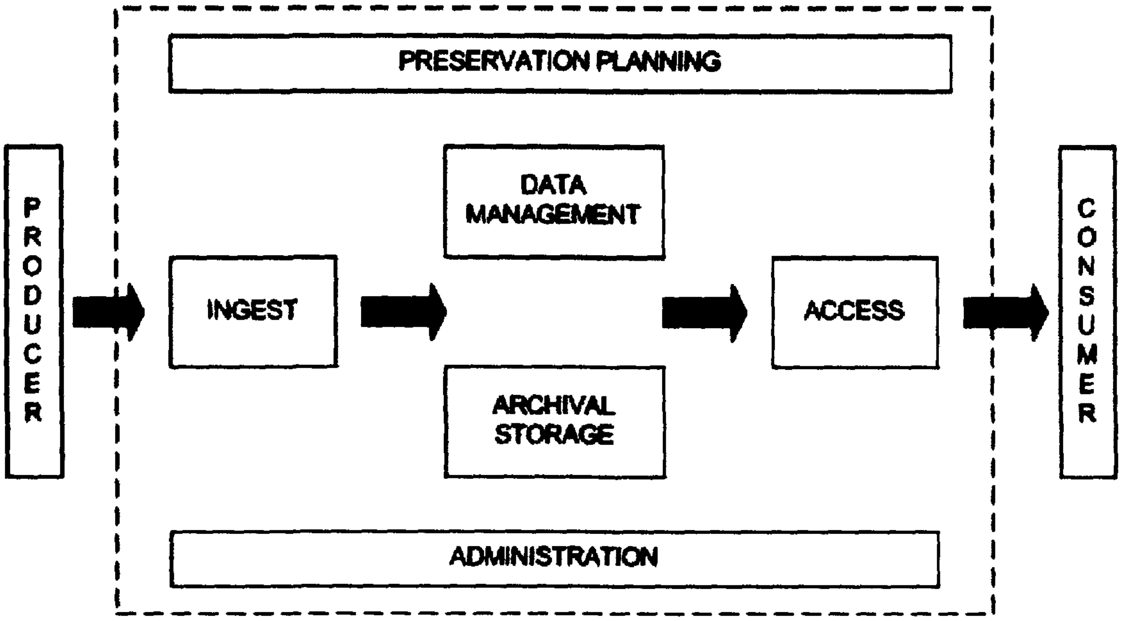
Next, the LM Team re-evaluated the system partitions using the OAIS partitions verbatim for the ERA System. The OAIS model is a functional view, with excellent functional cohesion and loose coupling. It is also simple, and readily understandable to the archival community. As a functional model that is primary focused on archival functional processes, the OAIS model lightly covers concepts that are critical for any large system's success, such as administration across multiple archives, technical layering, and physical partitioning. The LM Team adopted the OAIS model's archival functional partitioning and extended these where necessary for the ERA System, as described in Section 2.8.2.

2.8.2 Mapping from OAIS Model to ERA System Functional Architecture

The Open Archival Information System (OAIS) reference model provides a domain-specific framework of terms, concepts and components for "an archive consisting of an organization of people and systems that has accepted the responsibility to preserve information and make it available for a designated community".[16]

The OAIS functional model, depicted in Figure 17, is composed of six functional entities; Table 7 maps these entities to the ERA System functional architecture.

Figure 17 – Reference Model for an Open Archival Information System (OAIS)



[16] Reference Model for an Open Archival Information System, p. 1-1

Table 7 – Mapping of OAIS Model to ERA System Model

OAIS Model	ERA System Model	Comments
Ingest	Ingest, Records Management	The automated data extraction of descriptive information is performed in Records Management.
Archival Storage	Archival Storage	
Data Management	Records Management, LS&C	Access to data is provided by LS&C.
Administration	LS&C, ERA Management	
Preservation Planning	Preservation	The LM Team's approach goes beyond just preservation planning to manage all aspects of preservation.
Access	Dissemination	Name was changed to avoid confusion; the term "access" is commonly used in Information Technology (IT) documentation.
Common Services	LS&C	This component is typically not shown in the OAIS model diagram because of its pervasive nature.

2.8.3 Mapping from Requirements Categories to ERA System Functional Design

NARA's ERA RD categorizes the ERA System requirements in nine groupings that are based upon the OAIS model. Table 8 maps these categories to the system-level packages:

Table 8 – Mapping of Requirements Categories to System-Level Packages

SyRS Section Number	Requirements Categorization (SyRS)	System-Level Packages (SADD)
ERA1 – ERA6	Records Management	Records Management, LS&C
ERA7 – ERA9	Preservation	Preservation, Records Management
ERA10 – ERA12	Archival Storage	Archival Storage
ERA13 – ERA14	Security	LS&C, ERA Management
ERA15 – ERA16	Ingest	Ingest
ERA17 – ERA20	Access	Dissemination, Records Management, LS&C

SyRS Section Number	Requirements Categorization (SyRS)	System-Level Packages (SADD)
ERA21	User Interface	LS&C
ERA22 – ERA28	Administration	LS&C, ERA Management
ERA29 – ERA32	System Characteristics	LS&C

2.8.4 Data Overview

The ERA System manages the life cycle transactions for vast quantities of electronic records. The transitions and persistence of this information is a central element of the ERA architecture and NARA's mission. This requires a comprehensive approach to managing NARA "enterprise" data including collaboration with NARA data modeling experts.

This section provides a brief overview of how the ERA System manages data and how data is managed across Instances and Federations. More details are provided in the Section 2.11.

2.8.4.1 Modeling Approach

The LM Team's data modeling effort follows the methodology described in the NARA Data Architecture document. NARA's methodology consists of a hierarchy of modeling steps, with each step adding additional detail[17]:

- **Conceptual Model** – A high-level representation of the enterprise information from the perspective of the business.
- **Logical Model** – A high-level representation of the enterprise information from the perspective of IT systems.
- **Physical Model** – Detailed specifications for the organization, structure, and interrelationships of NARA's information assets.

The LM system engineering process follows a similar hierarchy of architecture and design steps. The ERA System architecture and design in this document reflects a full-fledged conceptual model, and a logical model for the key objects and key attributes. This system-level data model addresses only global persisted ERA System data. Data that is encapsulated within a given service and data that is transient are not included in this data model. The LM Team will collaborate with NARA's data modeling experts to further refine and expand the logical and physical model as part of the on-going engineering process during each of the Increments.

[17] NARA Enterprise Architecture, Data Architecture, Version 3.2, page 13

2.8.4.2 Data Stores

The ERA System architecture and design includes four main data stores:

- **Electronic Archives**
  - Contents – The Electronic Archives contain electronic records and other assets as specified by NARA policy, such as disposition agreements, transfer agreements, authority sources, templates, etc. The Electronic Archives for each Instance serves as a repository of the entire documentary materials ingested into that Instance (including the archival storage of transferred electronic records), and as a Safe-Store repository for assets from at least one other Instance in the same Federation.
  - Description – Since the Electronic Archives requires vast and ever increasing storage, the ERA System design includes an Archival Storage management layer that allows more storage to be brought online over time to meet this ever increasing demand. Archival Storage services also encapsulate the Electronic Archives, which insulates the rest of the ERA System from details on where, within the vast storage hierarchy, a particular asset is located – external services use Archival Storage to simply request a copy of an asset, or the storage of an asset.
  - Replication Strategy – Due to its enormous size, the Electronic Archives is not replicated to other Instances. However, a copy of its original (non Safe-Store) data is automatically copied to one other Instance in the same Federation using the Safe-Store mechanism. This ensures that exactly two Instances in the same Federation have one copy of everything in the Electronic Archives for each Instance in that Federation.
- **Ingest Working Storage**
  - Contents – Contains the electronic records transfers while they are undergoing automated ingest processing.
  - Description – Ingest Working Storage physically segregates transferred records to contain the possibility of contamination to the rest of the system from transferred records that could potentially contain viruses, or miss-classified records. Ingest Working Storage also physically segregates Title 13 and other sensitive information on separate media volumes while it is being processed. Transferred records are removed from Ingest Working Storage once they have been safely committed to the Electronic Archives through Archival Storage. The ERA System design currently sizes Ingest Working Storage to contain approximately two days worth of records transfers.
  - Replication Strategy – Since Ingest Working Storage is essentially an input buffer for ingest services at a particular Instance, the information in this data store is not replicated to other Instances in the Federation. There is a unique Ingest Working Storage for each full or partial Instance that contains the Ingest services.
- **Instance Data Store**
  - Contents – The Instance Data Store contains various performance-based caches of assets, such as disposition agreements, transfer agreements, authority sources, templates, etc. The Instance Data Store also contains the Asset Catalog, and any other data that is required for the Instance to operationally perform from other subject areas, such as Policy Data, Security Data, Operational Data, Decision Support Data, etc.

- Description – The ERA Asset Catalog in the Instance Data Store serves as a "master location registry" for all of the electronic records and assets. The Asset Catalog also contains record life cycle data, archival description, descriptive data, and arrangement information. The Asset Catalog data also supports the federated search and retrieve functions, which allow a Federation of Instances to appear as one cohesive electronic archive. The Instance Data Store is used throughout the ERA System to support the wide-ranging data requirements for Instance services. The size of the Instance Data Store is several orders of magnitude smaller than the Electronic Archives.
- Replication Strategy – Different kinds of data from the Instance Data Store are replicated across Instances in the same Federation and to the System Data Store, as described in Section 2.11. In this way, each of the Instances in the Federation has the same Instance Data Store information available to support operations, failover, and load balancing.

- **System Data Store**
  - Contents – The System Data Store contains various systems management data, such as logs, monitoring data, inventory data, Help Desk data, etc.
  - Description – The System Data Store supports the ERA Management functions that are described in Section 2.11.
  - Replication Strategy – Some of this data is replicated to the backup ERA Management System Data Store in the same collection of Federations, and some of this data is replicated to the applicable Instance Data Store in the associated Instance of the collection of Federations, as described in Section 2.11

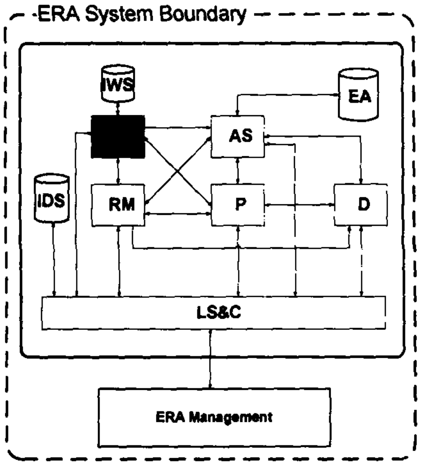
2.8.4.3 Data Encapsulation

The ERA System supports evolvability by allowing physical and conceptual models to change over time. The design includes two layers of abstraction to provide the required flexibility and adaptability to facilitate this evolutionary activity:

- **Enterprise Service Bus** – All Instance services make requests to retrieve and store data through the Enterprise Service Bus. The Enterprise Service Bus translates the request between the logical data model and the physical data model, and ommunicates with the Data Service layer to obtain the actual data from the physical implementation. Services make data requests using the logical data model without requiring knowledge of the underlying physical model.
- **Data Service** – The Data Service supports managing the physical data model in the file systems, the relational databases, and in the object-oriented databases – and could be extended to manage other kinds of data in the future.

These two layers of abstraction allow the conceptual models and the physical models to be changed independently, without disrupting the other services in the system. For example, the Enterprise Service Bus can transparently translate requests to a previous version of a logical model to the new version, and can also transparently migrate from an older to a newer version of a logical model. Similarly, the Enterprise Service Bus can connect to different versions of physical models while providing a consistent logical model view. The version and other configuration management information in the physical models are recorded to assist with this conversion. The Data Service allows new kinds of persistence mechanisms to be included into the system over time.

2.8.5 Ingest



The Ingest package receives electronic records and prepares them for storage within the ERA System.

The following section outlines the key requirements and the functional architecture process flows associated with the Ingest system-level package.

2.8.5.1 Ingest Key Requirements

Table 9 summarizes the Ingest key requirements that drive the architecture:

Table 9 – Ingest Key Requirements

Requirement Referenced	Requirement	Architectural Impact
ERA1.8	Tools for packaging associated transfer agreements, disposition agreements, and templates with records into a self-describing format for transfer into ERA.	Led to Ingest tools that are used to manage transfers.
ERA13.7	Segregation of electronic records during ingest based on potential access restrictions	Led to an Ingest working storage so that records remain segregated until their security access level is determined (and to segregate sensitive records such as Title 13).
ERA14.5	Virus Scanning	Led to an Ingest working storage so that records remain segregated until they are scanned for potential viruses.
ERA1.2	Management of Transfer Requests	Led to Ingest verification that a transfer request is valid prior to accepting a transfer.

Requirement Referenced	Requirement	Architectural Impact
ERA1.8	Tools for packaging associated transfer agreements, disposition agreements, and templates with records into a self-describing format for transfer into ERA.	Led to Ingest tools that are used to manage transfers.
ERA16.3	Confirmation of transfer status to the transferring entity	Led to Ingest providing transfer status to verify a transfer's success.

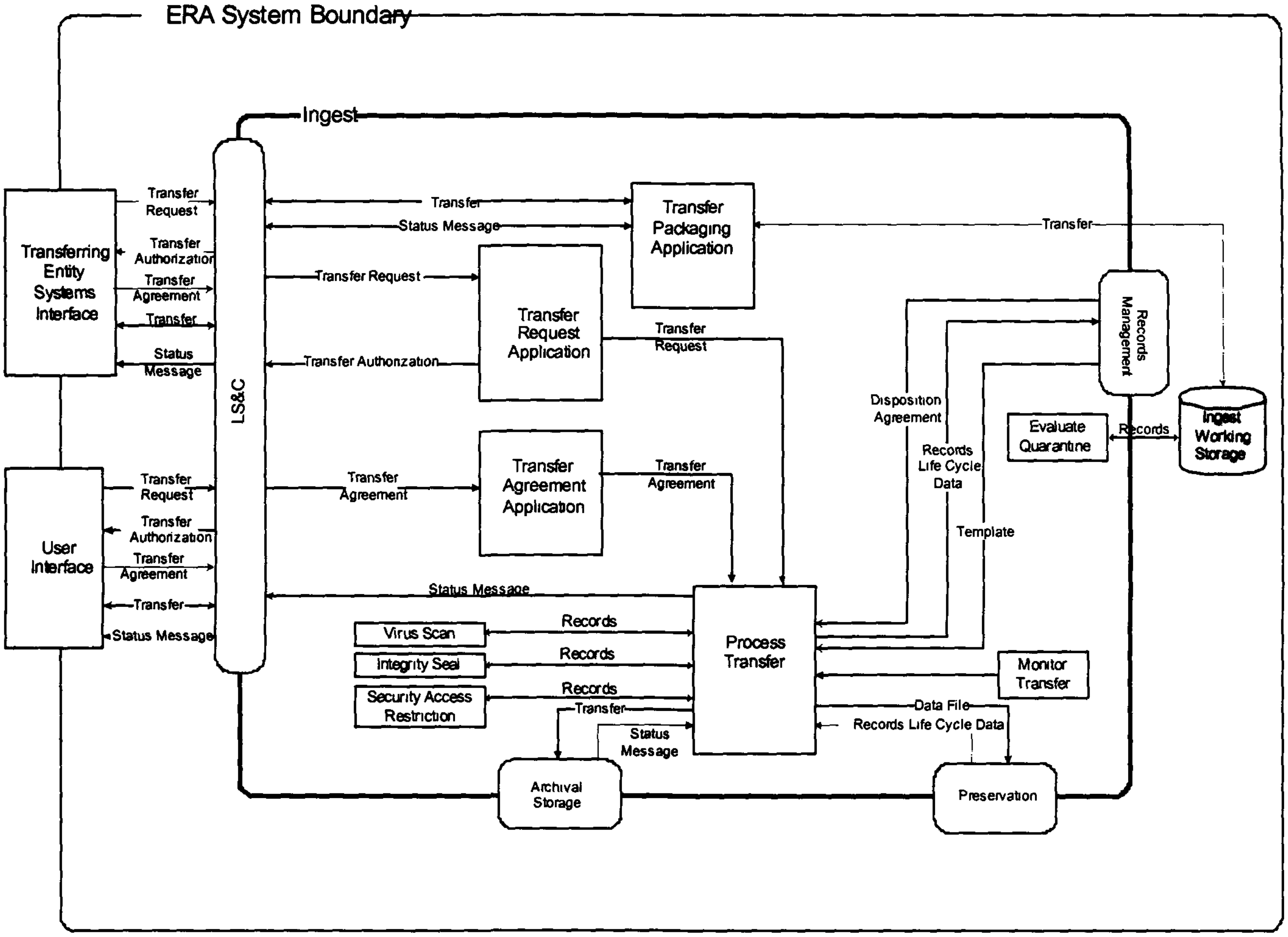
2.8.5.2 Ingest Functional Architecture

The Ingest functional architecture, shown in Figure 18, illustrates:

- The ERA System's external interfaces to the Ingest system-level package
- The internal system-level package interfaces to and from Ingest
- The Ingest logical grouping
- The conceptual data flow of the Ingest system-level package

The architecture supports receiving transferred records while guaranteeing that the records' content, context, structure, and arrangement remain intact.

Figure 18 – Ingest Functional Architecture



Note: An access to Archival Storage is through the Storage Federator service of LS&C.

2.8.5.2.1 Ingest Interfaces

ERA System external interfaces to and from the Ingest system-level package, including external interfaces through LS&C are shown in Figure 18 and identified in Table 10. The internal interfaces between Ingest and the other system-level packages, also shown in Figure 18, are identified in Table 11. The Source column identifies the provider of the data; the Destination column indicates the recipient of the data. The Data and Description columns describe the data across the interface.

Table 10 – Ingest External Interfaces

Source	Destination	Data	Description
Transferring Entity Systems, User	Ingest	Transfer Request	A Transfer Request received from the transferring entity user or a transfer entity system contains the disposition agreement, retrieval requirements, security access constraints, and method of transfer.
Transferring Entity Systems, User	Ingest	Transfer	• A Transfer can be created via the Manage Transfer sub-package. • A Transfer is submitted to the Ingest system-level package where it must undergo processing before it is committed to the ERA System. • This includes Transfers via both electronic submission and physical media submission.
Transferring Entity Systems, User	Ingest	Transfer Agreement	The transfer agreement is validated against the transfer request to ensure that the transfer is authorized.
Ingest	Transferring Entity Systems, User	Transfer Authorization	After validation of Transfer Request by Ingest, this authorization instructs the source of the transfer request (Transferring Entity System or User) to initiate the transfer of records to the ERA System.
Ingest	Transferring Entity Systems, User	Status Message	• After the Transfer is created, Manage Transfer returns a status message to the transferring entity that a Transfer has been successfully created. • Validate Transfer notifies the source of the transfer of a successful transfer or any issues with the transfer, including information on quarantined records and records not ingested due to security restraints.

Table 11 – Ingest Internal Interfaces

Source	Destination	Data	Description

Source	Destination	Data	Description
Records Management	Ingest	Disposition Agreement	The Transfer is validated against the disposition agreement.
Records Management	Ingest	Template	The record's archival properties (e.g., content, context, structure, behavior, provenance, fixity, etc.) are validated against the approved templates
Ingest	Records Management	Records Life Cycle Data	Records life cycle data are included within the Transfer.
Preservation	Ingest	Records Life Cycle Data	Records life cycle data are passed back to Ingest regarding the data type validation.
Ingest	Preservation	Data File	The records are validated against the Data Types Descriptor Registry.
Ingest	LS&C	Status Message	Status messages are passed back to LS&C to be distributed to the appropriate users and/or systems
Ingest	Archival Storage	Transfer	On successful completion of Ingest processing, the Transfer is submitted to Archival Storage.
Archival Storage	Ingest	Status Message	Status messages are passed back to Ingest.

2.8.5.2.2 Ingest Logical Grouping

The Ingest logical grouping, presented in Figure 18, is summarized below in Table 12:

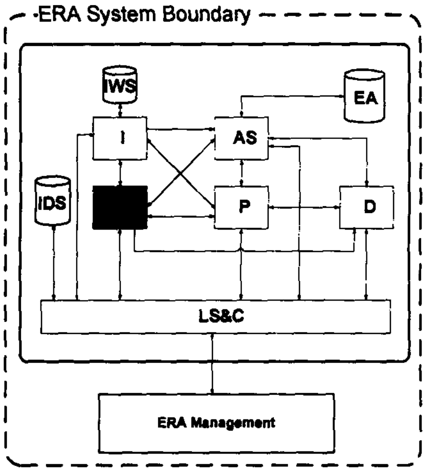
Table 12 – Ingest Groups

Group	Description
Transfer Packaging Application	The Transfer Application allows a user to package a transfer before it is ingested by ERA. A transfer container is an aggregation of files, either within a software envelope (.tar, .zip) or hardware envelope (disk, tape, CD.) The transfer created by the Transfer Application is compliant with the Transferring Entity Systems ICD. A transfer container can only contain electronic (digital) content.

Group	Description
Transfer Request Application	The Transfer Request application allows a user to create a Transfer Request, which is a request or offer from a Transferring Entity to transfer physical custody of documentary materials (Records) to NARA for archival storage. A Transfer Request could also be an agency's Request for records. This application also allows a user to submit a completed Transfer Request for approval. It also manages the workflow for approval of the Transfer Request.
Transfer Agreement Application	The Transfer Agreement application allows a user to create a Transfer Agreement, which is an agreement between NARA and a transferring entity, that specifies how the documentary materials (records) covered by disposition items will be prepared and physically transferred to NARA. Its purpose is to allow NARA to plan for the transfers that could occur in the distant future. The Transfer Agreement is used by NARA to get any software or hardware or container space required to facilitate the transfer.
Monitor Transfer Application	The Monitor Transfer application allows an authorized user to monitor the progress of a transfer during Ingest processing and views the details of an individual file. The user can also cancel the transfer as well as print out a detailed reported about a completed transfer.
Evaluate Quarantine Application	The Evaluate Quarantine application provides the users the ability to inspect, review, and take appropriate action for all potentially misclassified and virus-infected files once they have been moved to the access review quarantine location.
Process Transfer Business Process	The Process Transfer business process is a system-initiated process when a message of a received transfer is added to the Ingest Queue. This process controls ingest processing activities performed on a transfer and manages the writing of the material to archival storage. This includes creating asset catalog entries and capturing life cycle data from each step in the process.
Virus Scan Service	The Virus Scan business service scans all incoming files for viruses or malware. If a virus is detected, the file is sent to the access review quarantine location within Ingest Working Storage. In addition, the Virus Scan Business Service provides the capability to remove or eliminate a virus from a file.
Integrity Seal Service	The Integrity Seal business service which allows subsequent processes in the system to check that files are not altered after they are ingested into the ERA System applies an electronic integrity "seal" to each file being transferred.

Group	Description
Security Access Restriction Scan Service	The Security Access Restriction Scan business service examines the Security Access Level of each transferred file based upon a set of rules to verify that the data classification of the record is appropriate for the receiving ERA Instance and that no files with restricted access are transferred inappropriate for the level of system they are being ingested to. Files with potentially access restricted, inappropriate content, or undetermined Security Access Levels are sent to the access review quarantine location within Ingest Working Storage. There are currently no NARA TRM standards that specifically address scanning and checking for access restrictions. The security access restriction activities are reviewed as a part of the system Certification & Accreditation process and vulnerabilities will be judged based on the C&A process.

2.8.6 Records Management



The Records Management package provides the services necessary to manage archival properties and attributes of records and other assets, and to create and manage new versions of those assets. Records Management includes management functionality for disposition agreements, disposition instructions, appraisal, transfer agreements, templates, authority sources, asset life cycle data, descriptions, and arrangements. In addition, access review and redaction are included in Records Management because these two processes affect records' access properties and can result in the creation of new records or new versions of records.

2.8.6.1 Records Management Key Requirements

The key Records Management requirements that drive the architecture are presented in Table 13:

Table 13 - Records Management Key Requirements

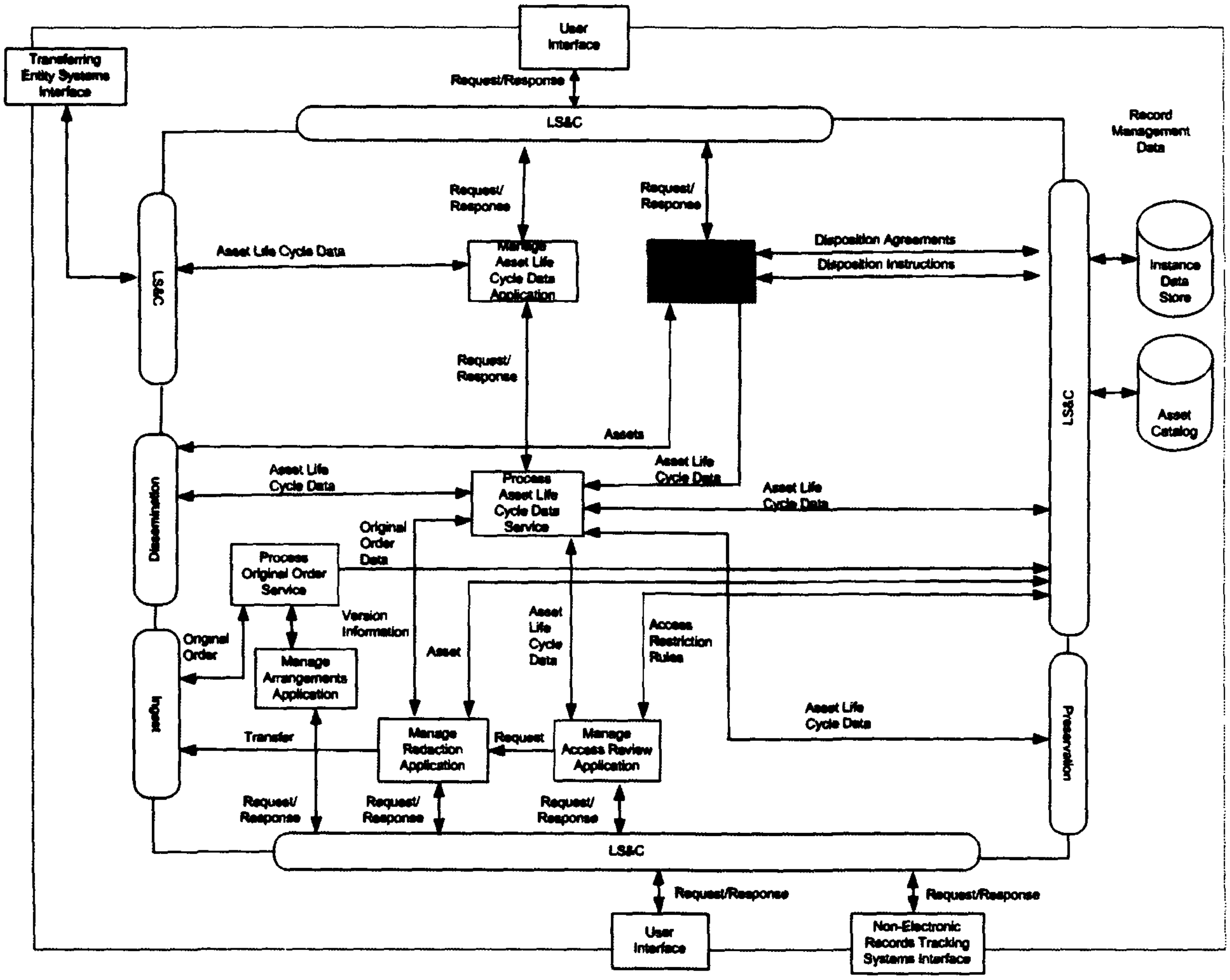
Requirement Number	Requirement	Architectural Impacts
ERA1	Manage the disposition of records	Led to the creation of the Manage Disposition Agreements application.
ERA1.11	Provide capability to appraise records	Led to the creation of the Manage Appraisals application.

Requirement Number	Requirement	Architectural Impacts
ERA3	Provide capability for descriptions	Led to the creation of the Descriptions in the Manage Disposition Agreements application.
ERA4	Manage authority sources	Led to the creation of the Manage Authority Sources.
ERA5	Provide capability to manage records life cycle data	Led to the creation of the Manage Asset Life Cycle Data application.
ERA7	Provide capability to manage templates	Led to the creation of the Manage Templates application.
ERA9	Provide capability for arrangements of electronic records	Led to the creation of the Manage Arrangements application.
ERA17	Provide capability for access review of assets	Led to the creation of the Manage Access Review application.
ERA18	Provide capability for redaction of assets	Led to the creation of the Manage Redaction.
ERA24.4, ERA24.5, ERA24.6	The system shall provide the capability to generate notices for other systems	Led to the creation of the Federal Register Notice application to provide input to the Federal Register.
ERA1.3	Provide capability to transfer legal custody of records to NARA	Led to the creation of the Manage Legal Transfer Agreements application.
ERA2.10, ERA2.11	Manage FOIA and Privacy Act requests	Led to the creation of the Manage FOIA and PA Requests.

2.8.6.2 Records Management Functional Architecture

The Records Management high-level functional architecture, shown in Figure 19, illustrates the high-level view of the Records Management system-level package. The box highlighted in gray is an aggregate of the, Manage Templates, Manage Arrangements, Process Original Order Service, Manage Descriptions, Manage Authority Sources, Manage Disposition Agreements, Manage Appraisals, Manage Legal Transfer Agreements, Manage Federal Register Notices, and Manage FOIA and PA Requests. The term, "record", is used to indicate more than one object data type for the conceptual data flow. Details for all of the Records Management logical groups can be found in Figure 19.

Figure 19 – Records Management High-Level Functional Architecture



2.8.6.3 Records Management Interfaces

The ERA System's external interfaces to and from the Records Management package, including User Interfaces through LS&C, are shown in Figure 19 and Figure 20, and identified in Table 14. The internal interfaces between Records Management and the other system-level packages, shown in Figure 19, are identified in Table 15. The Source column identifies the provider of the data; the Destination column indicates the recipient of the data. The Data and Description columns describe the data across the interface.

Figure 20 – Records Management Functional Architecture

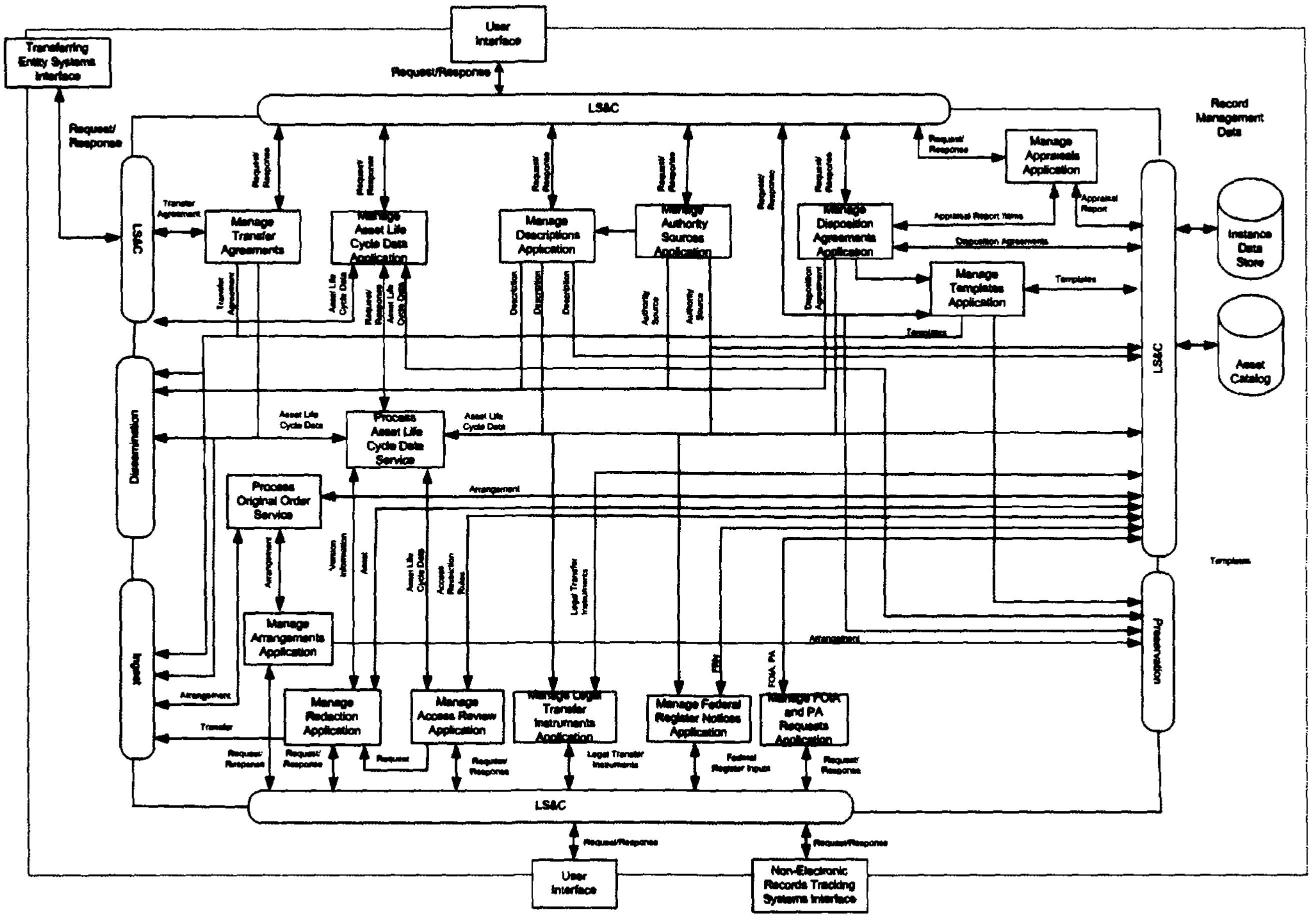

User Interface
Transferring Entity Systems Interface
Request/Response
LS&C
Request/ Response
Transfer Agreement
Manage Transfer Agreements
Manage Asset Life Cycle Data Application
Manage Descriptions Application
Manage Authority Sources Application
Manage Disposition Agreements Application
Manage Appraisals Application
Appraisal Report Items
Appraisal Report
Disposition Agreements
Manage Templates Application
Templates
Record Management Data
Instance Data Store
Asset Catalog
Asset Life Cycle Data
Description
Authority Source
Disposition Agreement
Dissemination
Process Asset Life Cycle Data Service
Process Original Order Service
Arrangement
Version information
Asset
Access Redaction Rules
Legal Transfer Instruments
Manage Arrangements Application
Ingest
Transfer
Manage Redaction Application
Manage Access Review Application
Manage Legal Transfer Instruments Application
Manage Federal Register Notices Application
Manage FOIA and PA Requests Application
FRN
FOIA, PA
Request
Federal Register Inputs
Preservation
Non-Electronic Records Tracking Systems Interface

Table 14 – Records Management External Interfaces

Source	Destination	Data	Description
User	Records Management	Request	Requests (through LS&C) to invoke services and their methods.
Transferring Entity System Interface	Records Management	Request	Transfers records and other information to the ERA System.
Non-Electronic Records Tracking Systems Interface	Records Management	Request	Submits non-electronic records tracking information to the ERA System.
Records Management	User	Response	Responses provided (through LS&C) from services to the user.
Records Management	Transferring Entity System Interface	Response	Provides status updates and other notification messages regarding transferred records.
Records Management	Non-Electronic Records Tracking Systems Interface	Response	Provides status updates and other notification messages.

Table 15 – Records Management Internal Interfaces

Source	Destination	Data	Description
Preservation	Records Management	Asset Life Cycle Data	Asset Life Cycle Data about the preservation processes conducted on a record.
LS&C	Records Management	Asset	An asset retrieved from storage in order to redact it.
Ingest	Records Management	Asset Life Cycle Data	Asset Life Cycle Data about ingested records.
Ingest	Records Management	Arrangement	An arrangement for records or other assets input to ERA through Ingest.
LS&C	Records Management	Request/Response	A request from a user forwarded to Records Management by LS&C.

Source	Destination	Data	Description
Records Management	Preservation	Asset Life Cycle Data	Asset Life cycle data that includes which appraisals and templates are associated with an asset.
Records Management	Preservation	Preservation Template	A preservation template needed for preservation processes.
Records Management	Preservation	Arrangement	An arrangement sent to Preservation in order to verify that preservation processes have not changed the logical arrangement of records.
Records Management	Preservation	Authority Sources	Authority source for record type used in the development of a Preservation and Service Plan.
Records Management	Preservation	Disposition Agreement	A disposition agreement used in the development of a Preservation and Service Plan.
Records Management	Ingest	Transfer Agreement	A transfer agreement sent to Ingest to verify that a transfer conforms to its agreement.
Records Management	Ingest	Records Template	A records template used for verification of the contents of a transfer.
Records Management	Ingest	Transfer	A Transfer containing new records created by Redaction that need to be formally introduced to the system through Ingest.
Records Management	Ingest	Arrangement	An arrangement for records or other assets input to ERA through Ingest.
Records Management	Dissemination	Asset Life Cycle Data	Asset Life cycle data containing information the system will display for the user, data on which template(s) to use for presentation, or asset Life cycle data to which a user has requested access.
Records Management	Dissemination	Authority Source	Authority source for doing controlled list searches or searches within authority sources, for building an index, or for satisfying a user's request to access an authority source.
Records Management	Dissemination	Transfer Agreement	A transfer agreement that satisfies an access request.

Source	Destination	Data	Description
Records Management	Dissemination	Arrangement	An arrangement that satisfies an access request.
Records Management	Dissemination	Description	A description that satisfies an access request.
Records Management	Dissemination	Disposition Agreement	A disposition agreement that satisfies an access request. The disposition agreement includes disposition items and disposition instructions.
Records Management	Dissemination	Appraisal Report	An appraisal report that satisfies an access request.
Records Management	Dissemination	Template	A template that satisfies an access request.
Records Management	LS&C	Asset	An asset or records associated with a redaction notice.
Records Management	LS&C	Arrangement	An arrangement sent/received for storage in the Instance Data Storage.
Records Management	LS&C	Description	A description sent/received for storage in the Instance Data Storage.
Records Management	LS&C	Authority Source	An authority source sent/received for storage in the Instance Data Storage.
Records Management	LS&C	Disposition Agreement	A disposition agreement sent/received for storage in the Instance Data Storage. Disposition agreement data may include disposition items, disposition instructions, and other associated items.
Records Management	LS&C	Appraisal Report	An appraisal report sent/received for storage in the Instance Data Storage.
Records Management	LS&C	Asset Life Cycle Data	Asset life cycle data sent/received for storage in the Instance Data Storage.
Records Management	LS&C	Template	A template sent/received for storage in the Instance Data Storage.
Records Management	LS&C	Legal Transfer Instrument	A Legal Transfer Instrument request sent/received for storage in the Instance Data Storage.

Source	Destination	Data	Description
Records Management	LS&C	Federal Register Notice Abstract	A Federal Register Notice Abstract sent for storage in the Instance Data Storage and exported from ERA for input to the Federal Register.
Records Management	LS&C	FOIA or PA Request	A FOIA or Privacy Act request sent/received for storage in the Instance Data Storage.
Records Management	LS&C	Request/Response	Responses from services sent/received to LS&C to forward to the user.

2.8.6.3.1 Records Management Logical Grouping

The Records Management logical grouping, presented in Figure 20, is summarized in Table 16 below:

Table 16 – Records Management Groups

Group	Description
Manage Disposition Agreements Application	• The Manage Disposition Agreement application provides the capability to manage disposition agreements, disposition items, disposition instructions and disposition agreement packages. Processes in the Manage Disposition Agreement application allow users to create, update, or delete disposition items within disposition agreements. • The Manage Disposition Agreements application manages disposition instructions for invocating periodic access review, destruction, and expungement of records and assets. It also interfaces to tools that support monitoring and assess the carrying out of disposition instructions. • The Manage Disposition Agreements application communicates with an LS&C interface to access the Instance Data Storage to store and retrieve disposition agreements. This application also obtains templates from Manage Templates and provides asset life cycle data to the Process Asset Life Cycle Data service for input to Instance Data Storage. Users can interact with Manage Disposition Agreements via LS&C interfaces, and can leverage collaboration tools within that system-level package.

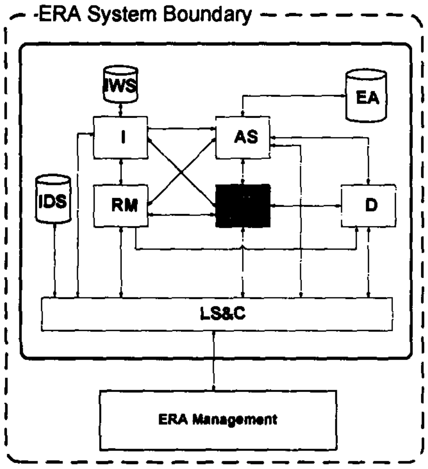
Group	Description
Manage Appraisals Application	• The Manage Appraisals application provides the primary tools that Appraiser users employ. It allows the creation, access, modification, and deletion of appraisal report items. It also provides the capability to compile an appraisal report, which is the sum of all appraisal report items associated with disposition items within a particular disposition agreement. • Manage Appraisals interacts with users through LS&C. Appraisal report items and a Disposition Agreement level appraisal information will be stored in the Instance Data Storage through LS&C with an association to a Disposition Agreement.
Manage Authority Sources	• The Manage Authority Sources provides the services for creating, modifying, accessing, and deleting authority sources. This data is then shared with description, life cycle, and dissemination functions in order to provide standard ways to reference controlled ontologies for people, places, and organizations. • The Manage Authority Sources provides data to the Dissemination system-level package. It stores its data through LS&C to the Instance Data Storage. Users can interact with Manage Authority Sources through LS&C.
Manage Asset Life Cycle Data Application	• The Manage Asset Life Cycle Data application provides the capability for users to create, update and delete asset life cycle data framework and extracts asset life cycle data from and associates this data with records, templates, and disposition agreements. In addition, this application also allows managing metadata, as specified by NARA policy. • The Manage Asset Life Cycle Data application invokes the Process Asset Life Cycle Data business service to access and store asset life cycle data in the Asset Catalog.
Manage Templates Application	• The Manage Templates application provides the capability to create, update, delete and store business and non-business templates. Records templates will be chiefly employed within Records Management and Ingest, presentation templates will be used in Dissemination, and preservation templates will be used in Preservation services. • Users perform template management through an LS&C interface. Manage Templates interfaces with the Instance Data Storage through LS&C.

Group	Description
Manage Arrangements Application	- The Manage Arrangements application provides the capability to create and manage the original order for records and assets. The initial original order and subsequent for records and assets are stored within the Asset Catalog. As new arrangements for records or assets are defined or existing arrangements are modified, Manage Arrangements invokes the Process Original Order Service to save the original order in the Asset Catalog. - Users can interface with Manage Arrangements through LS&C. Manage Arrangements also interacts with Preservation.
Manage Access Review Application	- The Manage Access Review application provides the capability for NARA personnel to conduct security access reviews on assets and change access restrictions if required. Initial access restrictions are provided by Transferring Entities. Processes in the Manage Access Review application allow users to review, approve or modify access restrictions. - Manage Access Review can generate requests for the Redaction application. Users can interact with Access Review through LS&C. The results of access review processes are sent to Manage Asset Life Cycle Data for association with records and storage.
Manage Redaction	- The Manage Redaction provides a framework and services for redaction capabilities on different record types and data types. The system employs the framework to determine which service to invoke depending on the record attributes and the user preferences and capabilities. Redaction is invoked by a request from the Manage Access Review application. - Redaction receives requests from the Manage Access Review application and retrieves copies of the assets for redaction from Archival Storage. Users can provide input to Manage Redaction through an LS&C interface. Upon completing, Manage Redaction builds a Transfer for the redacted assets and forwards it to the Ingest package for formal entry into the ERA System. It also informs Manage Asset Life Cycle Data within Records Management in order to associate the new asset with the original version.

Group	Description
Manage Legal Transfer Instruments Application	• The Manage Legal Transfer Instruments application provides the capability to manage LTI associated with the transfer of records and assets to NARA. The processes in the Manage Legal Transfer Instruments application allow users to create, update and store a LTI. • Manage Legal Transfer Instruments receives requests from users through an LS&C interface and utilizes a different LS&C interface to store them with their statuses in the Instance Data Storage.
Manage Federal Register Notice Application	• The Manage Federal Register Notices application provides the capability to manage generation of NARA ERA inputs to the Federal Register. The processes in the Manage Federal Register Notices application allow users to access and create Federal Register input from templates. • Manage Federal Register Notice receives requests from users through an LS&C interface and utilizes a different LS&C interface to store them with their statuses in the Instance Data Storage.
Manage FOIA and PA Requests	• The Manage FOIA and PA Requests provides tools to track and manage requests made under the Freedom of Information Act and the Privacy Act. Its responsibility will be to monitor and update the status of each request. • Manage FOIA and PA Requests receives requests from users through an LS&C interface and utilizes a different LS&C interface to store them with their status in the Instance Data Storage.

Group	Description
Process Asset Life Cycle Data Service	• The Process Asset Life Cycle Data service processes asset life cycle metadata associated with records, templates, disposition agreements, other ERA assets and as specified by ERA policy. In addition, it provides asset life cycle data to the Dissemination system-level package and interacts with users through an LS&C interface to provide asset life cycle data management functions. • Process Asset Life Cycle Data controls asset life cycle data built from information provided by the Manage Transfer Agreements, Manage Templates, Manage Disposition Agreements and other Records Management applications.. The Preservation system-level package also provides data to this service for asset life cycle data extraction related to preservation activities while receiving asset life cycle data to support its own processes. The Process Asset Life Cycle Data service sends metadata to LS&C to store as asset life cycle data in the Asset Catalog and associates this data to records and assets managed by ERA. • The Asset Catalog holds asset life cycle data associated with assets in the ERA System. Descriptions are managed consistently across all assets and serves as a search and performance cache for the ERA System components.
Process Original Order Service	• The Process Original Order Service provides the services to set, save and update the original order for records in the Asset Catalog. Only one original order will be maintained for a set of records or assets at any time. • This service is invoked by applications to access, save or update original order information.

2.8.7 Preservation



The Preservation system-level package provides services to manage the preservation of electronic records ensuring their continued existence, accessibility, and authenticity over time. Preservation provides management functionality for preservation assessments, Preservation and Service Plans, authenticity assessment and digital adaptation of electronic records. Additional management functionality is provided for data type descriptors and digital adaptation descriptors.

The Preservation system-level package provides functionality for handling requests for digital adaptation of records at any point in their life cycle. Request can be made as part of routine preservation processing or on-demand for presentation purposes. Users will be able to make an assessment of the authenticity of both the digital adaptation processor and their products

In addition to providing preservation processing services, the Preservation system-level package includes services for file data type identification and attributes extraction to add to records life cycle data.

2.8.7.1 Preservation Key Requirements

The key Preservation requirements and functionality that drive the architecture are presented in Table 17:

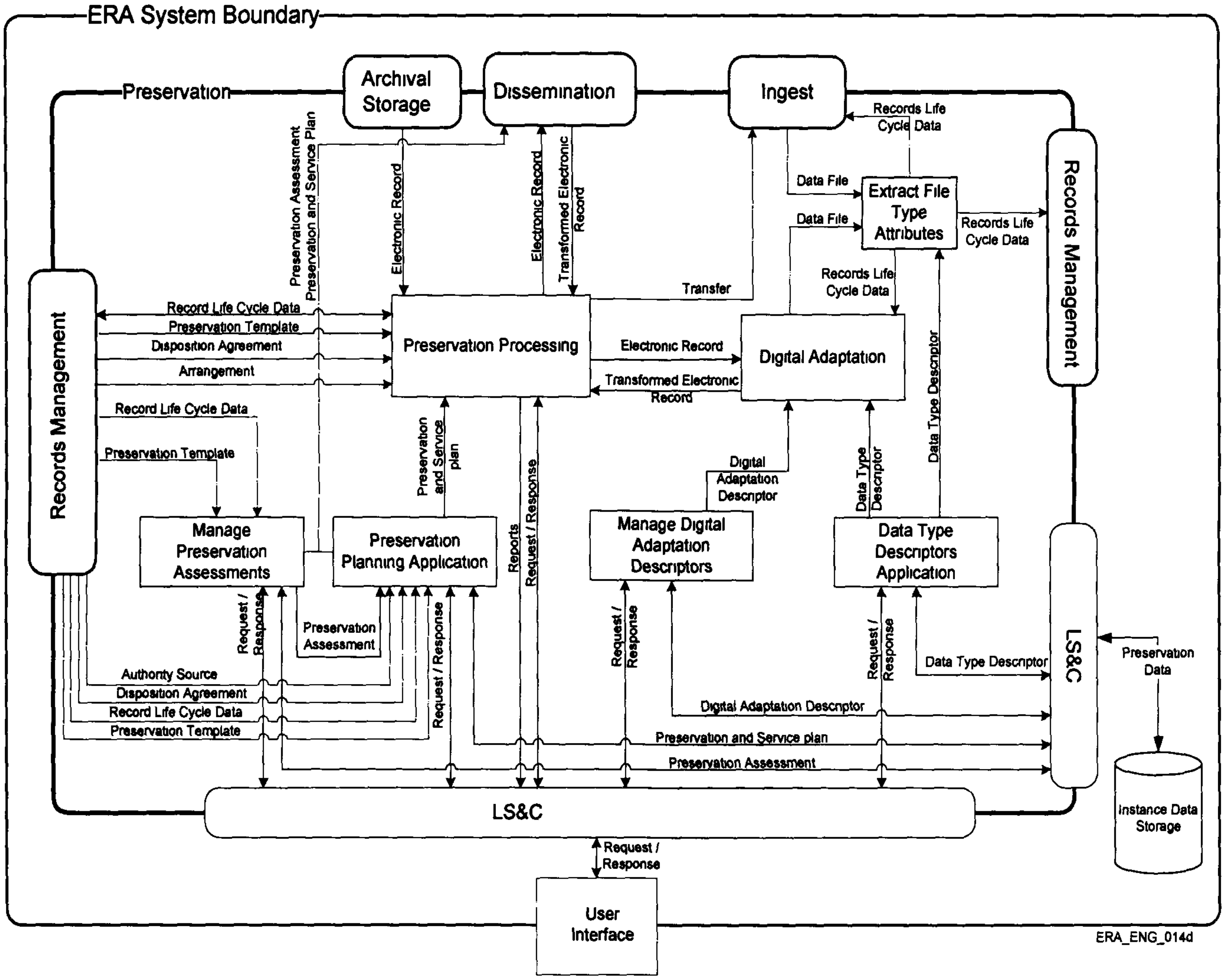
Table 17 – Preservation Key Requirements

Requirement Referenced	Requirement	Architectural Impact
ERA8	Preservation of electronic records	Led to the creation of the Preservation system-level package.
ERA8.1	Manage the preservation processing of electronic records	Led to the creation of Preservation Processing to centralize all preservation processing services.
ERA8.1.1	Provide the capability for preservation assessments	Led to the creation of the Manage Preservation Assessments.
ERA8.1.2, ERA8.1.3	Queue and initiate preservation processing	The capabilities to queue and initiate preservation processing are included in the Preservation Processing.
ERA8.3	Extract data file attributes	Led to the creation of the Extract File Type Attributes service for providing data file identification and attribute extraction.
• ERA8.5, ERA18.6 • ERA8.26	• Perform digital adaptation • Provide a registry of digital adaptation descriptors	Led to the creation of a framework for providing access to digital adaptation engines, the Digital Adaptation, and to manage a registry of digital adaptation descriptors, Manage Digital Adaptation Descriptors.
ERA8.9	Support preservation planning	Led to the creation of the Preservation Planning application.
ERA8.10	Provide a registry of data type descriptors	Led to the creation of an application to manage the registry of data type descriptors, Data Type Descriptors.

2.8.7.2 Preservation Functional Architecture

The Preservation functional architecture, shown in Figure 21, illustrates: (1) the ERA System's external interfaces to the Preservation system-level package; (2) the internal system-level package interfaces to and from Preservation; (3) the Preservation logical grouping; and (4) the conceptual data flow of the Preservation system-level package.

Figure 21 – Preservation Functional Architecture



Note: An access to Archival Storage is through the Storage Federator service of LS&C.

2.8.7.2.1 Preservation Interfaces

The ERA System's external interfaces to and from the Preservation package, including User Interfaces through LS&C are shown in Figure 21 and identified in Table 18. The internal interfaces between Preservation and the other system-level packages, also shown in Figure 21, are identified in Table 19. The Source column identifies the provider of the data; the Destination column indicates the recipient of the data. The Data and Description columns describe the data across the interface.

Table 18 – Preservation External Interfaces

Source	Destination	Data	Description
User	Preservation	Requests	Requests via LS&C for invocation of preservation service methods.
Preservation	User	Response	Responses from the invocation of preservation service methods. Responses may implicitly include serialized records or references to data objects.

Table 19 – Preservation Internal Interfaces

Source	Destination	Data	Description
Records Management	Preservation	Record Life Cycle Data	• Records life cycle data relating to the electronic record(s) undergoing preservation processing. • Also required for the generation of preservation assessments and Preservation and Service Plans.
Records Management	Preservation	Preservation Template	A preservation template required for the generation of a Preservation and Service Plan, and for preservation processing.
Records Management	Preservation	Arrangement	An arrangement required to verify that preservation processes have not changed the logical arrangement of electronic records.
Records Management	Preservation	Authority Source	Authority Sources for defining preservation processes, such as data type names, essential characteristics taxonomies, etc.
Records Management	Preservation	Disposition Agreement	Disposition Agreement used for preservation processing.
Ingest	Preservation	Data Files	A record with associated data files that require attribute extraction and type identification.
Archival Storage	Preservation	Electronic Record	An existing electronic record that requires digital adaptation or preservation processing.

Source	Destination	Data	Description
Dissemination	Preservation	Electronic Record	A record that requires digital adaptation for presentation purposes.
LS&C (Instance Data Storage)	Preservation	Digital Adaptation Descriptor	An existing digital adaptation descriptor required either for preservation processing, or for update as part of the management service.
LS&C (Instance Data Storage)	Preservation	Preservation and Service Plan	An existing Preservation and Service Plan required either for preservation processing, or for update as part of the management service.
LS&C (Instance Data Storage)	Preservation	Data Type Descriptor	An existing data type descriptor required either for preservation processing, for use in the data file identification, or for update as part of the management service.
LS&C (Instance Data Storage)	Preservation	Preservation Assessment	An existing preservation assessment required for preservation processing or planning.
Preservation	Records Management	Record Life Cycle Data	• Updated records life cycle data relating to electronic record(s) that have undergone preservation processing. • Updated records life cycle data relating to the extraction of file type attributes.
Preservation	Ingest	Record Life Cycle Data	Record Life Cycle Data containing extracted file attributes.
Preservation	Ingest	Transfer	The output from a digital adaptation of electronic records in the form of a Transfer. This is sent to Ingest, with Preservation acting as a transferring entity. The Transfer will indicate that these are not new records.
Preservation	Dissemination	Transformed Electronic Record	The output for a digital adaptation of an electronic record for presentation purposes.
Preservation	LS&C	Reports	Reports on the characteristics of preservation processing.
Preservation	LS&C (Instance Data Storage)	Digital Adaptation Descriptor	A new or updated Digital Adaptation Descriptor sent for storage in the Instance Data Storage.
Preservation	LS&C (Instance Data Storage)	Preservation and Service Plan	A new or updated Preservation and Service Plan sent for storage in the Instance Data Store.
Preservation	LS&C (Instance Data Storage)	Data Type Descriptor	A new or updated Data Type Descriptor sent for storage in the Instance Data Storage.

Source	Destination	Data	Description
Preservation	LS&C (Instance Data Storage)	Preservation Assessment	A new or updated Preservation Assessment sent for storage in the Instance Data Storage.
Preservation	LS&C	Response	A status response to a request for preservation processing.
LS&C	Preservation	Request	A request for preservation processing.

2.8.7.2.2 Preservation Logical Grouping

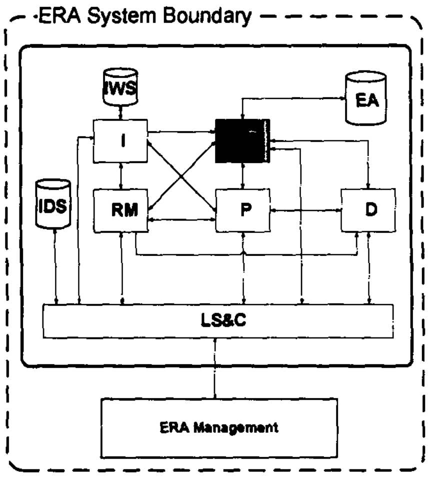
The Preservation logical grouping, presented in Figure 21, is summarized in the table below:

Table 20 – Preservation Logical Grouping

Group	Description
Preservation Processing	• The Preservation Processing contains services to manage the digital adaptation of data types. Functionality will include the ability for a user to request individual digital adaptations, or to schedule a unit of work. Digitally adapted records (excluding digital adaptations for presentation only) are sent as a transfer to the Ingest system level package for ingest into archival storage. • Preservation Processing provides functionality to verify and report on the results of digital adaptation on content, structure and behavior. • Also included are services to allow a user to make an assessment of the authenticity of records that have undergone the digital adaptation process.
Digital Adaptation	• The Digital Adaptation provides a framework for digital adaptation engines as defined in the digital adaptation descriptors. The framework includes functionality to determine the appropriate digital adaptation engine to use during preservation processing, based on the record attributes and the capability of a digital adaptation engine. In essence the service is a Façade pattern to each of the digital adaptation engines within the framework. • It provides for an extensible capability for digital adaptation where new engines can be added to the framework as and when they become available.
Manage Preservation Assessments	Preservation assessments involve the review of electronic records to determine the potential need for preservation and may be conducted at any point in the records life cycle. Services are provided for the creation, retrieval, modification, and deletion of a preservation assessment. Inputs to the services include preservation templates and record life cycle data. Preservation assessments are subsequently used in the creation of a Preservation and Service Plan.

<table>
<tr><th>Group</th><th>Description</th></tr>
<tr><td>Data Type Descriptors (DTD) Application</td><td>Decomposed into ten processes:
<table>
<tr><th>Process Name</th><th>Description</th></tr>
<tr><td>Create DTD</td><td>Provides the user the capability to create, delete, update, associate, and verify DTD</td></tr>
<tr><td>Create Data Type Template</td><td>Provides the user the capability to create, delete, and update Data Type Templates</td></tr>
<tr><td>Create Application Profile</td><td>Provides the user the capability to create, delete, update, and associate Application Profiles</td></tr>
<tr><td>Create Vendor Profile</td><td>Provides the user the capability to create, delete, update, and associate Vendor Profiles</td></tr>
<tr><td>Search DTD</td><td>Provides the user the capability to search for DTD(s)</td></tr>
<tr><td>Search Data Type Template</td><td>Provides the user the capability to search for Data Type Template(s)</td></tr>
<tr><td>Search Application Profile</td><td>Provides the user the capability to search for Application Profile(s)</td></tr>
<tr><td>Search Vendor Profile</td><td>Provides the user the capability to search for Vendor Profile(s)</td></tr>
<tr><td>Browse DTD</td><td>Provides user the capability to browse inventory of DTD(s)</td></tr>
<tr><td>Browse Data Type Template</td><td>Provides user the capability to browse inventory of Data Type Template(s)</td></tr>
</table></td></tr>
<tr><td>Preservation Planning Application</td><td>Decomposed into two processes:
<table>
<tr><th>Process Name</th><th>Description</th></tr>
<tr><td>Create PSP</td><td>Provides the user the capability to create, delete, update, and associate Preservation & Service Plan (PSP)</td></tr>
<tr><td>Search PSP</td><td>Search PSP- Provides the user the capability to search for PSP(s.)</td></tr>
</table></td></tr>
<tr><td>Manage Digital Adaptation Descriptors</td><td>The Manage Digital Adaptation Descriptors contains services for the creation, retrieval, modification and deletion of digital adaptation descriptors that describe the engines used in the digital adaptation framework.</td></tr>
<tr><td>Extract File Type Attributes Service</td><td>Services are provided for the identification and extraction of data file attributes. This includes the identification of the data type itself. These services are normally called from the Ingest system-level package during the validation of a transfer; however, they have been included here to be available during the digital adaptation process.</td></tr>
</table>

2.8.8 Archival Storage



The Archival Storage system-level package abstracts the details of mass storage from the system-level packages. This abstraction allows the Archival Storage system-level package to be scaled and new technology introduced independent of the other packages according to NARA's business requirements. The services in the Archival Storage system-level package are the storing and management of the assets and the automated handling and management of the removable media.

2.8.8.1 Archival Storage Key Requirements

The key Archival Storage requirements and functionality that drive the architecture are presented in the table below:

Table 21 – Archival Storage Key Requirements

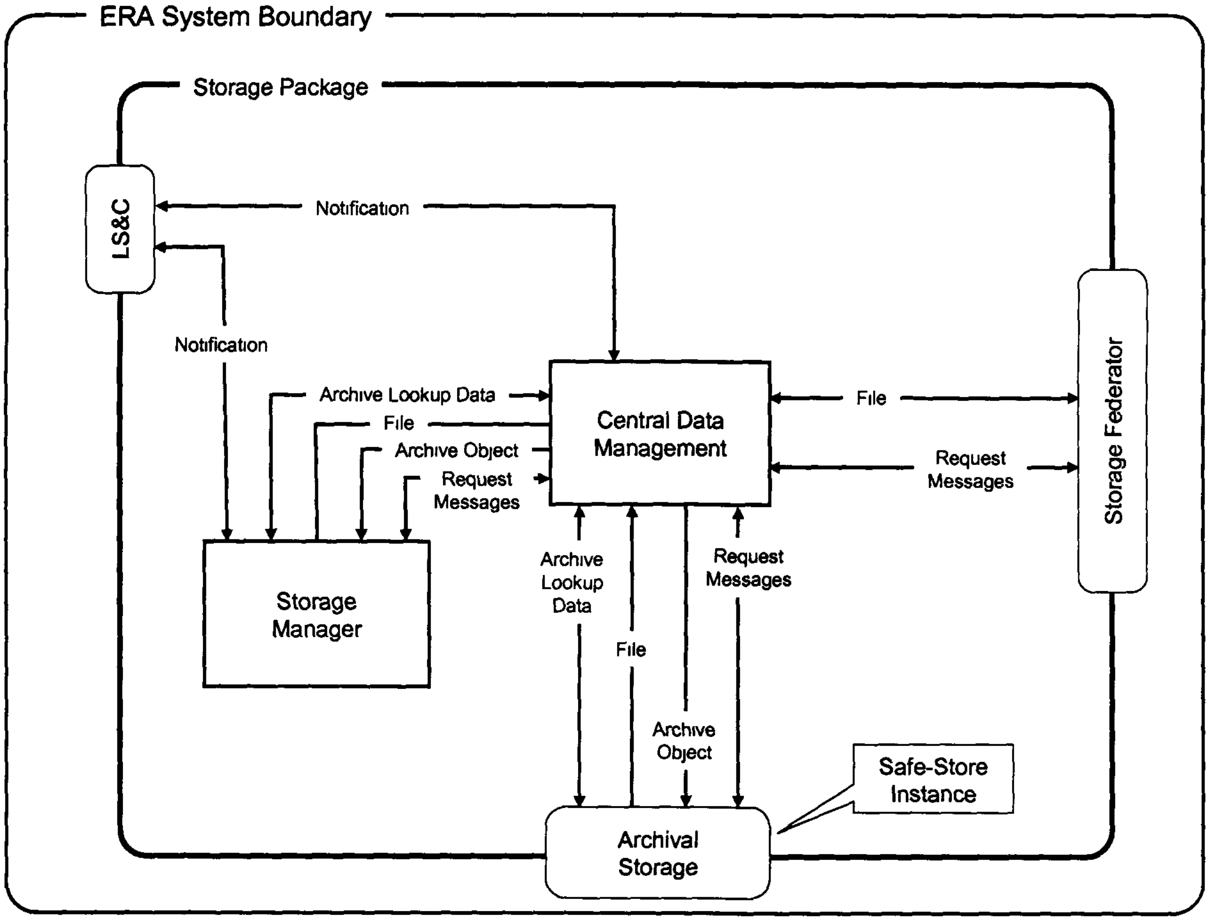
Requirement Referenced	Requirement	Architectural Impact
ERA10.1	The capability to store copies of all electronic records	Led to the creation of a scalable and extensible solution.
ERA10.1.4	The capability to store a duplicate copy of an asset at another ERA site	Led to the creation the Active Safe-Store architecture.
ERA10.2.4	Location-transparent access to electronic assets.	Led to a solution with a virtual file system interface.
ERA11.3	Automated access to information stored on removable archive media	Led to the storage management application that abstracts removable media libraries.
ERA12.1	Automated movement of electronic records to different media to accommodate new technology.	Led to a solution that is not storage media or supplier dependent.
ERA31.2	The Active Safe-Store architecture is scaleable to 1 exabyte	Led to a scalable and extensible solution.

Requirement Referenced	Requirement	Architectural Impact
ERA31.3	The Active Safe-Store architecture is scaleable to 10 teraobjects	Led to a scalable and extensible solution.

2.8.8.2 Archival Storage Functional Architecture

The Archival Storage functional architecture, shown in Figure 22 illustrates: (1) the internal system-level package interfaces to and from Archival Storage; (2) the Archival Storage services; and (3) the conceptual data flow of the Archival Storage system-level package. There are no ERA System external interfaces to Archival Storage; this ensures the integrity, authenticity, and security of the electronic archives.

Figure 22 – Archival Storage Functional Architecture



2.8.8.2.1 Archival Storage Internal Interfaces

The internal interfaces between Archival Storage and the system-level packages, shown in Figure 22, are identified in Table 22. The Source column identifies the provider of the data; the Destination column indicates the recipient of the data. The Data and Description columns describe the data across the interface.

Table 22 – Archival Storage Internal Interfaces

Source	Destination	Data	Description
LS&C	Archival Storage	Notification	Management and control messages
Storage Federator	Archival Storage	Files	Storage of files and retrieval of copy of a file
Storage Federator	Archival Storage	Request Messages	Request for a file
Archival Storage (Safe-Store Instance)	Archival Storage	Archive Lookup Data	Locator data for requested file
Archival Storage (Safe-Store Instance)	Archival Storage	Files	Retrieval of copy of a file
Archival Storage	LS&C	Notification	Management and control messages
Archival Storage	Archival Storage (Safe-Store Instance)	Archive Lookup Data	Storage of Archive Lookup Data
Archival Storage	Archival Storage (Safe-Store Instance)	Archive Objects	Storage of Archive Objects
Archival Storage	Archival Storage (Safe-Store Instance)	Request Messages	Request for a file

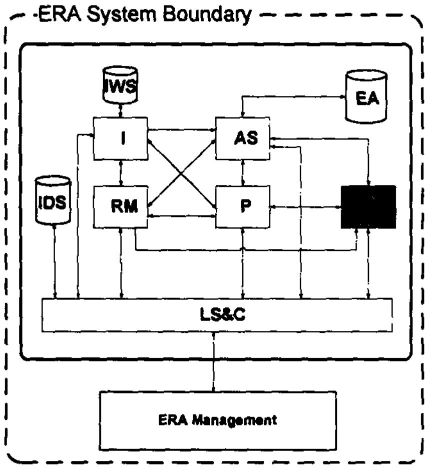
2.8.8.2.2 Archival Storage Services

The Archival Storage services, presented in Figure 22, are summarized in Table 23:

Table 23 – Archival Storage Services

Services	Description
Central Data Management	• Central Data Management controls the storage and access of all assets. Central Data Management provides a consistent location-transparent interface for receiving and disseminating assets. • Central Data Management writes an Archive Object to the Storage Manager at the primary store and the Safe-Store. • If a requested asset is located in the performance cache, Central Data Management will copy the asset directly from the cache. If the Archive Object containing the asset has been transferred to the Storage Manager then Central Data Management will issue a request to the primary store's Storage Manager for a copy of the asset. If the primary store is unavailable or if the asset is not in the primary store, then Central Data Management will issue a request to the Safe-Store's Storage Manager for a copy of the asset.
Storage Manager	• The Storage Manager abstracts the details of the physical mass storage and provides the management services for the storage media. The abstraction of the physical storage provides the ability to add new mass storage technology without affecting production. • Upon receiving a request for an asset from the Central Data Management the Storage Manager will copy the asset from the storage media, verify the copy of the asset and transfer the copy to the Central Data Management.

2.8.9 Dissemination



The Dissemination system package provides functionality to manage search and access requests for assets within the ERA System. Users have the capability to generate search criteria, execute searches, view search results, and select assets for output or presentation. The architecture provides a framework to enable the use of multiple search engines offering a rich choice of searching capabilities across assets and their contents.

Functionality also exists for the management of the search indices, which includes entity extraction tools to assist in content index creation.

2.8.9.1 Dissemination Key Requirements

The key Dissemination requirements and functionality that drive the architecture are presented in the table below:

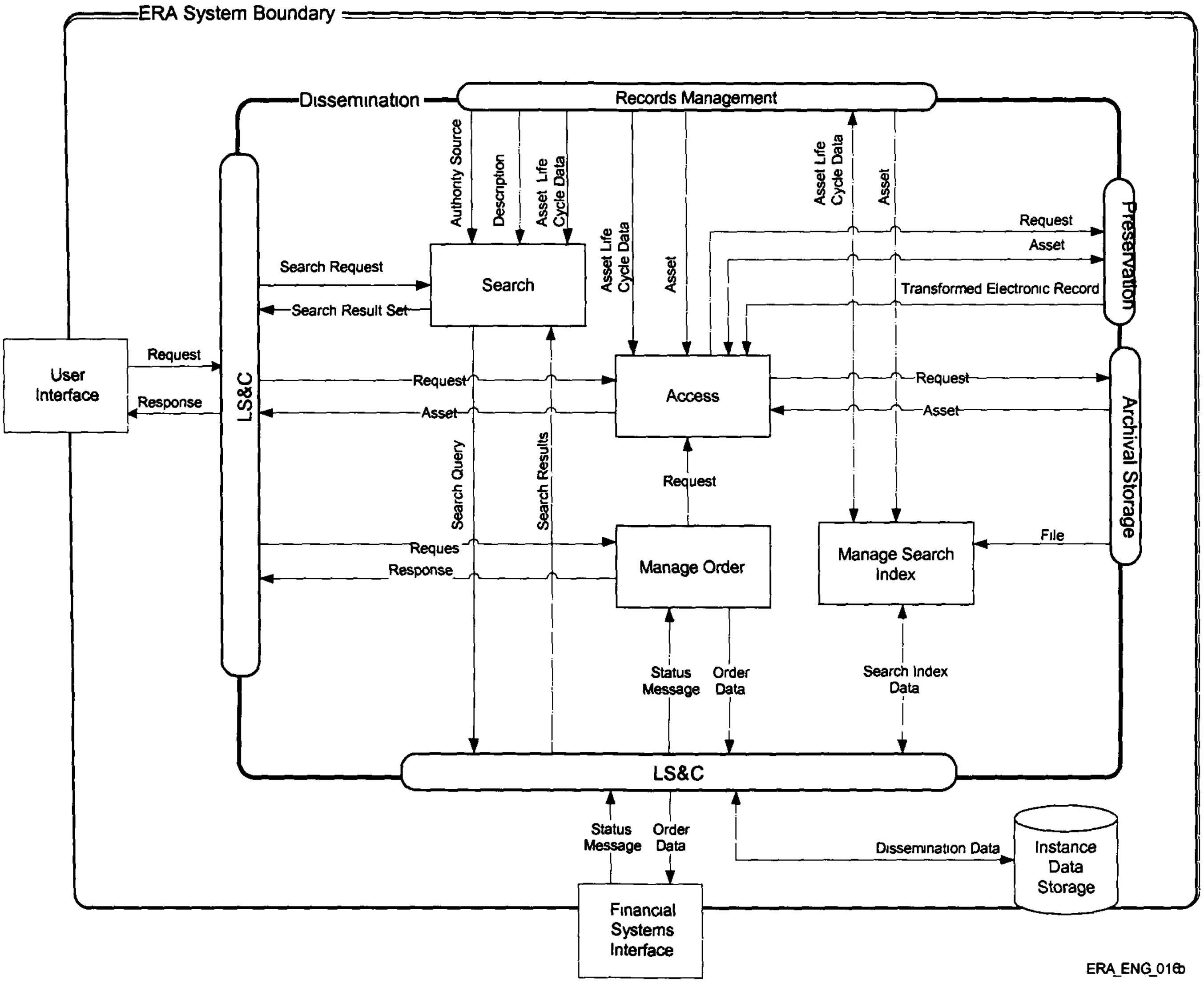
Table 24 – Dissemination Key Requirements

Requirement Referenced	Requirement	Architectural Impact
ERA19	The system shall provide the capability to search the assets it contains	Led to the creation of sets of services to manage the search of assets.
ERA19.1. ERA19.3, ERA19,4, ERA19.5, ERA19.9 ERA19.11	Creation of search criteria	Led to the creation of the Search to provide searching functionality and Manage Search Index to manage indices to support criteria-based searching.
ERA19.2, ERA19.7	Content searching	Led to the creation of the Manage Search Index to manage indices to support content-based searching
ERA19.8, ERA19.12	Presentation of search results	Led to the creation of the Search to manage the presentation and persistence of search results to the user.
ERA20.1, ERA20.2, ERA20.3	Presentation and output of assets	Led to the creation of the Access providing access to assets. It will provide functionality to handle requests for both the presentation and output of assets.
ERA20.4, ERA20.5	Asset access independent of creation hardware and software.	Led to interface between Dissemination services with the Digital Adaptation services in the Preservation system-level package.

2.8.9.2 Dissemination Functional Architecture

The Dissemination functional architecture, shown in Figure 23, illustrates: (1) the ERA System's external interfaces to the Dissemination system-level package; (2) the internal system-level package interfaces to and from Dissemination; (3) the Dissemination logical grouping; and (4) the conceptual data flow of the Dissemination system-level package. The architecture supports requests for ERA System assets from users and prepares the returned assets for presentation or output to the users.

Figure 23 – Dissemination Functional Architecture



Note: An access to Archival Storage is through the Storage Federator service of LS&C.

2.8.9.2.1 Dissemination Interfaces

The ERA System's external interfaces to and from the Dissemination package, including User Interfaces through LS&C are shown in Figure 23 and identified in Table 25 – Dissemination External Interfaces. The internal interfaces between the ERA System-level packages, also shown in Figure 23, are identified in Table 26 – Dissemination Internal Interfaces. The Source column identifies the provider of the data; the Destination column indicates the recipient of the data. The Data and Description columns describe the data across the interface.

Table 25 – Dissemination External Interfaces

Source	Destination	Data	Description
User	Dissemination	Request	Requests via LS&C for invocation of Dissemination service methods. User requests include: a search request, a request to access an asset either through presentation or output and an order request.
Dissemination	User	Response	Responses from a service invoked within Dissemination. Responses can include: a set of search results, and output/presentation of a requested asset.
Dissemination	Financial Systems Interface	Order Data	Order information, which can contain billing information, product order information, and service order information.
Financial Systems Interface	Dissemination	Status Message	• Message indicates to Dissemination to either fulfill or deny an order request. • This message may also relate to an order that was created outside of the ERA System.

Table 26 – Dissemination Internal Interfaces

Source	Destination	Data	Description
Records Management	Dissemination	Asset	• Requires access to all assets managed by the Records Management system-level package, for fulfillment of user access requests. • Asset in this case includes: – Disposition agreements – Disposition instructions – Templates – Appraisal Reports – Arrangements – Descriptions – Records Life Cycle Data
Records Management	Dissemination	Records Life Cycle Data	Used in the generation of an informative search result set or to determine available options for output and presentation.

Source	Destination	Data	Description
Records Management	Dissemination	Description	Required when presenting search results to the user.
Records Management	Dissemination	Authority source	Required during the generation of search criteria.
Preservation	Dissemination	Asset	• Requires access to all assets managed by the Preservation system-level package, for fulfillment of user access requests. • Asset in this case includes: – Preservation Assessments – Preservation and Service Plans
Preservation	Dissemination	Transformed Electronic record	A copy of an asset transformed by a preservation process so that it can be presented to the user.
Archival Storage	Dissemination	File	A copy of a file retrieved from Archival Storage. Used for both delivery to a user to fulfill an access request, and for the generation of content-based search indices.
LS&C	Dissemination	Request	A user request for access to an asset or set of assets. A user request for an order of assets.
LS&C	Dissemination	Search Request	A user request for a search of assets.
LS&C	Dissemination	Status Message	A status message from the external financial system related to order fulfillment.
LS&C	Dissemination	Search Index Data	Search index data for use by the Manage Search Index.
LS&C	Dissemination	Search Results	A set of search results passed to the Search. Contains a set of record identifiers that match the search criteria.
Dissemination	LS&C	Search Query	A set of user search criteria to be retrieved from the Instance Data Store.
Dissemination	Records Management	Records Life Cycle Data	Updates to Record Life Cycle Data resulting from entity extraction.
Dissemination	Preservation	Request	A request for an asset managed by the Preservation package.

Source	Destination	Data	Description
Dissemination	Preservation	Asset	A record that needs to undergo digital adaptation in order to be presented.
Dissemination	Archival Storage	Request	A request for an asset in Archival Storage.
Dissemination	LS&C (Instance Data Storage)	Search Index Data	Search index data for use by the Manage Search Index held in the Instance Data Store.
Dissemination	LS&C	Search Query	• A search query to be made against the search indices. • A set of user search criteria to be persisted in the Instance Data Store.
Dissemination	LS&C	Search Result Set	A set of user search results to be persisted in the Instance data store.
Dissemination	LS&C	Order Data	Order data to be sent to the external financial systems.
Dissemination	LS&C	Response	A response to user requests made to the Manage Order.

2.8.9.2.2 Dissemination Logical Grouping

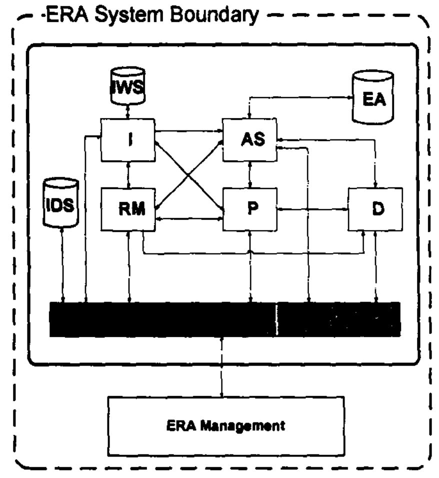
The Dissemination logical grouping, presented in Figure 23, is summarized in the table below:

Table 27 – Dissemination Logical Grouping

Group	Description
Search	• The Search contains the functionality for conducting a search against the assets within the ERA System. Capability is provided for a user to specify and save the search criteria, execute searches against a number of indices (including content indices), present search results to the user, and save the search results for future use. • The functionality permits users to determine the complexity of their search, and offers the flexibility to satisfy the needs of many different types of users. Authority sources can be used as input to the search criteria. • A framework of search engines provides the execution of Search This allows a best-fit search engine to be used depending upon the nature of the user's query. For example a search of the contents of assets will require a different approach as opposed to a search against descriptions. The framework includes the functionality to choose the most appropriate search engine for any set of search criteria. Federated searches and federated content searches are provided at a single classification level and run when an authorized user chooses to make a search federated or when the search

Group	Description
	framework determines that a federated search is appropriate to fulfill a search request. Requests are distributed to the participating Instances via LS&C. • Search is supported by two application processes, each consisting of a single task. – Metadata Search – Browse Asset Catalog • Search is also supported by business service functionality consisting of two services to provide the mechanism for searching. – Search Framework – Metadata Search
Access	• The Access provides the functionality to present and output copies of assets to a user. Functionality includes the ability to offer a user a range of output options, including media (e.g., CD-ROM) or electronic for download, and format options (as applicable). The package also includes any tools that are required in order to present assets electronically. The group interfaces to all other system-level packages that have the responsibility for the management of assets including Archival Storage. Although retrieval is location transparent with the Dissemination system-level package, the services within LS&C and Archival Storage that the Access calls enable federated retrieval across ERA Instances within a classification level. An interface to the Preservation system-level package is included for on-demand digital adaptation of assets for presentation purposes. • Media production functionality is also included to fulfill any requests for assets output to media.
Manage Order	The Manage Order contains the functionality for a user to create an order within the ERA System, capture and exchange order and billing information with external systems, and fulfill order requests by interfacing with the Access group.
Manage Search Index	The Manage Search Index contains the functionality for the management of all the search-related indices within the ERA System. This includes description indices, asset content indices, and any indices of records life cycle data. Functionality exists to create indices based upon entity extraction and parsing of asset content.

2.8.10 Local Services and Control



The Local Services and Control (LS&C) system-level package provides the physical network connectivity to an ERA Instance from users, other NARA systems, and external interfaces, as well as the interfaces between ERA Instances. LS&C provides the first layers of the ERA System security defense-in-depth. Network security includes firewalls, intrusion detection systems, and auditing at the network interface.

The LS&C system-level package provides a portal-based interface for the ERA System users. Users access their workbenches, including access to assets and services, according to their roles and authorizations. Security services invoked by the portal include the Directory Service for user identification, authentication, and authorization.

The LS&C system-level package includes the service-based interfaces and queues to orchestrate workflows using services from the Ingest, Records Management, Preservation, Archival Storage, and Dissemination system-level packages.

2.8.10.1 LS&C Key Requirements

The key LS&C requirements and functionality that drive the architecture are presented in Table 28.

The LS&C system-level package includes the service-based interfaces and queues to orchestrate workflows using services from the Ingest, Records Management, Preservation, Archival Storage, and Dissemination system-level packages.

Table 28 – LS&C Key Requirements

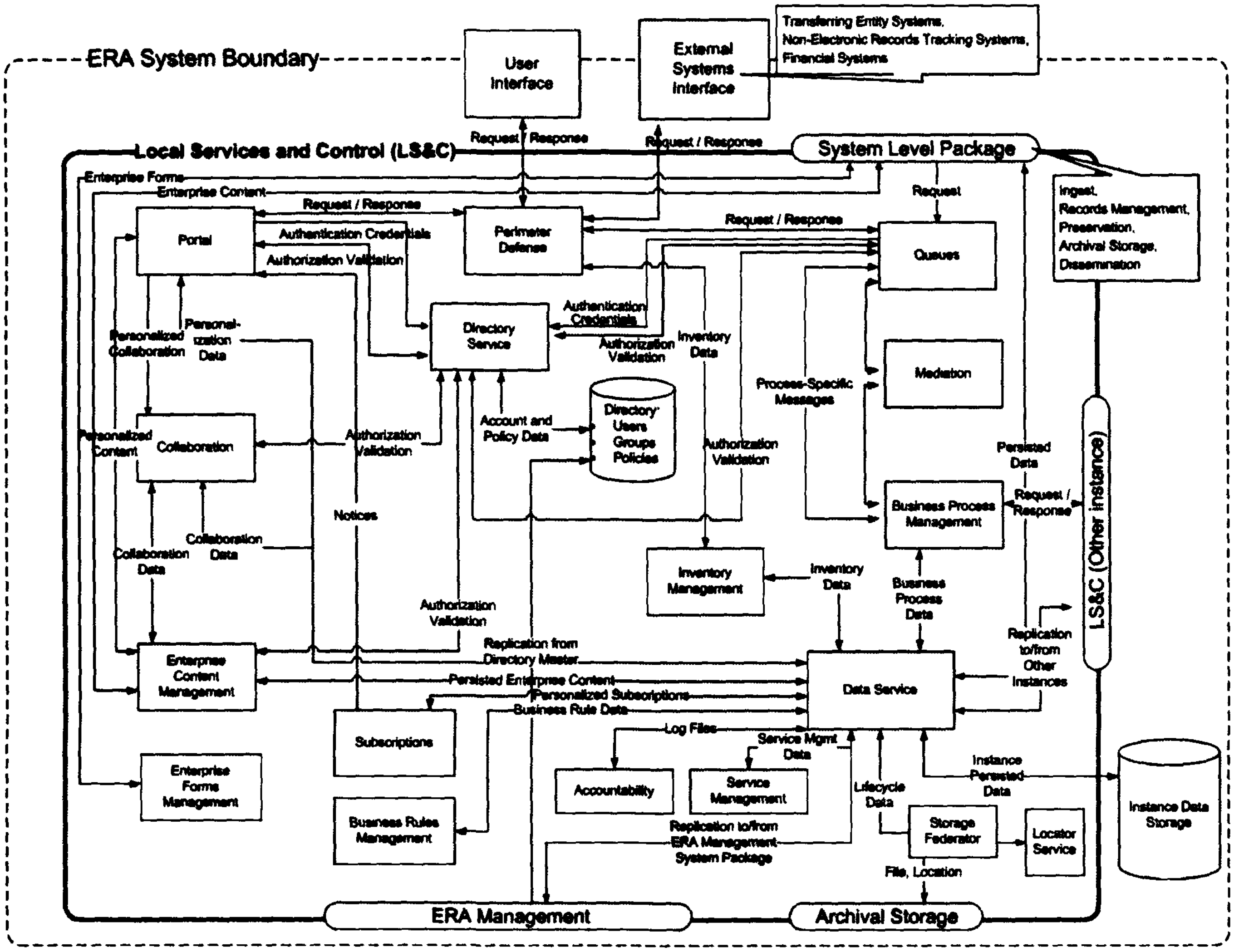
Requirement Referenced	Requirement	Architectural Impact
ERA2	Ability to manage workflows	Led to the architectural decision to include a mediation/business process management service to orchestrate services for the SOA.
ERA13	Manage security for electronic records	Led to the architectural decision to require authenticated and authorized access to all system services and assets that are not unconditionally releasable to the general public.
ERA14	Manage security for ERA itself	Led to the architectural decision to include a single point of access from user networks, including security appliances.

Requirement Referenced	Requirement	Architectural Impact
ERA21	Provide user interfaces	Led to the architectural decision to front the ERA System with a Portal framework.
ERA24.2	The system shall provide the capability for dialoguing between NARA and users	Led to the architectural decision to include asynchronous collaboration tools.
ERA29	Ability to manage user subscriptions to services	Led to the architectural decision to include subscription management framework.
ERA30	Provide service management	Led to the architectural decision to include Service Management, including Service Registry.

2.8.10.2 LS&C Functional Architecture

The LS&C functional architecture, shown in Figure 24, illustrates: (1) the ERA System's external interfaces to the LS&C system-level package; (2) the internal system-level package interfaces to and from LS&C; (3) the LS&C services logical groupings; and (4) the conceptual data flow of the LS&C system-level package.

Figure 24 – LS&C Functional Architecture



2.8.10.2.1 LS&C Interfaces

LS&C is the ERA System boundary to users and systems external to the ERA System. It is also the single system-level package that borders on all other system-level packages in any given ERA Instance. Interactions between external users, systems, and other ERA System-level packages are managed by the service invocations and business process orchestrations of LS&C.

The ERA System's external interfaces to and from the LS&C package are shown in Figure 24 and identified in Table 29. LS&C is the ERA System boundary to users and systems external to the ERA System. The internal interfaces between the ERA System-level packages and LS&C, also shown in Figure 24, are identified in Table 30. The Source column identifies the provider of the data; the Destination column indicates the recipient of the data. The Data and Description columns describe the data across the interface.

Table 29 – LS&C External Interfaces

Source	Destination	Data	Description
User, External Systems Interface	LS&C	Request	Request for service.
LS&C	User, External Systems Interface	Response	Response to user/external systems request.

Table 30 – LS&C Internal Interfaces

Source	Destination	Data	Description
ERA Management	LS&C	Replication from Directory Master	Replication of User, Group, and Policy data from the Directory Master to each LS&C Instance's Directory Replica.
ERA Management	LS&C	Replication from ERA Management System Package	Pushdown of centrally managed data to each Instance, including software, configuration files, and monitoring rules.
LS&C	ERA Management	Replication to ERA Management System Package	Roll-up of distributed accountability, inventory, and system monitoring data for centralized management.
System-Level Package	LS&C	Control Message	Business services in the other system-level packages invoked by orchestrations in LS&C.
System-Level Package	LS&C	Data to be persisted	Data from system-level packages sent to be persisted in the Instance Data Store to LS&C.
LS&C	System-Level Package	Control Messages	Business services in the other system-level packages invoked by orchestrations in LS&C.
LS&C	System-Level Package	Persisted Data	Instance Data Store accessed by system-level packages through LS&C.

2.8.10.2.2LS&C Services

The LS&C system-level package organizes services into five major logical groupings: Security, Portal, Data Services, Enterprise Service Bus, and Additional services. Additional services are included in LS&C that are associated with system management. These have been allocated to LS&C because of their distributed nature. Centralized services, including "masters" of distributed services, are allocated to the ERA Management system-level package.

The LS&C services logical groupings, presented in Figure 24, are summarized in Table 31 through Table 35.

Table 31 – LS&C Security

Service	Description
Perimeter Defense	LS&C includes the network perimeter of each ERA Instance. This interface will be secured with router filtering, firewalls, and intrusion detection devices to deter and detect attempts of unauthorized access.
Directory Service	The Directory Service provides user, group, and access policy management. Each LS&C Instance includes a replica of the Master Directory that is hosted at the ERA Management package. This local replica provides for balanced loading of the Directory servers, and enables an ERA Instance to operate in the event that the Master Directory is not available. In addition, single sign-on is provided among all ERA System services. • **Identification/Authentication** – The Identification and Authentication methods prompt for and validate the appropriate credentials of users and external systems. This service will be required for assets and services that have restricted access. • **Access Control** – Users and external systems will be permitted access to assets and services based on their authorizations (access privileges). Users may be assigned to one or more groups within the Directory. Within a service, groups are assigned one or more roles that define the permissions to assets and services. This design allows security to be managed in a modular way, optimizing flexibility of the system.
Accountability	The Accountability provides for event and audit logging. It also provides for log filtering, for reporting, and for roll-up to the master Accountability service at the ERA Management system-level package.

Table 32 – LS&C Portal

Services	Description
Portal	• The Portal is a personalized user interface that contains an aggregate of tools relevant to a user's role. The portal comprises the user interface to a human user. The "portlets" do not themselves provide business functionality – rather, they access services and queues that are provided by LS&C and by other system-level packages. • Tools included in a workbench are based on a user's role. Each user can personalize the portal. While some tools in a workbench may be required, other tools included in the default configuration of that workbench may be moved or removed by the user. Users may also add optional tools to their personalized workbench that are allowed for their roles.
Collaboration	Collaboration facilitates communication such as threaded discussion, calendars, and point of contact and subject matter expert registries.
Enterprise Content Management	Enterprise Content Management enables collaborative development of document or file-based content. It includes configurable workflow for coordination, approval, and publication.
Enterprise Forms Management	Enterprise Forms Management enables creation, development, and management of custom extensions to standard forms

Enterprise Service Bus is the hub of the Service Oriented Architecture.

Table 33 – LS&C Enterprise Service Bus

Services	Description
Queues	Queues provide a set of locations where messages being passed into the system, out of the system, and between system services can be deposited. Placing a message in a queue is a system event that can be subscribed to, and that may initiate a business process (workflow) to operate on that message.
Subscriptions	The Subscription provides for notification events, including placing an object in a queue, database triggers, stored searches, or any loggable system event.
Mediation	The Mediation maps message attributes to a canonical schema, and performs element-level data format transformations.
Business Process Management	The Business Process Management codifies processes in a set of orchestrations. Each Orchestration can be created, modified, deployed, and dynamically managed independent of other orchestrations.

Services	Description
Business Rules Management	The Business Rules Management provides centralized management of business rules that are codified in configuration data.

Table 34 – LS&C Data Services

Services	Description
Data Service	The Data Service provides persistent data stores, including file systems, relational databases, and object databases. This service is invoked by services within other system-level packages to manage their persistent data, and to manage persistent data that is used in long-lived business processes. Major data versions are persisted to Archival Storage

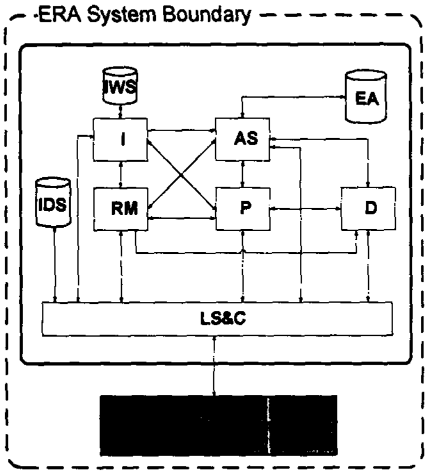
Table 35 – LS&C Additional Services

Services	Description
Inventory Management	A local copy of the Inventory Management data store will reside within LS&C. It will be a replica of the original Inventory Management data store that resides within ERA Management. This ensures that local inventory management functions, including receipt and ingest of records can continue in the event that the master Inventory Management data store in the ERA Management system-level package is unavailable.
Service Management	The Service Management provides functionality to monitor, suspend, stop/restart, and limit service execution resources.
Utility Services	The Utility Service grouping includes the Object Identity Service which may be used by any application or service that needs unique IDs, but its main role is to create identifiers for assets held in the Electronic Archives.

Table 36 – LS&C Storage Management Services

Services	Description
Locator Service	Managed storage has been separated into the Locator Service and the Storage Federator Service. The Locator Service decouples the relationship between the Asset Identifier (AID) and managed storage.
Storage Federator Service	The Storage Federator Service provides a common interface to the other services and orchestrations.

2.8.11 ERA Management



ERA Management provides the centralized services to manage the ERA System. This includes data masters for identification and authentication, roll-ups (i.e., summaries) of event and audit logs, and roll-ups of inventory management. ERA Management also provides centralized system monitoring and management, system configuration management and administration, and the ERA Help Desk.

2.8.11.1 ERA Management Key Requirements

Table 37 summarizes the key ERA Management requirements and functionality that drive the architecture.

Table 37 – ERA Management Key Requirements

Requirement Referenced	Requirement	Architectural Impact
ERA22	User Registration	Led to the architectural decision to implement Centralized Directory Service.
ERA23.1	User Assistance	Led to the architectural decision for integrated user assistance, including help screens and Frequently Asked Questions (FAQs).
ERA23.3	Provide Help Desk support	Led to the architectural decision for an interface with the NARA help desk to create a seamless help desk model.
ERA25	Maintain event log	Led to the architectural decision to centralize roll-up of event logs.
ERA26	Reports Management	Led to the architectural decision for comprehensive reporting, including creation and modification of reports.

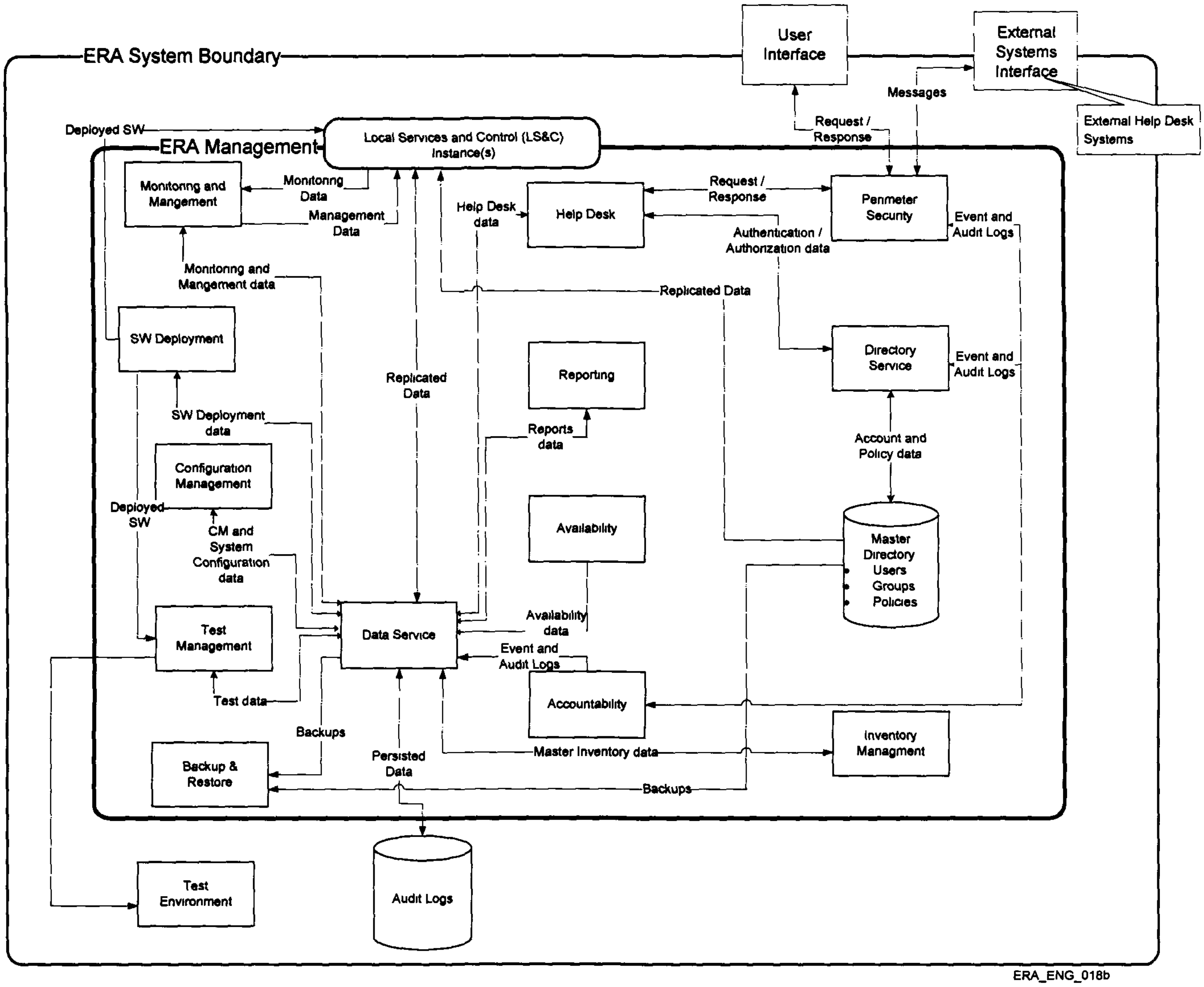
Requirement Referenced	Requirement	Architectural Impact
ERA27	Systems administration	Led to the architectural decision for centralized monitoring, management, and remote administration of the ERA System resources.
ERA28	Logistics Management	Led to the architectural decision for tracking of all the ERA System assets.
ERA32	Availability	Led to the architectural decision for clustering of servers for each Instance and the global load balancing among Instances.

2.8.11.2 ERA Management Functional Architecture

The ERA Management functional architecture, shown in Figure 25, illustrates: (1) the ERA System's external interfaces to the ERA Management system-level package; (2) the internal system-level package interfaces to and from ERA Management; (3) the ERA Management services logical groupings; and (4) the conceptual data flow of the ERA Management system-level package.

The ERA Management system-level package is external to any ERA Instance, and provides centralized system management services across all Instances at a given classification level. Administrative users access the ERA Management system-level package to operate and monitor the ERA System.

Figure 25 – ERA Management Functional Architecture



2.8.11.2.1 ERA Management Interfaces

The ERA System's external interfaces to and from the ERA Management package, shown in Figure 25, are identified in Table 38. The internal interfaces between the ERA System-level packages, also shown in Figure 25, are identified in Table 39. The Source column identifies the provider of the data; the Destination column indicates the recipient of the data. The Data and Description columns describe the data across the interface.

Table 38 – ERA Management External Interfaces

Source	Destination	Data	Description
User	ERA Management	Requests	User requests for ERA Management services.
ERA Management	User	Response	ERA System reports to Users, including: • Live monitoring • Status • Responses to system administrator initiated actions
Help Desk Systems Interface	ERA Management	Messages	Status updates on tickets sent from the ERA System to the NARANET Help Desk.
ERA Management	Help Desk Systems Interface	Messages	Tickets on issues for which the NARANET Help Desk is the appropriate respondent.

Table 39 – ERA Management Internal Interfaces

Source	Destination	Data	Description
LS&C	ERA Management	Monitoring Data	Network device, server, operating system (OS), application, and security appliance monitoring data roll-up.
LS&C	ERA Management	Replicated Data	Replication of User, Group, and Policy data from the Directory Master to each LS&C Instance's Directory Replica.
ERA Management	LS&C	Management Data	Network device and physical server configuration data is pushed to each distributed Instance at the same classification level.
ERA Management	LS&C	Replicated Data	Replication of User, Group, and Policy data from the Directory Master to each LS&C Instance's Directory Replica.
ERA Management	LS&C	Deployed Software	Deployed OS patches, COTS patches, developed code, and configuration files.

2.8.11.2.2ERA Management Services

The ERA Management organizes services into three major logical groupings: Enterprise Service Management, Security, and Data Services. Additional services are associated with system management. The ERA Management services, presented in Figure 25, are summarized in Table 40 through Table 42.

Table 40 – ERA Management Enterprise Service Management

Service	Description
Monitoring & Management	The Monitoring & Management provides centralized monitoring and management of network, server hardware, operating systems, COTS, and applications. This service uses the Simple Network Management Protocol (SNMP) standard, and provides a unified user interface for all system components.

Table 41 – ERA Management Security

Service	Description
Perimeter Security	Each ERA Management Instance includes security for the network perimeter. This network interface will be secured with router filtering, firewalls, and intrusion detection devices to deter and detect attempts at unauthorized access.
Directory Service	The Directory Service provides user, group, and access policy management. The Master Directory provides for user account creation, validation, and update. The Master Directory also provides for delegated administration of group membership. User and group data are replicated from the Master Directory at ERA Management to local Directories at each LS&C Instance. • **Identification/Authentication** – The Identification and Authentication methods prompt for and validate the appropriate credentials of users and external systems. This service will be required for assets and services that have restricted access. • **Access Control** – Users and external systems will be permitted access to assets and services based on their authorizations (access privileges). Users may be assigned to one or more groups within the Directory. Within a service, groups are assigned one or more roles that define the permissions to assets and services. This design allows security to be managed in a modular way, optimizing flexibility of the system.
Accountability	The Accountability provides a centralized roll-up of audit and event logs. The level of detail that is rolled-up to the system-level is dynamically configurable.

Table 42 – ERA Management Data Services

Service	Description

Service	Description
Data Service	The Data Service provides persistent data stores, including file systems, relational databases, and object databases. This service is invoked by services within other system-level packages to manage their persistent data, and to manage persistent data that is used in long-lived business processes.

Table 43 – ERA Management Additional Services

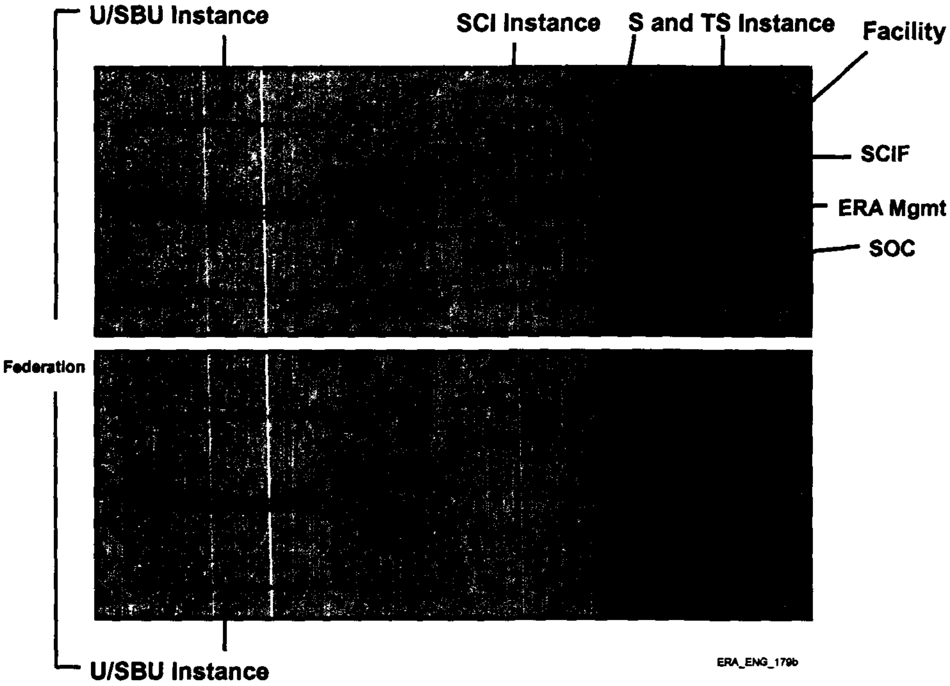
Service	Description
Test	The Test provides test data and test scripts, and executes test hardware (HW) and software (SW) in test environment.
Help Desk	The Help Desk provides user support functions for all Information Technology (IT) issues. Provides services to answer questions, provide technical support, and capture problem reports. This service can be invoked by external systems, users or by other services within the ERA System.
Reporting	The Reporting provides report generation functionality for both ad hoc and routine reports. The reporting service will automatically generate scheduled reports without user interaction. Changes to routine reports are under Configuration Management control. Users also have the capability to generate, run, and save ad hoc reports.
Inventory Management	Inventory Management provides master inventory data across the ERA System. Managed inventory include: accountable inventory and records/assets. (Consumable inventory is not tracked after receipt.) This service is invoked by services within other ERA packages to manage the inventory at a central location.
Software Deployment	The Software Deployment provides centralized management and deployment of software including operating system patches, COTS patches, software configurations, and developed code for applications. This service ensures that all system resources that have been allocated to a single function are configured identically, with exceptions only for locally-configured aspects.
Configuration Management	The Configuration Management includes configuration of hardware, software and operations. The configuration management procedures include release authorization control through the Change Control Board (CCB). • Hardware – configurations for network devices, servers, and storage devices • Software – history of versions, operating system patches, COTS patches, software configuration patches, and developed code patches • Operations – procedures for doing System Administrator tasks
Backup & Restore	The Backup & Restore provides for persisted data and files.

Service	Description
Availability	The Availability provides centralized monitoring and management of Instance and network loads, and the balancing of user and interface load across Instances.

2.9 Physical Architecture

The physical architecture of the ERA System is defined and described using the following terms, as illustrated in Figure 26 – Physical Design Terms.

Figure 26 – Physical Design Terms



- **Instance** – An Instance comprises the applicable hardware (servers connected by routers and switches), software (System-level Services), and security appliances (firewalls, intrusion detection devices) necessary to operate the ERA functionality within a specific Federation at an individual facility. An Instance only operates on one classification level. For example, the U/SBU Instance will not interface with any of the Instances within the Secret, Top Secret, or SCI Classified Instances. This ensures that there will not be any unintended passing of classified assets between Instances of different levels of classifications. There is no limit to the number of Instances that ERA may support. However, there is a limit to the size that an Instance may grow without impacting user performance, ability to manage devices, and exceeding limitations on the cost-effective physical size of a computing center.

- **Federation** – A Federation is made up of one or more inter-connected Instances with the same data classification level (i.e. U/SBU, Secret, Top Secret, or SCI).
- **Management** – The ERA Management system-level package is isolated on a separate VLAN from the main ERA Instance. ERA Management comprises the applicable hardware, software, and security appliances to accomplish this functionality. There are four unique deployments of the ERA Management system-level package: one for the U/SBU Federation, one for the Secret, and one for the Top Secret, and one for the SCI Federation. The ERA Management system-level service connects to the main services of an Instance via an "out of band" network – no user traffic and no archival assets traverse this management network.
- **Facility** – Within the context of the ERA System, a Facility is an actual physical location that may contain one or more Instances, one or more Federations. A Facility may also contain a System Operation Center (SOC).
- **System Operations Center (SOC)** – The SOC is the location at which the network, security, and system monitoring and management is performed by a staff of administrators. The SOC physically resides at two of the Facilities for redundancy. There are four unique components of the SOC: one for the U/SBU Federation, one for the Secret, one for the Top Secret, and one for the SCI Federation. There are three components at the secondary site, one each for U/SBU, S, and TS. SCI Instances use tape backup rather than a second site.

The following sections surrounding the ERA System physical architecture consist of the following items:

- Identifying the number of locations of the ERA facilities
- Describing the various data classifications that will be stored and processed at each of the facilities
- Describing the network topology, both external to the ERA System as well as internal to the ERA System
- Describing the logical representation of a facility
- Introducing the physical architecture of a typical Instance of the ERA System, including the SOC
- Describing the topology of the development and test sites that will be used to support the development, acceptance, and maintenance of the ERA System by NARA

2.9.1 Active Safe-Store

The ERA System architecture employs an Active Safe-Store approach to protect and preserve NARA's electronic assets. In this approach, the system actively manages backup copies of its information assets, continuously preparing to recover from hardware, software, network, and facility failures. The LM Team has selected the Active Safe-Store model over a dedicated backup facility with conventional backup vaulting for three primary reasons:

1. Active Safe-Store distributes backup information in the same way as primary information. A catastrophic facility failure prevents access to only a portion of the backups whereas in a conventional backup recovery scheme, the failure of a dedicated backup facility removes 100% of the ERA System's remote information redundancy.
2. Active Safe-Store provides a more graceful failover strategy. When the Active Safe-Store approach is used with the LM Team's Storage Management approach, the safe-stored copy of an electronic record retains the same globally unique identifier as the primary copy. Should a primary facility suffer a prolonged outage, the ERA System will automatically retrieve records from Safe-Store while primary facility services are being restored.

3. Active Safe-Store provides balanced load-sharing during catastrophic failures. Under a dedicated backup facility model, all primary facility failures result in failover to a single backup facility. Under the extreme condition of multiple primary facility failures, the backup facility will be quickly overwhelmed. Active Safe-Store permits each primary facility to act as a failover facility. The failover load resulting from multiple failures is distributed among the remaining sites and overall performance suffers less degradation.

This architectural approach offers a number of significant distinct benefits over a traditional backup approach:

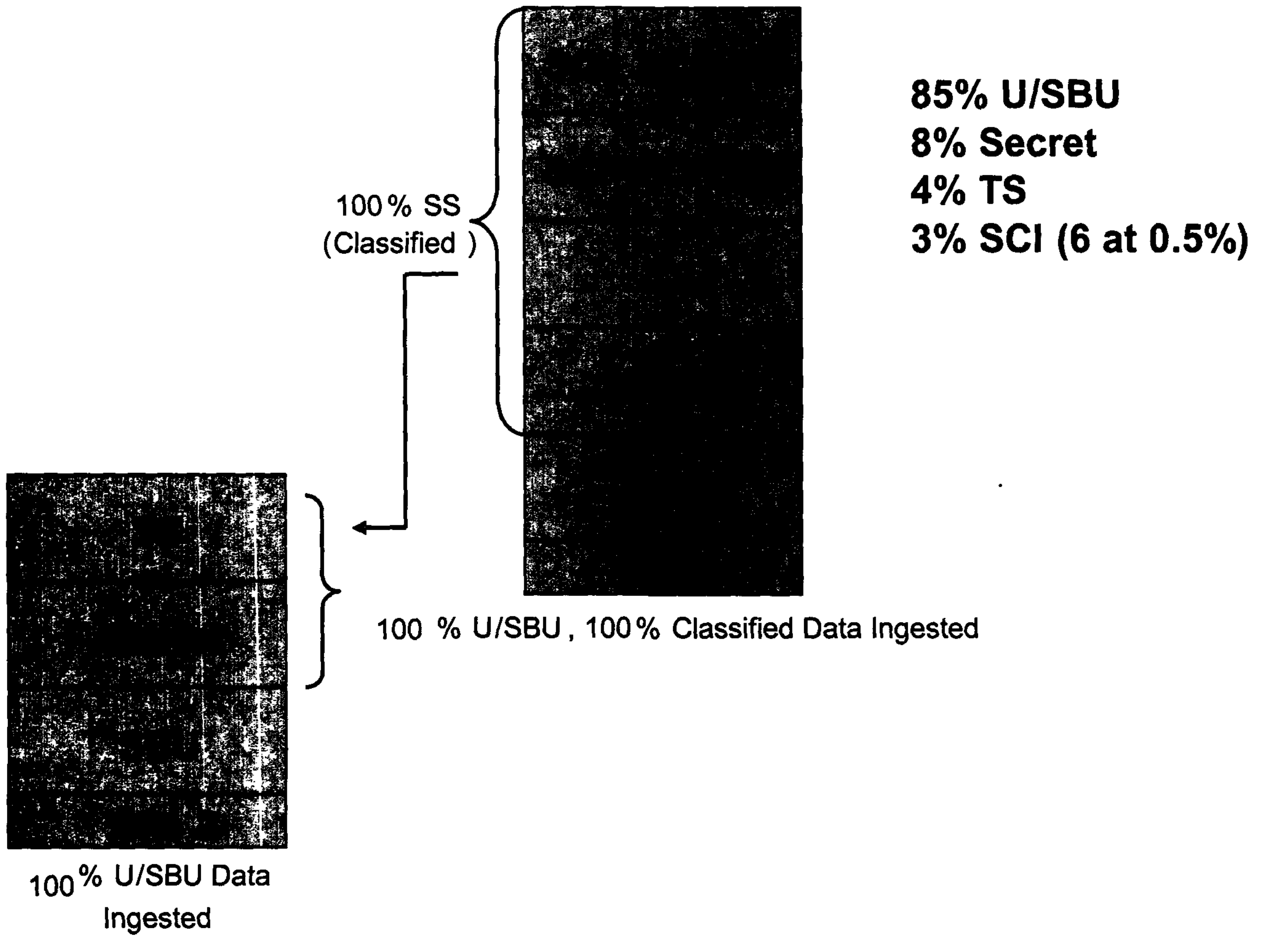
- All ERA primary facilities share a common architecture. Developing sites specialized for backup would require unique hardware and software configurations, different skill sets in the operational staff, and different operational processes and procedures and would increase the overall complexity and cost of a backup solution.
- Safe-Store media receive the same maintenance as the active archive media. For example, if new technology made the choice of higher density tapes attractive, the conversion processes and procedures would be the same for all of the data held on the old tape media.
- Active Safe-Store provides for backups, not simply replicas. File and database replicas are created on a near real-time basis; however, backups are created more deliberately as part of ongoing business processes. Holdings change infrequently and under very controlled conditions and with higher quality assurance. When Ingest submits new electronic records to the Storage, the system commits the new records to the primary store and the Safe-Store as part of the Ingest process. Only after the successful "double commit" is the Ingest process judged to be complete. Dynamic operational data, such as customer information, orders, database indices, and workflow process states, undergo more conventional backup processing and then the backups are committed to a Safe-Store. This avoids having some form of systemic corruption propagate itself through the primary data copy and the backup copy at the same time.

Active Safe-Store is more responsive in the face of failure. It permits servers to be reconfigured to offer access to safe-stored data in the event of a prolonged outage at the primary facility. In a vaulting method, the access to the data is interrupted until the system (or a new facility) can be reconstituted.

Architectural flexibility allows that some ERA facilities will not serve in both primary and Safe-Store roles. When smaller or partial Instance facilities, such as the Presidential libraries, are deployed, the solution will leverage the Safe-Store backup functionality of a larger ERA facility, such as one of the U/SBU sites.

Figure 27 illustrates the Active Safe-Store configuration design for the three notional sites. Also shown in this figure, is the percent distribution of the data under storage by classification. Original guidance called for 85% U/SBU, 14% classified, and 1% PRA. It was necessary to further refine these percentages to properly design and size each of the Instances as well as the Federations. The LM Team's architecture and candidate design are flexible and scaleable such that the actual configurations can change to accommodate greater or lesser loads and volumes based upon the actual transfers to the ERA System from the transferring entities.

Figure 27 – Notional Safe-Store Approach



ERA_ENG_021c

The notional Safe-Store approach is described below:

- Site 1 (government owned and controlled) will ingest 25% of the U/SBU records and 100% of the classified records. Site 2 will act as the Safe-Store facility for 100% of Site 1's classified records and Site 3 will act as the Safe-Store facility for 100% of Site 1's U/SBU records.
- Site 2 (government owned and controlled) will ingest 25% of the U/SBU records. Site 3 will act as the Safe-Store facility for 100% of Site 2's U/SBU records.
- Site 3 (contractor owned and conrolled) will ingest 50% of the U/SBU records. Site 2 will act as the Safe-Store facility for 50% of Site 3's records and Site 1 will act as the Safe-Store facility for the remaining 50% of Site 3's records.

This facility and Safe-Store configuration achieves the following goals:

- All records are actively Safe-Stored
- The U/SBU ingest load is balanced across three sites
- 100% of the U/SBU records are stored at government-controlled sites (Site 1 has 25% primary and 25% as Safe-Store; Site 2has 25% primary and 25% as Safe-Store). This complies with NARA

instructions, and provides the government with a complete copy of all the assets in the archives in sites under its control.

- 100% of the classified records are ingested at Site 1, which already has archivists with the appropriate security clearance, and SCIF and facility security measures in place to handle classified researchers
- 100% of the classified records are stored at government-controlled sites, including both primary and Safe-Store (Site 1 has 100% primary; Site 2 has 100% Safe-Store). This avoids the cost of establishing links to government secure networks (such as JWICS) at new sites.

This is presented as a notional configuration, and actual configurations will depend on the characteristics and number of sites slated for deployment.

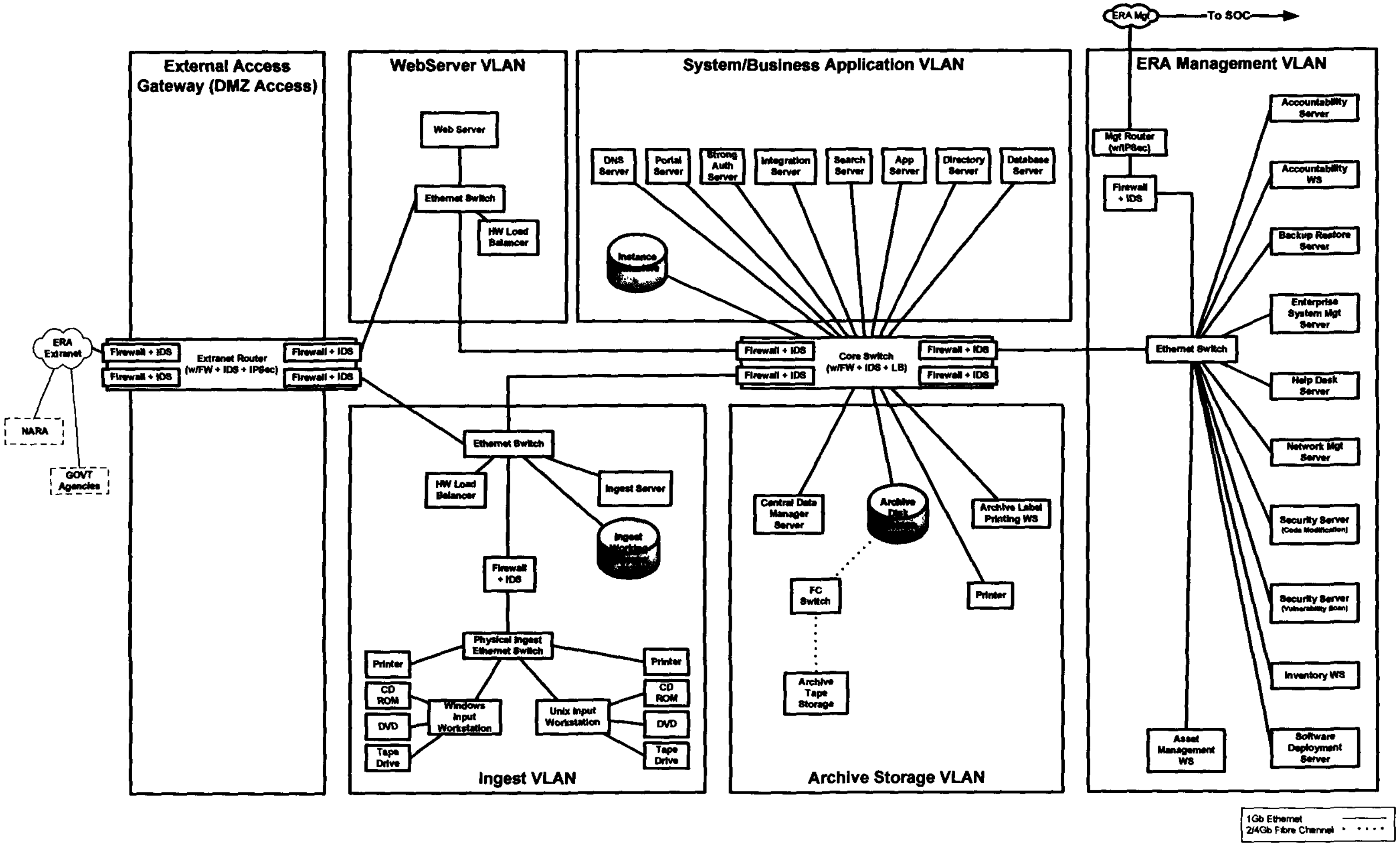
2.9.2 ERA Instance

The ERA System initial physical architecture is shown in Figure 28, which conceptually illustrates how the functional architecture in the previous sections will be implemented and how the system will interface with external resources. However, this illustration currently depicts the deployment of ERA during Initial Operating Capability (IOC). The full state of the physical architecture will be incrementally advanced to reflect the end state at FOC. The classified Instances do not connect to external public networks or NARAnet, even though the diagram shows the possibility of this outcome.

The physical architecture is designed to be scalable both horizontally (more hardware) and vertically (more powerful or additional hardware within the same enclosure), as well as providing the ability to accommodate new technology as it becomes available. The physical architecture is also designed to scale down: both hardware elements and software elements can be omitted from an Instance, as required for a particular configuration. For example, one Instance could omit or scale down Ingest, in favor of scaling up Dissemination. The system is highly reliable and available, with no single points of failure. The physical architecture is implemented with dual functional components (network and processing infrastructure), and relies on the Safe-Store approach to ensure data redundancy.

The physical network architecture of the ERA Instance is comprised of five virtual local area networks (VLAN). The following sections describe the five VLANs.

Figure 28 – Physical Architecture



2.9.2.1 *Ingest VLAN*

Ingest is allocated its own VLAN to support segregating sensitive records (i.e. Title 13 and classified data) from the rest of the system during the initial transfer processing within the Ingest process. The Ingest VLAN is located within a Demilitarized Zone (DMZ) isolated by Firewalls and Intrusion Detection Systems (IDS) to minimize the risk to the rest of the ERA System from external threats and attacks and to ease recovering from a security violation that would occur if records that are misclassified were mistakenly sent to an Instance at the incorrect classification level. DMZs are neutral zones that also prevent outside access to the internal system data.

The Ingest VLAN contains a temporary Ingest working storage, to contain the electronic records while both virus scanning and data classification checking are performed. Access to the Ingest VLAN in Unclassified Instances is through a perimeter security layer. The perimeter security layer interfaces to the Internet, and NARANET to receive data transfers into the ERA System. This VLAN carries applications for Ingest services and also interfaces with other services in the System/Business Applications VLAN.

For Sensitive Compartmented Information (SCI), Top Secret, and Secret Instances users must physically be located within the SCIF using hardware directly connected to the Instance to perform the Ingest functions. It is not envisioned that electronic transmission of classified information will initially occur, thus all classified information will be processed through the physical media input devices. The ERA System architecture does not preclude the addition and incorporation of an electronic interface to accept the electronic information. JWICS or SIPRNET connections and interfaces can easily be incorporated to provide this functionality.

2.9.2.2 *WebServer VLAN*

The WebServer VLAN is one of the external access points to the ERA System. The external user accesses the Webserver VLAN through one of the following mechanisms:

- The public Internet
- NARANET
- Other Government Networks (i.e., i2, SIPRNET, NIPRNET, JWICS)

The WebServers are allocated their own VLAN in a DMZ. This is to ensure security protection to the rest of the physical architecture from external users and a potential external security network-based attack. Inbound requests, which enter through a perimeter security layer, are proxied through the WebServer VLAN that in turn communicates and interfaces with the Ingest or System/Business Applications VLANs for application processing. The data forwarded outbound is then proxied through the WebServer VLAN.

2.9.2.3 *Archival Storage VLAN*

Archival Storage is allocated its own VLAN to ensure maximum segregation and perimeter control over the archival records. This VLAN consists of two main components, the archive management servers and the media storage devices. The archive management servers process the inbound and outbound requests for data and records from the electronic archive. The storage media devices provide for working storage, performance disk cache and archive tape libraries.

For Unclassified Instances, Archival Storage will serve simultaneously as both a primary and a Safe-Store location. For Sensitive Compartmented Information (SCI), Top Secret and Secret Instances, Archival Storage will typically only be either a primary or a Safe-Store location.

2.9.2.4 System/Business Applications VLAN

The System/Business Applications VLAN contains the main business process components of the ERA System and interfaces directly with the Archival Storage VLAN to store data and process data requested by the Ingest and WebServer VLANs. The Web Server DMZ ensures that there is no direct interaction by external users or systems with components on the System/Business Applications VLAN. The processors for this VLAN contain applications for Dissemination, Preservation, Records Management and some of Ingest and LS&C services. The Instance data storage that supports all operational Instance data is also part of this segment.

2.9.2.5 User VLAN

The User VLAN is a separate multi-purpose VLAN within a facility that will be used for various User Roles such as Help Desk operators, archivists, and system administrators. These systems can be expanded or removed based upon policy and their actual need during operations. In the classified Instances, this User VLAN will be within the appropriate SCIF and will be used predominantly by the archivist and researcher performing their ERA roles and responsibilities.

2.9.2.6 ERA Management VLAN

The ERA Management VLAN is a separate VLAN that hosts the system monitoring and management tools. The ERA System physical architecture leverages the same security and network infrastructure stack, cluster server hardware and software, and working storage devices as archival Instances. The SOC, like the Instances, is also configured with redundant hardware to guarantee accessibility in the event of a system failure. Additional bandwidth, processors or servers can be added to accommodate future growth, if required.

The Management VLAN is connected to rest of the ERA System via an out-of-band network, and is isolated with a firewall. System operators at the SOC are on a separate VLAN, and connect to the ERA Management functionality via a Web browser.

2.9.3 System Operations Center

The SOC provides ERA System support by providing ERA management functionality such as ongoing centralized monitoring and management services. Another primary function of the SOC is to communicate with the development facility to receive software releases and distribute them to the ERA Instances.

All U/SBU ERA Management functionality can be accessed remotely via the public network infrastructure (assuming proper security authorization is granted), providing a great deal of deployment flexibility. The physical configuration follows the safeguards and procedures required by the classification level it manages.

2.9.4 Development Sites/Environments

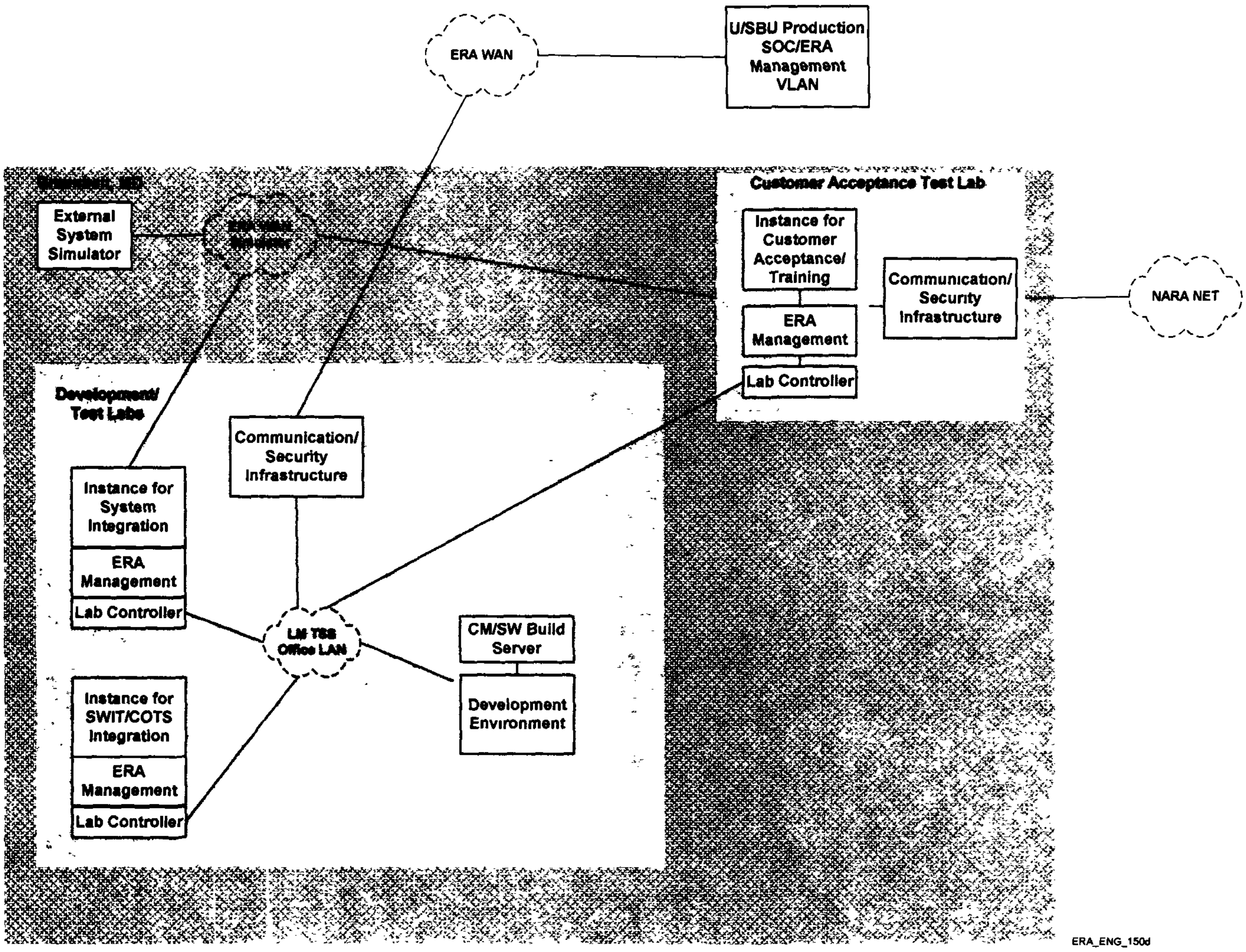
Figure 29 shows the four separate lab environments required within the LM Team's ERA System. These development and test labs are:

- Development/Test Labs includes:
  - Development Environment
  - COTS Integration lab (including a fully functional ERA Management Instance)
  - System Integration Lab (including a fully functional ERA Management Instance)
- Customer Acceptance Test/Training Lab (includes a fully functional ERA Management Instance)

These labs will be used to develop, integrate, and test all of the COTS products as well as any custom developed software. The Customer Acceptance Test/Training Lab is used by NARA to perform all acceptance testing prior to accepting and deploying the Increment or Release software versions, and also for training.

An ERA WAN simulator will also be deployed such that network traffic as well as other Instances within a Federation can be simulated without having to deploy additional test sites and Instances.

Figure 29 – Development Environment


ERA WAN
U/SBU Production SOC/ERA Management VLAN
Greenbelt, MD
External System Simulator
ERA WAN Simulator
Customer Acceptance Test Lab
Instance for Customer Acceptance/ Training
ERA Management
Lab Controller
Communication/ Security Infrastructure
NARA NET
Development/ Test Labs
Communication/ Security Infrastructure
Instance for System Integration
ERA Management
Lab Controller
LM TSS Office LAN
CM/SW Build Server
Development Environment
Instance for SWIT/COTS Integration
ERA Management
Lab Controller
ERA_ENG_150d

2.9.5 Instance/Facility Constraints

The LM Team experience has shown that there is a natural limit to the size of a data center, beyond which there are diseconomies of scale due to system management and operational control, as well as logistical considerations overwhelming the efficiency equation. For example, in a case of a data center where the ratio of operators to physical devices (servers, storage devices, network elements) becomes too small, the operational effectiveness decreases and service levels can be negatively affected. In these cases, building two smaller data centers (even in the same Facility) instead of one extremely large data center can be more operationally efficient and lower the overall total cost of ownership.

The operational efficiency constraint for data centers constantly changes as new administrative tools and technology are introduced. For example, one of the main variables in the equation is physical floor space, and new technology provides ever-increasing storage and processing densities, which in turn allows data centers to provide more storage and processing capacity per square foot. This also translates to fewer computing elements (servers and storage elements) that need to be maintained and managed. The availability of new administrative tools, and their ever increasing automation, will also allow the system managers and administrators to manage more and more elements over time. Therefore, as the density of the processing and storage increases and the increase in automation and efficiency of the management tools increase the need for expanding to additional facilities might be diminished, depending on whether the rate of technology improvements is higher than the ever-increasing rate of ingested records.

The LM Team recognizes that the optimal size of the data center will eventually be met. The LM Team's initial ERA System physical design includes three facilities based on an analysis of efficiency and size. Both the ERA System architecture and design support adding additional Instances and Facilities over time to scale up to meet the ever increasing processing and storage needs of NARA. The approach of Federating Instances across geographically diverse Facilities provides the most flexibility in scaling the ERA System in a cost-effective manner.

The LM Team expects to complete an analysis during Increment 1 that will establish an upper bound. Establishing a finite size limit prior to the test program will provide specific limits for the testing program to verify. In addition, the LM Team will continuously monitor the management metrics of the data centers to ensure that the service levels of the ERA System are met. Once a threshold has been crossed, the LM Team and NARA can make decisions regarding the creation of a new ERA Instance or Facility to accommodate the anticipated growth.

2.9.6 Partial Instance Deployment

The LM Team's physical architecture and design support the concept of partial Instance deployments. A partial Instance is composed conceptually of only a portion of the actual functionality (i.e. services in the Service Oriented Architecture). Partial Instances can be decomposed to the level of individual services, and may include portions of the Ingest, Dissemination, or Storage functionality. For example, if NARA is planning the acceptance of a large transfer of records from a particular agency, NARA might want to set up a special Ingest-only Instance to process this transfer of records into the ERA System. In this example, this partial Ingest Instance would only require the associated equipment (hardware, software, infrastructure, and services) to support the Ingest and temporary storage functionality of the ERA System. Other functionality (Dissemination, Records Management, etc.) would not have to be deployed to support this partial Instance deployment concept.

Other examples could include deploying a Storage-only partial Instance, or a Dissemination and Storage Instance such that NARA can optimally utilize the ERA System based upon the service levels, funding profiles, and records transfers and access that are required. This concept allows NARA to configure the ERA System in whatever manner serves its policy and business needs by deploying the group of services that are required to support these business needs. The important aspect of the LM Team's architecture and design is that the entire ERA System does not need to be deployed to achieve a limited subset of the ERA System functionality.

2.10 Security Architecture

Information Assurance and security architecture is central to the deployment of the ERA System. Security is a composite of personnel, facilities, administration, and IT mechanisms. This section describes the mechanisms that meet the security requirements specified in the SyRS, with the key requirements summarized in Section 2.10.1. In this section, the security data are shown internal to the security boundary since security functions protect it. In actuality, the security data are part of the Instance Data Storage and System Data Storage.

While security is part of the LS&C and ERA Management system-level packages presented in Sections 2.8.10 and 2.8.11, the ERA System security architecture is separately presented in this section to provide the additional details required to address security within the ERA System. The security architecture and design sections are also formatted differently because they are intended to "stand-alone" and be reviewable separately from the rest of the document. In addition, security is prevalent throughout the system, and therefore requires a different presentation style.

Security can be divided into two major components:

1. Infrastructure security (defense of the ERA System against external or internal attack)
2. Application security (proper controls for system assets and user access)

To understand how the ERA System security protects the system and its assets, it is necessary to understand not only the security mechanisms, but also the environment in which they are implemented. This explanation is presented in Section 2.10.2.

2.10.1 Key Security Requirements

The key security requirements that drive the system architecture, as well as the security architecture, are listed in the table below:

Table 44 – Key Security Requirements

Requirement Referenced	Functionality	Architectural Impact
ERA13	The system shall manage security for electronic records	Protection of records is paramount.
ERA13.2	The system shall provide the capability to manage electronic records according to the access restrictions of the record	Access control is based on record restrictions and user access permissions.
ERA13.2.1	The system shall provide the capability to control data up to the Top Secret/ Sensitive Compartmented Information (TS/SCI) level	Data sensitivity ranges from unclassified to TS/SCI and must be protected accordingly.

Requirement Referenced	Functionality	Architectural Impact
ERA13.2.2	The system shall physically separate records classified as Top Secret or higher from other records	Air-gaps, cryptographic separation and firewalled separation are used to isolate ERA System Instances of different classification levels.
ERA13.4	The system shall recognize multiple access restriction levels defined by NARA	The ERA System supports an extensible set of access restrictions and rights.
ERA14	The system shall provide security for itself	The ERA System protects the system and its data from unauthorized access, modification, and prevention of external intrusions and attacks.
ERA14.1	The system shall prevent unauthorized system access in accordance with the Security Plan	All protection mechanisms in the System Security Plan (SSP) must be implemented.
ERA14.11	The system shall control access to records life cycle data based on a user's access privileges	Records life cycle data is based on data access restrictions and user access privileges.
ERA14.7	The system shall operate in accordance with applicable security guidance and rules	The ERA System meets the additional security requirements specified in the guidance documents.
ERA17.5	The system shall provide the capability to declassify assets	The ERA System provides mechanisms to move declassified information from higher to lower classified Instances.
ERA22	The system shall provide the capability for user registration	The ERA System supports registered and unregistered users; unregistered users have access only to "public" data.
ERA25	The system shall maintain an event log	Significant events related to the system, to archival processing and to security must be auditable.

2.10.2 Functional Security Architecture

The top-level security architecture is presented in Figure 30. The four building blocks of security are listed below. These are the traditional top-level services of security architectures.

- **Identification and Authentication (I&A):** establishes the identity of a user or external system that wishes to connect to an ERA Federation. This must be done before the user or external system can access any ERA System assets or receive any information from the ERA System. This ensures that only authorized users can access a particular Federation of the ERA System and the information contained in that Federation.

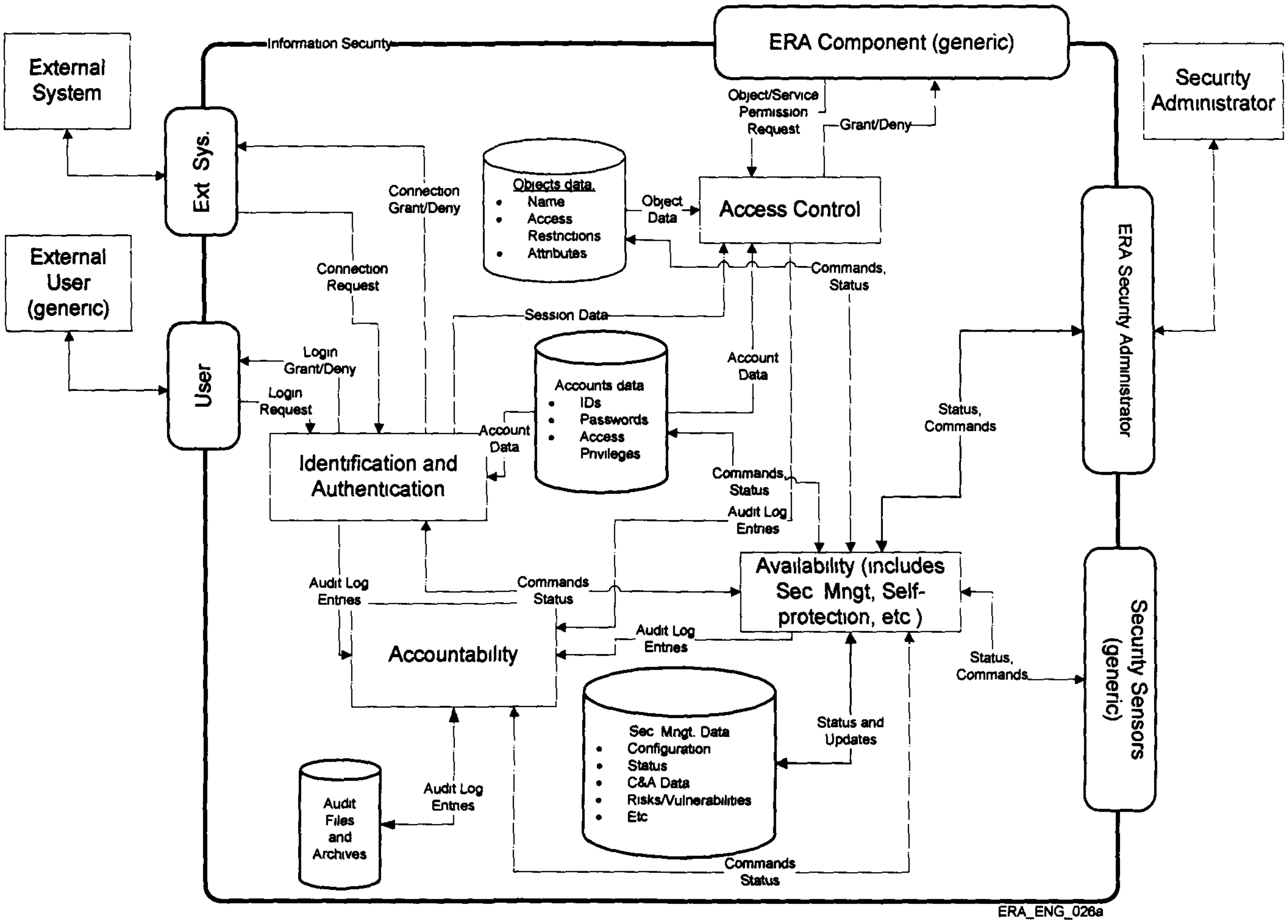
- **Access Control:** uses the established identity to control access to resources – both to data assets and to functions/services. In the ERA System security architecture, users and external systems are restricted first to functions/services for which they are authorized; and then, using those authorized functions/services, they access information for which they are authorized. This ensures that not only are users restricted to accessing permitted data assets, but that users can only perform authorized functions upon that data.

- **Accountability:** irrevocably links users to the actions that they perform. Accountability includes non-repudiation functions (including, as needed, auditing, digital signatures, secure hashes, and other techniques). In the ERA System, every significant event is auditable (i.e., capable of being audited); the audit administrator will select which events are meaningful for the environment. Accountability ensures that user and system activity can be reconstructed and proper responsibility assigned.

- **Availability:** encompasses all functions which are concerned with keeping the security mechanisms operational in spite of user or attacker attempts to bypass or subvert them. Security availability differs from system availability in that security availability is concerned with system attacks that might limit the ability of the ERA System to perform whereas system availability is concerned with the reliability of the ERA System hardware and software components. Security availability includes a wide variety of services, ranging from security management to resource utilization to infrastructure protection to Certification and Accreditation maintenance.

All ERA System services and functions invoke security services to determine if the caller (user, service or external system) is authorized to use the service and to ensure the accountability of subject actions. Invokers are checked for authority and their actions audited.

Figure 30 – High Level Security Architecture



2.10.2.1 Access Control

Access Control has two primary functions:

- The first function validates the right of the invoker to access the requested resource. The caller may be a service, an external system or a user. When services are invoked by other services, in general, Access Control checks to see if the user or the external system has the right credentials.
- The second function is responsible for the prevention of scavenging of information through the examination of the physical media on which an information object resides. If the system does not eliminate traces of the prior contents of a deleted or moved object, a new object assigned that space could read the old object contents. There are three acceptable techniques to prevent this:
  - When an object is deleted or moved, the prior location is overwritten with a meaningless pattern.
  - When an object is created or increased in size, the added space is overwritten with a meaningless pattern before the requestor is given access.

- The system can enforce a strict "write before read" capability, ensuring that prior contents are overwritten before being read back (so that, for example, a user cannot read past the end-of-file mark on a tape.)

This function is also responsible for addressing the problem of magnetic remanence. When an object is decommissioned, all traces of prior use must be removed. Material will be disposed of in accordance with applicable standards, which includes over-writing multiple times, or destruction.

2.10.2.2 Accountability

Accountability has two functions:

- **Audit** is responsible for capturing all relevant security information desired by the audit administrator. All significant system, archives and security events are auditable, but the administrator will set the audit function to capture those events required by the audit policy. When audit logs near capacity, older events will be archived in accordance with audit policy. This function also provides the audit reports in response to requests by the administrators. Audit logs ensure that user actions can be incontrovertibly tied to the user.

- **Expunge Audit Records** provides the capability to expunge audit records about electronic assets that are being expunged from the archives. Expunge means that all traces of the electronic asset should be deleted, including the audit records that describe the actions taken on the electronic asset.

2.10.2.3 Availability

The Availability contains several disparate functions that ensure that the system, its functionality, and its data remain available for use. It includes management functions since management is devoted to the continued, proper operation of security mechanisms. The services in Availability include:

- **Security Management** consists of all services that deal with management aspects of the security mechanisms from account management to mechanism management to key generation and exchange.

- **Self Protection** consists of all services that protect the system against attacks, penetrations, and vulnerabilities.

- **Assurance Maintenance** consists of all services that help maintain the system's accreditation.

2.10.2.4 Identification and Authentication

Identification and Authentication consists of a set of services that deal with identifying a user or external system (assertion of who the subject is) and authenticating the user (validating the subject's identity assertion is correct). These include:

- **Login** is used to collect the user's ID and authentication inputs; it invokes the authentication service to verify that the right authentication has been entered and invokes the credentials service to associate the proper access rights and privileges with the session being established.

- **Interface/System Identification** is used to identify external systems and interfaces that require positive identification before data exchanges are allowed: for example, an external financial system.
- **Authentication** manages and verifies authentication tokens (passwords, PINs, biometrics, etc.), authentication aging, complexity, etc. to positively establish a subject's identity.

Session Control provides the capability to set up and control a user session, including ascertaining the right authorizations and privileges for the user, based on the combination of the user and group permissions, and for control session activity, time-outs, and so forth.

2.11 Data Architecture Methodology

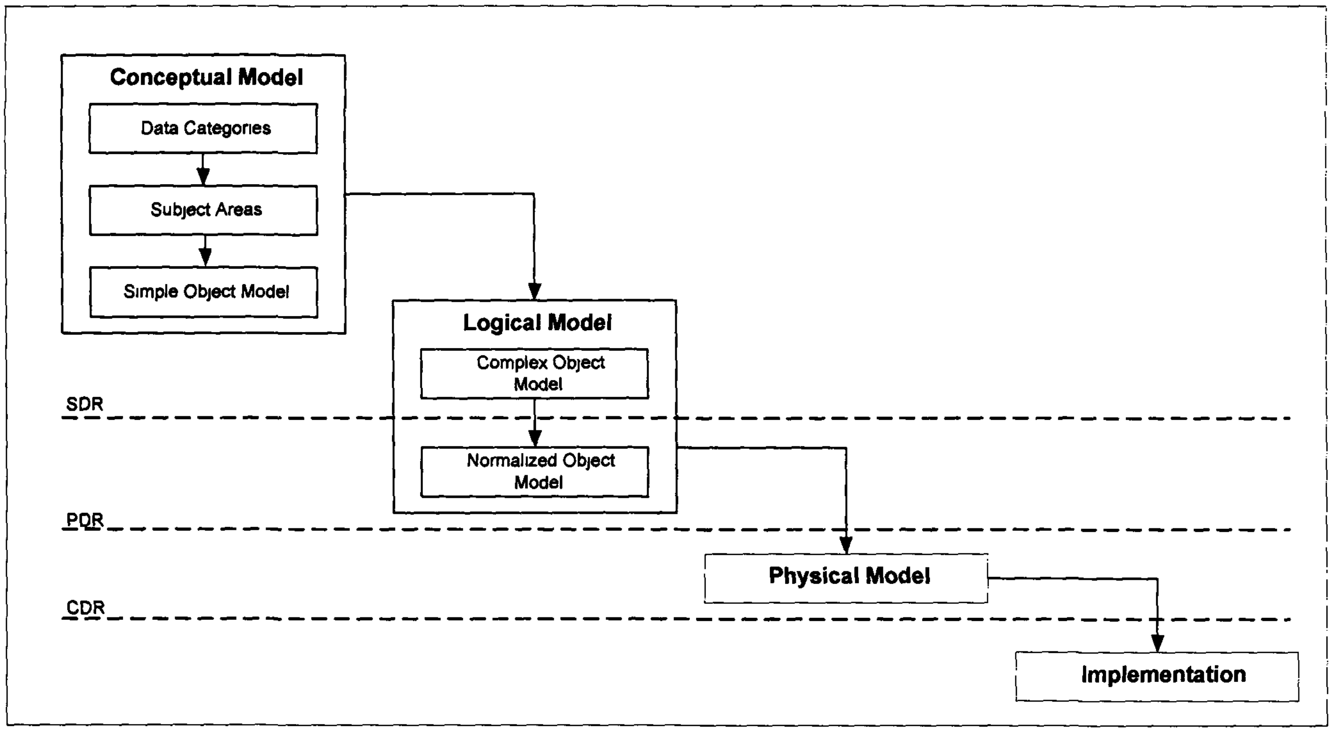
The ERA System data modeling follows the methodology described in the NARA Data Architecture document. This methodology is based upon a set of principles, constraints and assumptions; as prescribed by the EA, all NARA data models must be compliant with these PCAs.

Figure 31 – ERA Data Architecture Methodology illustrates the ERA System data architecture compliance. The methodology consists of a hierarchy of modeling steps each adding more detail than the previous step:

- Step 1: The data modeling starts with the development of the conceptual model, which defines data elements and their interactions at the real-world, domain level without particular regard for how this will be implemented. In the NARA Data Architecture document, NARA has started this process by defining a series of Data Categories made up of Subject Areas. The applicability and scope of these subject areas are investigated for use in the ERA System leading to the definition of ERA Subject Areas each of which is closely mapped to the NARA Subject Areas. Each ERA Subject Area is then decomposed into a conceptual object model. The methodology used in conceptual modeling is further described in Section 2.11.1.
- Step 2: The simple conceptual object model is then decomposed into a logical model, which states how the system will be developed at the application systems design perspective. Starting from the objects in the conceptual simple object model, a complex object model is developed during the design and development life cycle.
- Step 3: The logical model is further developed into a physical model, which states how the system will be implemented (e.g., as a relational database schema, XML schemas etc.). This model is then subject to CDR.
- Step 4: The physical model then forms the basis for the implementation.

This flow down is illustrated in Figure 31, which also indicates at which point in the development cycle each of the models will be produced and reviewed.

Figure 31 – ERA Data Architecture Methodology



ERA_ENG_027a

2.11.1 Methodology for the Conceptual Model

The top level of the Conceptual Data Model is defined in the NARA Data Architecture. The NARA data model is divided into seven Data Categories each with a number of subject areas. The subject areas that are stated in NARA Data Architecture document cover all of NARA's activities. However, all the NARA subject areas are not applicable to the ERA System domain model while in some other cases, due to the more focused scope of the ERA System, the distinction between two or more NARA subject areas is not relevant at this level of conceptual modeling. As a result, ERA Subject Areas are mapped to the NARA Subject Areas but do not necessarily have a one to one correspondence. As far as possible the names of the NARA Subject Areas are used for the ERA Subject Area. Where there is possibility of confusion, i.e. misrepresentation of the scope or collision with other sections of SADD, the ERA Subject Area name is qualified or renamed (e.g. to the industry standard name).

NARA has used Information Engineering (IE) techniques to perform this decomposition. However, UML does have a hierarchical construct (the Package) that can capture this information. One of the key advantages of UML is that it provides a seamless language that allows designs to be drilled down into more detail without the need for any change in modeling constructs. Hence, package diagrams are created to illustrate this hierarchy of classes and their dependencies on each other. To ensure that the hierarchical levels are distinguished from any other packages in the model, the LM Team defines two UML stereotypes <<Data Category>> and <<Subject Area>> which, when applied to UML packages, identify their hierarchical level.

The simple object model representation of the conceptual model is achieved by expanding the data types comprising ERA Subject Areas into simple object packages. These classes are named and defined and the relationships among them are defined. However, at this point no attributes are added.

Also, note that to avoid confusion the NARA subject area "Documentary Material" will be referred to by its expanded name "Documentary Material Subject Area".

2.11.2 Methodology for the Logical Model

The logical model further decomposes the conceptual model classes to define:

- Object classes
- Attributes
- Cardinalities

Each of these classes is contained within a UML package named the same as the conceptual model class. This simplifies the mapping between these models.

The relationship between the object classes can be:

- **Association:** This indicates that the two classes are related. The relationship may be one-to-one, one-to-many or many-to-many. Some many-to-many relationships will be resolved into Association classes if this illustrates an important concept.
- **Inheritance:** This relationship indicates that a sub-class is inherited from a super-class. The sub-class inherits all the attributes of the super-class and has additional attributes.
- **Aggregation:** The relationship indicates that the aggregate class is made up of the other classes but the associated classes have an existence independent of the aggregate class.
- **Composition:** The relationship indicates that the dependent classes are a part of the composing class (i.e. the related classes have no existence independent of this class).

All of this information is modeled using UML class diagrams with an associated data dictionary.

2.11.3 Logical Model Development

The ERA conceptual data model is made up of six Data Categories each decomposed into a set of Subject Areas as described in Section 2.11.6.2. Each of the Subject Areas in the conceptual model is presented as a collection of Simple Objects. These Simple Objects form the starting point for the development of the logical model.

In the logical model each of the Simple Objects from the conceptual model is represented as a UML package. Additional packages are created as needed during the logical model design. The contents of each UML package contain:

- Object classes
- Association classes (If the association itself is an impotant concept)
- Key Attributes
- Cardinalities

The LM Team has intentionally defined its data classes with only attributes and no operations. This stems from a design decision to keep all operations in the services in the Service Oriented Architecture and the data classes limited to structural information to promote the concept of the persistent archives. The services can be thought of as classes with only operations and no attributes. This, too, stems from a design decision to keep all services stateless; in other words, they have no persistent state that would normally be contained in attributes. The notation for class diagrams are shown in Appendix C.

The logical model also includes the composite classes for the objects that were used for the data flow in the System-level packages such as Ingest, Records management, Storage, Preservation, and Dissemination, and for the interfaces. The messages such as "Request", "Status" or "Notification" that appear as data objects on sequence diagrams are not part of persisted data. Hence they are not included in the data model.

2.11.4 Derived Entities

The logical data model represents the set of business objects that will be persisted by the system. In some cases the data transmitted within the system via message passing will not correspond directly to the entities described above: composite entities will sometimes be used (e.g., when creating a Transfer) or partial entities (e.g., if a search returns a list of records, it will only return part of the information held on these records).

2.11.5 Conformance to NARA EA Data Architecture

Table 45 through Table 47 demonstrates the ERA System Data Architecture's compliance with each of the data principles, constraints and assumptions contained in the NARA Enterprise Architecture (EA) Data Architecture.

Table 45 – ERA System Data Architecture Compliance with NARA Data Architecture Principles

EA Data Architecture Principle	ERA System Conformance
NARA enterprise data will be managed and protected as an agency asset	This has been achieved by the creation of a NARA Data Architecture and data integrity and security policies with which the ERA data architecture is compliant. In addition data is replicated.
NARA enterprise data will be presented to the business users in a format appropriate to business needs	The ERA System data comes in many formats and is presented in a format appropriate to business needs. For example, different classes of internal users will use different workbenches that will be tailored to allow them to work efficiently and consumers will be able to see many manifestations of records through digital adaptation for output.
NARA enterprise data will be organized and stored in a manner that optimizes performance, as well as assures integrity and maintainability	The ERA System data is organized and stored in a manner that optimizes performance, as well as assures integrity and maintainability. Performance will be optimized through the use of a configurable and scalable arrangement of sites (and data servers within sites).

EA Data Architecture Principle	ERA System Conformance
Enterprise data created during the course of NARA's business will have common definitions and consistent usage across the enterprise	• The ERA System data created during the course of NARA's business has common definitions and consistent usage across the enterprise. • The ERA System is designed to consistently enforce the use of common data definitions and data standards across the agency by generating and maintaining a glossary. For example, many templates will include the use of authority sources to restrict the allowed values of data. • The ERA System data administration will have the tools to conduct periodic quality reviews to ensure that enterprise data is in compliance with this principle. The reviews will be based on quality metrics and measurement standards adopted from the industry and/or developed within NARA.
NARA will provide quality information products according to the NARA Information Quality Guidelines	• The ERA System provides quality information products according to the NARA Information Quality Guidelines; the dissemination process conforms to these guidelines. • As written, an excerpt from this guideline states that the quality guidelines describe procedures that NARA uses to assure the quality of NARA's information products including their utility, objectivity and integrity.
NARA's Data Architecture will evolve to support the requirements of the Federal Government	Regular reviews are carried out so that the ERA data architecture supports the requirements of the Federal Government.
NARA will control data redundancy as well as promote data interoperability and data sharing	By following a normalization process, the ERA data design has control over data redundancy. By careful data modeling, the ERA data architecture promotes data interoperability and data sharing.
NARA's Data Architecture will specify standard data access interfaces to business applications	The ERA data architecture specifies standard data access interfaces to business applications by a layer of Local Common Services.
Every data class of the NARA Conceptual Data Model will have at least one business owner who controls and manages that data class	Every data class of the ERA Conceptual Data Model has at least one business owner who controls and manages that data class.
The NARA Glossary will be managed and controlled at the NARA enterprise level to help achieve enterprise-wide data integration	The ERA Glossary is managed and controlled at the NARA enterprise level to help achieve enterprise-wide data integration.

EA Data Architecture Principle	ERA System Conformance
NARA's data will be made available to anyone with a credible need and authorization for use	The ERA System's data is made available to anyone with a credible need and authorization for use. The credibility and authority of requester are verified by security procedures. Further, the redaction process is used to make data available conforming to the authority of requester.
NARA's electronic information assets will be location transparent	The ERA System's electronic information assets are managed in such a way as to be location transparent. The ERA System insulates the data by allowing access through Local Services and Control services. The requester is presented a workbench without exposing the location of the data.
NARA will assure the confidentiality, integrity, and availability of its information assets	The ERA System design assures the confidentiality, integrity, and availability of its information assets by incorporating industry standard procedures modified as required to meet ERA standards,

Table 46 – ERA System Data Architecture Compliance with NARA Data Architecture Constraints

EA Data Architecture Constraint	ERA System Conformance
Commercial-off-the-shelf (COTS) products will generally implement product specific data security and authorization controls within their databases and applications. These product specific controls may not conform to NARA's security standards	The ERA System is designed so that it has guidelines for reviewing the data security measures implemented by COTS products and assessing the risks of those measures to the agency.
Since all modeling paradigms are limited in their ability to accurately and completely represent real-world phenomena, not all data business rules can be represented as data modeling structures	The ERA System automates all data business rules that can be represented within the data models.
The dynamic aspects of NARA's enterprise data will not be well-represented by static data modeling methods such as Entity-Relationship (ER) diagrams or UML class diagrams	The dynamic aspects of the ERA System data are represented by using the applicable aspects of Entity Relationship diagrams, UML class diagrams, Information Engineering, XML Schemas and extensions of these methods as required.
Because business terms may be used in different contexts, multiple definitions for business terms should be expected	The ERA System aggressively manages the semantics of business terminology across IT automation projects for data elements that are expected to have a high degree of reuse across the agency. The overused terms are qualified with adjectives indicating the context e.g. Policy had different meanings in the management context and the security context. The term policy is qualified with appropriate adjectives.
Many legacy systems do not provide standards-based data integration support, therefore, system-to-system interfaces and data transformations may be required to access and integrate the data contained within legacy systems	The ERA System has developed custom interfaces to integrate legacy data stores.
Enterprise Data Architecture is inherently a high-level design perspective that is meant to assure the consistency and interoperability of data across all systems in the enterprise rather than to address the implementation details of specific systems	The ERA System Data Architecture specifications and processes are designed with enough flexibility to absorb unforeseen changes without major impact.
Security and privacy imperatives may restrict NARA's ability to provide certain data to other governmental agencies, non-governmental entities, and individuals	The ERA System uses redaction and access policies to provide data to other governmental agencies, non-governmental entities, and individuals

Table 47 – ERA System Data Architecture Compliance with NARA Data Architecture Assumptions

EA Data Architecture Assumption	ERA System Conformance
NARA's Data Architecture must comply with E-Government principles and guidelines for data interoperability and sharing	"Implementing the President's Management Agenda for E-Government Strategy", issued by the Executive Office of the President of the United States, states three principles: Citizen-centered, Results-oriented and Market-based. The ERA System follows these guiding principles.
XML is emerging as a standard for moving and sharing information among different organizations and systems	• XML is emerging as a standard for moving and sharing information among different organizations and systems. • The ERA Data Architecture ensures that the XML specifications asserted by NARA data standards, strategies, and guidance are well supported outside NARA and in alignment with the industry trends for XML.
NARA will develop standards for data transformation and transport to facilitate data sharing	The ERA System has developed standards for data transformation and transport to facilitate data sharing.
Data diagnostic and analysis processes will be implemented to track and report data inconsistencies	• The ERA System has developed standards and metrics to define the measures and tolerances for data inconsistencies. • The ERA System has developed analytical and diagnostic processes that are designed to track and report data inconsistencies and are available for dissemination. • The ERA System has procedures to implement the analytical and diagnostic processes through data quality audits and reviews.
NARA's business and IT support staff will work in partnership to ensure data quality for the agency	The ERA System's business and IT support staff works in partnership to ensure data quality for the agency. A key aspect of the flexibility is the use of Templates in the data design.
Data requirements will evolve and change as a result of Business Process Reengineering (BPR) efforts and IT systems redesign efforts	The ERA Data Architecture is flexible enough to absorb and reflect any additional data requirements discovered during BPR and IT systems redesign efforts.
The Life Cycle Data Requirements Guide is a recognized standard, but will continue to evolve	The ERA Data Architecture is flexible enough to absorb and reflect any data requirements precipitated by the Life Cycle Data Requirements Guide. In particular, life cycle data requirements are met through the use of templates, which build in inherent flexibility.
When business requirements impose demands that conflict with the Data Architecture, the data architecture will be adjusted to accommodate those demands	ERA data architecture is flexible enough to adjust to and reflect changes imposed by business requirements. As well as the use of Templates, described above, the entire ERA System design is designed to be loosely coupled hence reducing the impact of even unforeseen future change. In particular, within the Data Architecture, the hierarchical use of Packages helps to limit the dependency of one part of the model on other parts.

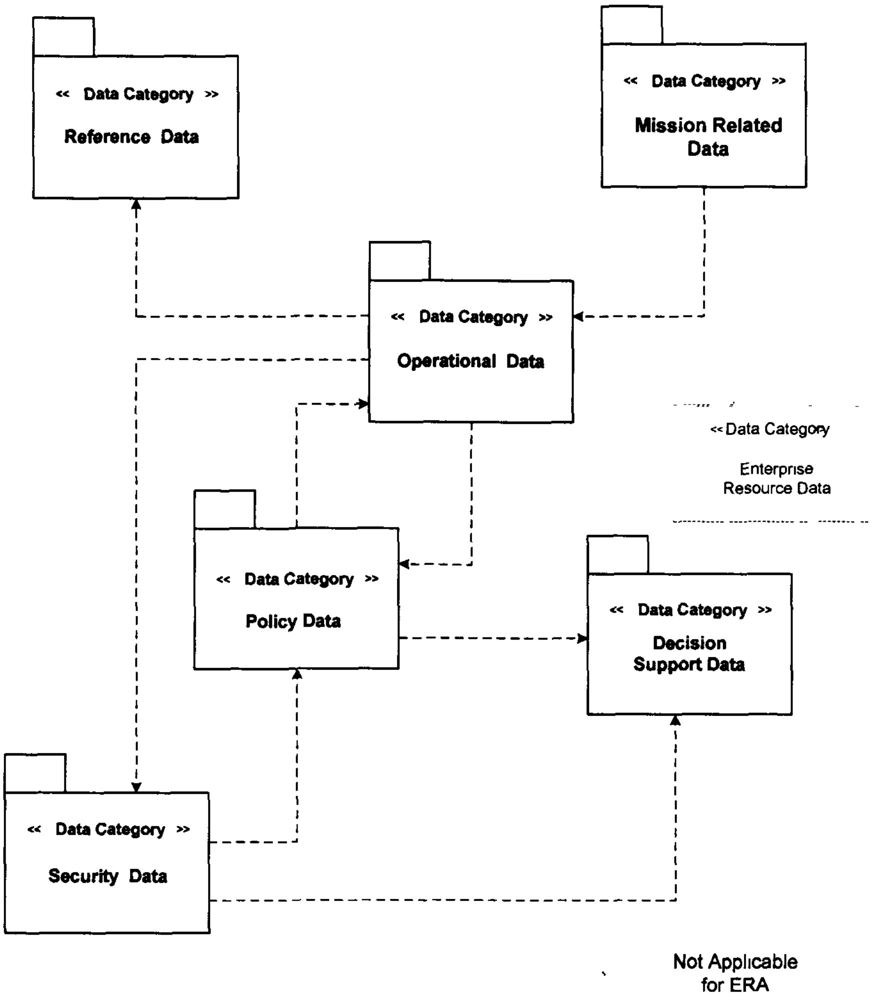
2.11.6 ERA Conceptual Data Model

As described in the methodology section the conceptual data model consists of a Data Category view, a Subject Area view and a Simple Object Model view. These three views of the conceptual model are presented in this section of the document.

2.11.6.1 Data Category View

Figure 32 shows the highest level of the conceptual view of the ERA System data model as represented by a UML package dependency diagram. It consists of the data categories and their relationships taken from the NARA conceptual data model that are relevant to the ERA conceptual model. The Enterprise Resource Data category is shown in a dotted line box since it is not relevant to the ERA System. The constituent subject areas described in the next section characterize the data categories.

Figure 32 – ERA Conceptual Model: Data Categories

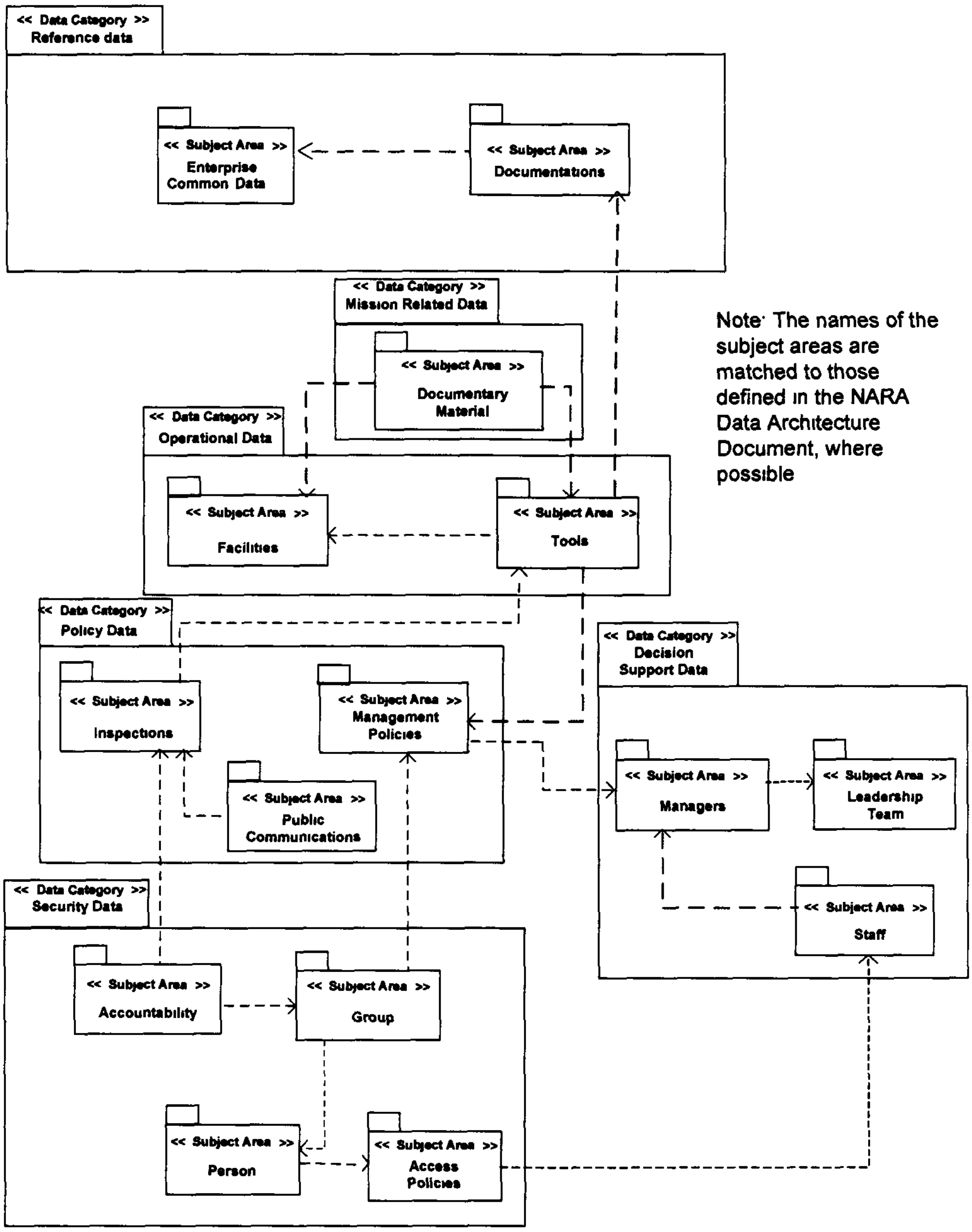


ERA_ENG_028a

2.11.6.2 Subject Area View

Figure 33 shows the next level of the conceptual view of the ERA System data model as represented by a UML package dependency diagram. It consists of the NARA Subject Areas within the identified Data Categories and their relationships. As described in the Methodology section above, not all NARA Subject Areas are relevant to the ERA System; only the Subject areas relevant to the ERA System have been included (see Table 48.)

Figure 33 – ERA Conceptual Model: Subject Areas



<< Data Category >> Reference data
<< Subject Area >> Enterprise Common Data
<< Subject Area >> Documentations
<< Data Category >> Mission Related Data
<< Subject Area >> Documentary Material
<< Data Category >> Operational Data
<< Subject Area >> Facilities
<< Subject Area >> Tools
<< Data Category >> Policy Data
<< Subject Area >> Inspections
<< Subject Area >> Management Policies
<< Subject Area >> Public Communications
<< Data Category >> Decision Support Data
<< Subject Area >> Managers
<< Subject Area >> Leadership Team
<< Subject Area >> Staff
<< Data Category >> Security Data
<< Subject Area >> Accountability
<< Subject Area >> Group
<< Subject Area >> Person
<< Subject Area >> Access Policies

Note· The names of the subject areas are matched to those defined ın the NARA Data Archıtecture Document, where possıble

ERA_ENG_029c

In addition, in some other cases, the distinction between two or more NARA subject areas is not relevant at this level of conceptual modeling. ERA Subject Areas are defined and mapped to the

NARA Subject Areas in Table 48. For the most part, the NARA subject area names are used for the corresponding ERA Subject Area. Where there is possibility of confusion, i.e., misrepresentation of the scope or collision with other sections of SADD, the ERA Subject Area name is qualified with a qualifier or renamed.

Table 48 – ERA Subject Areas

Data Category	NARA Subject Areas	ERA Subject Area	Description of ERA Subject Area
Policy Data	Policies	Management Policies	These are ERA management policies that act as driver for the ERA System activities
	Plans	N/A	
	Directives	N/A	
	Oversight	N/A	
	Legal	N/A	
	Inspections	Inspections	These include certification and accreditations
	Communications	Public Communications	These define the communications from the ERA System to the public
Mission-related Data	Documentary Material	Documentary Material Subject Area	This subject area covers all the information held about NARA's holdings that are within the scope of the ERA System. This includes all of NARA's documentary material, their descriptions, provenance and disposition agreements as well as electronic record specific information such as the conceptual and physical views of records and templates. Its scope is the same as the Record, Disposition, Document and Description Packages as defined by the document ERA DOMAIN MODEL, EDM v1.0, WBS #1.1.15.4, November 22,2004
	Parties	N/A	
	Grants	N/A	
	Events	N/A	
	Merchandise	N/A	

Data Category	NARA Subject Areas	ERA Subject Area	Description of ERA Subject Area
	Legal Publications	N/A	
Operational Data	Lines of Business	N/A	
	Tools	Tools	Tools include all the tools such as software, Help Desk and other data required for the system operation
	Facilities	Facilities	Facilities include all the data of the facilities.
Decision Support Data	Leadership Team	Reports	These are various reports created to assist the corresponding personnel to make decisions
	Managers		
	Staff		
Enterprise Resource Data	Finance	N/A	
	Accounts	N/A	
	Procurements	N/A	
	Contracts	N/A	
	Human Resources	N/A	
	Payroll	N/A	
	Technology	N/A	
Security Data	Access	Access Policies	These policies define the rules for granting access to assets entrusted to the ERA System.
	Authorizations	Group	Group defines the roles based on the access policies.
	Authentications	Person	This is the user data that includes user identification information and group to which the user belongs.
	Audit	Accountability	These various logs including event logs, audit logs, etc.
Reference Data	Internal/External Standards	Documentations	Documentation for all standards, glossaries, frameworks and architecture.
	Glossaries		

Data Category	NARA Subject Areas	ERA Subject Area	Description of ERA Subject Area
	Frameworks		
	Architectures		
	Enterprise Common Data	Enterprise Common Data	This includes all the common ERA System-wide data including Authority Sources.

2.11.6.3 Simple Object Model View

The final level of the conceptual model hierarchy is the simple object model. Each of the subject areas illustrated in Table 48 and Figure 33 are decomposed into a series of simple objects. Where appropriate, dependencies are shown on the simple object views. This forms the starting point for the development of the logical model, where the simple objects are fully decomposed.

2.11.6.3.1 Mission Related Data Object Model View

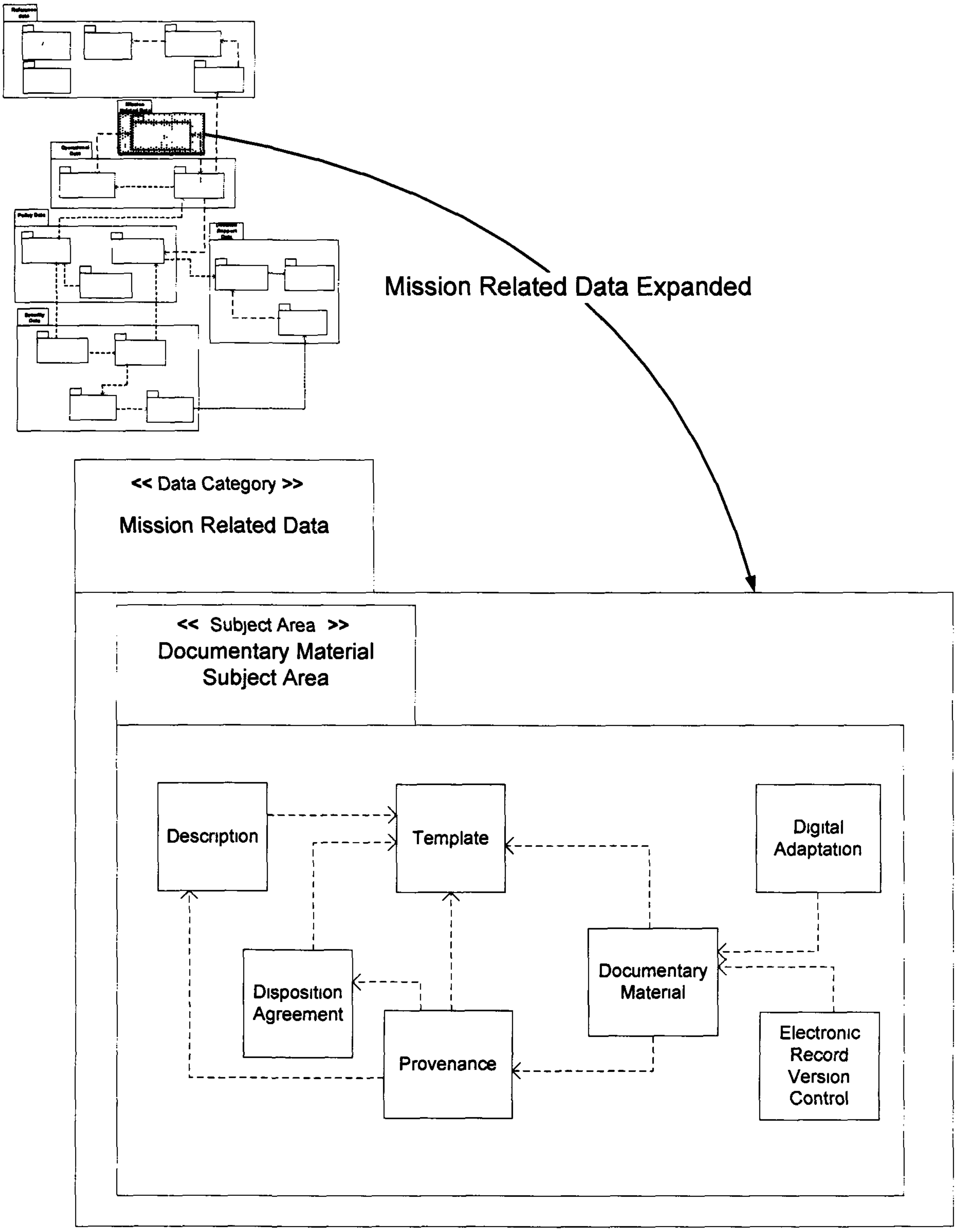
The subject areas of this data category consist of the conceptual objects listed in Table 49. Figure 34 illustrates the Mission Related Data Object model view. This data category is composed of a single package Documentary Materials Subject Area. The object model view of the this package is based on the NARA supplied document "ERA Domain Model", EDM v1.0, WBS #1.1.15.4, November 22, 2004.

Table 49 – Mission Related Data Object Model View

Subject Area	Simple Objects	Simple Objects Description
Documentary Material Subject Area	Documentary Material	This simple object is any documentary material that can be held by NARA. It contains parts of the Record, Document and Description packages described in the NARA supplied domain model.
	Provenance	This simple object is the hierarchical arrangement of documentary materials based on their provenance and/or some archivally-imposed order. It contains parts of the Record and Description Packages described in the NARA supplied domain model.
	Disposition Agreement	This simple object is the disposition agreement associated with a documentary material together including all its constituents and related material (e.g., appraisal reports etc.). It maps directly to the Disposition package described in the NARA supplied domain model.
	Description	This simple object is the Description for a Documentary Material based off one or more templates. It contains part of the Description package described in the NARA supplied domain model.

Subject Area	Simple Objects	Simple Objects Description
	Electronic Record Version Control	This simple object is a conceptual electronic record. It includes all of the record's metadata and all of the various manifestations of that record including links to the data files that make up those manifestations but it does not include the files themselves. It is based on parts of Document package described in the NARA supplied domain model.
	Digital Adaptation	This simple object is a physical electronic record that consists of the data files that make up each manifestation of that record together with information on the source of that information (e.g., whether it was a supplied accession or created through digital adaptation). It is based on parts of Document package described in the NARA supplied domain model.
	Template	This simple object contains all the templates including the template registry.

Figure 34 – Mission Related Data Object Model View



ERA_ENG_030b

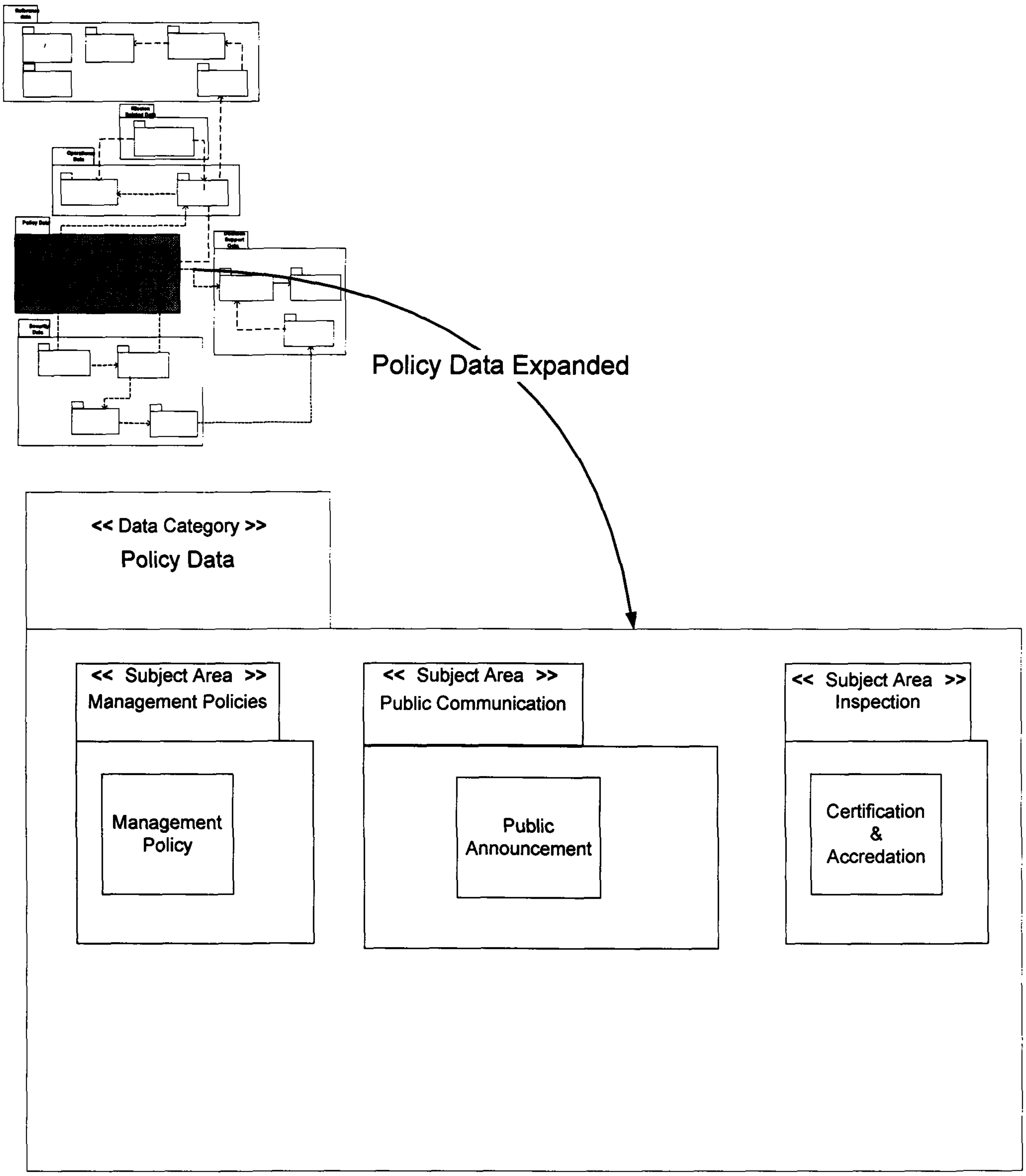
2.11.6.3.2 Policy Data Object Model View

The subject areas of this data category consist of the conceptual objects listed in Table 50. Figure 35 illustrates the Policy data object model view.

Table 50 – Policy Data Object Model View

Subject Area	Simple Objects	Simple Objects Description
Management Policies	Management Policy	This simple object defines the policies governing the ERA System activities (e.g., workflow management).
Public Communications	Public Announcement	This simple object defines the public announcements made by the ERA System (e.g., announcements on the portal).
Inspection	Certification & Accreditation	This simple object is responsible keeping track of certification and accreditation process for the in-house and COTS software.

Figure 35 – Policy Data Object Model



ERA_ENG_031a

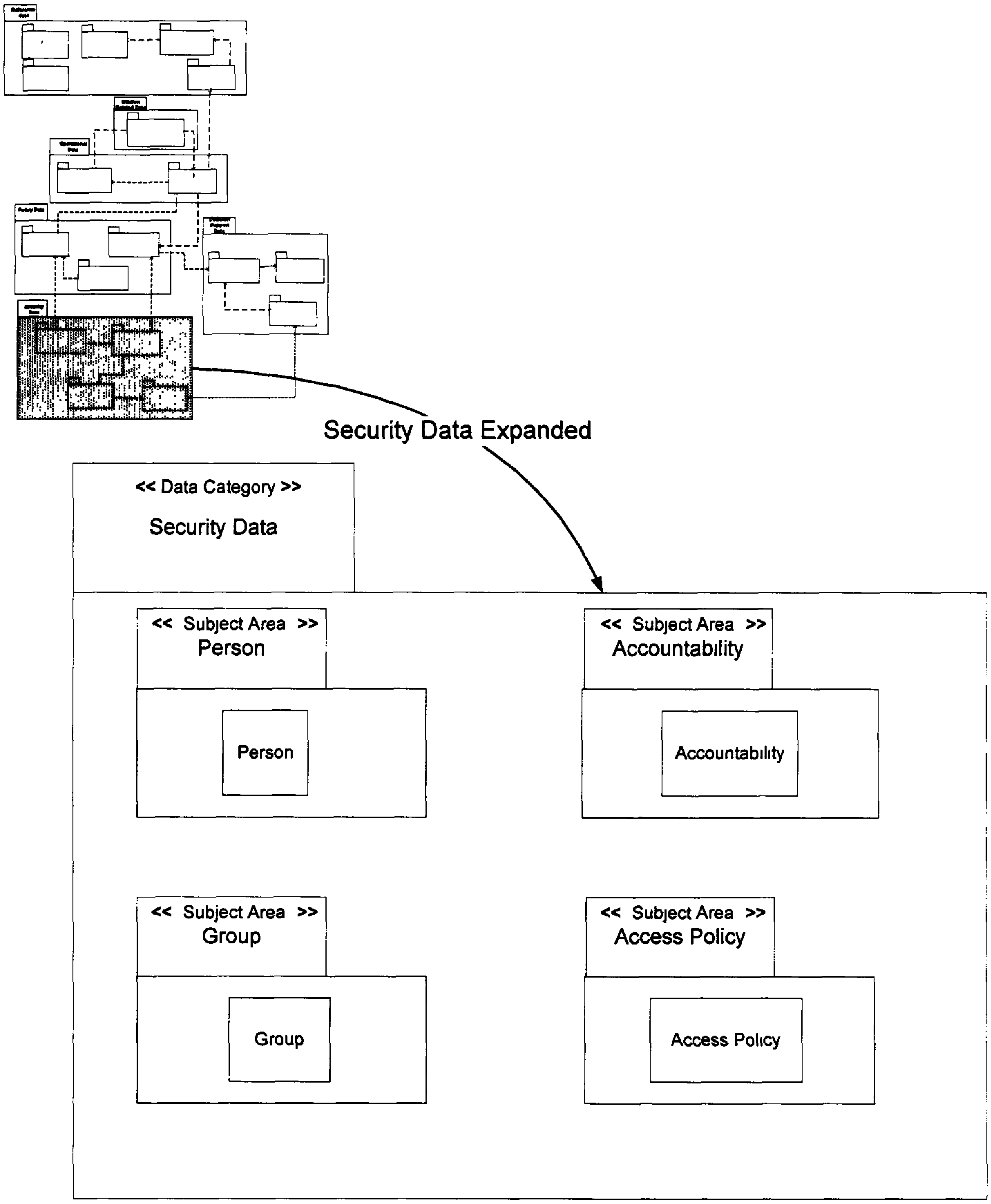
2.11.6.3.3 Security Data Object Model

Figure 36 illustrates the Security Data Object Model, which consists of four objects defined in Table 51.

Table 51 – Security Data Object Model

Subject Area	Simple Objects	Simple Objects Description
Person	Person	This simple object tracks the user information such user id, name, etc.
Group	Group	This simple object defines group members, which are people and other groups.
Access Policies	Access Policy	This simple object manages access policies by mapping groups in the Directory to roles in an application, or to asset or service access restrictions.
Accountability	Accountability	This object created to track of event logs and audit logs.

Figure 36 – Security Object Model



ERA_ENG_032b

2.11.6.3.4 Operational Data Object Model View

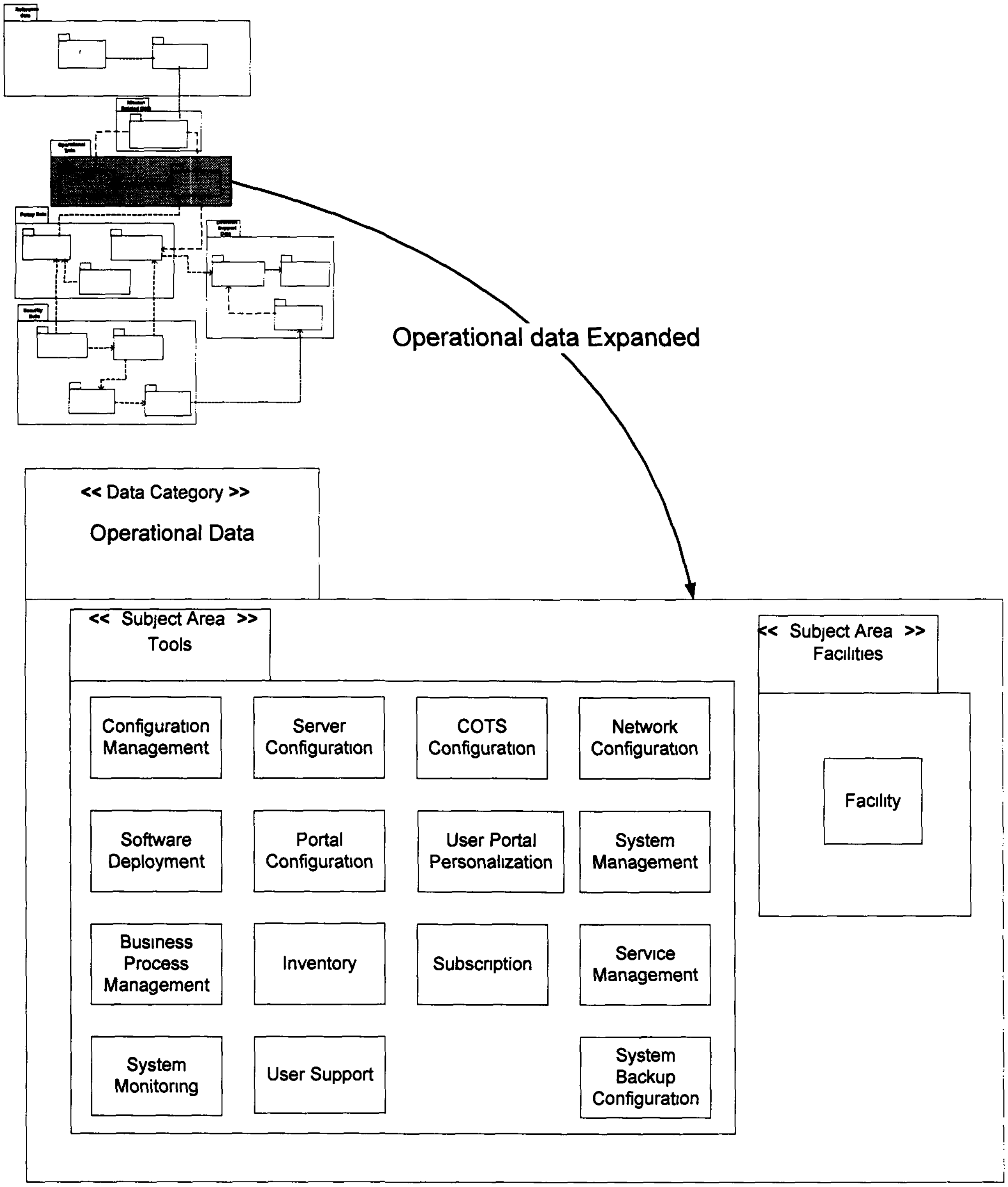
In the simple objects model view, this data category consists of the following simple objects as described in Table 52. Figure 37 illustrates the Operational data object model view.

Table 52 – Operational Data Object Model

Subject Area	Simple Objects	Simple Objects Description
Facilities	Facility	This simple object tracks the facility information such as address, area, etc.
Tools	Configuration Management	This simple object consists of classes to perform configuration management for software, ERA documents, etc.
	Software Deployment	This simple object consists of classes to track the Deployment of Software Operating Systems, Software developed in house, COTS products and Application Software.
	Business Process Management	This simple object consists of classes to define orchestrations and business rules.
	System Monitoring	This simple object consists of classes of to monitor the systems.
	Server Configuration	This simple object consists of classes to keep track of the server configuration data.
	Portal Configuration	This simple object consists of classes to keep track of the Portal configuration data.
	Inventory	This simple object consists of classes to track physical inventory including consumables and software.
	User Support	This simple object consists of classes to track the help desk activities such as trouble tickets and mediated searches.
	COTS Configuration	This simple object consists of classes to keep track of the COTS product configuration data.
	User Portal Personalization	This simple object consists of classes of to keep track of the user personalization data for the personalization of the portals.
	Subscription	This simple object consists of classes to track the subscriptions for users, agencies and other entities.
	Network Configuration	This simple object consists of classes to keep track of the Network Configuration data.

Subject Area	Simple Objects	Simple Objects Description
	System Management	This simple object consists of classes to keep track of the System Management data.
	Service Management	This simple object consists of classes to keep track of the Service Management data and Service interface data required flowing from the ERA System to the interacting entities.
	System Backup Configuration	This simple object consists of classes to keep track of the System Backup Configuration data.

Figure 37 – Operational Data Object Model



ERA_ENG_033d

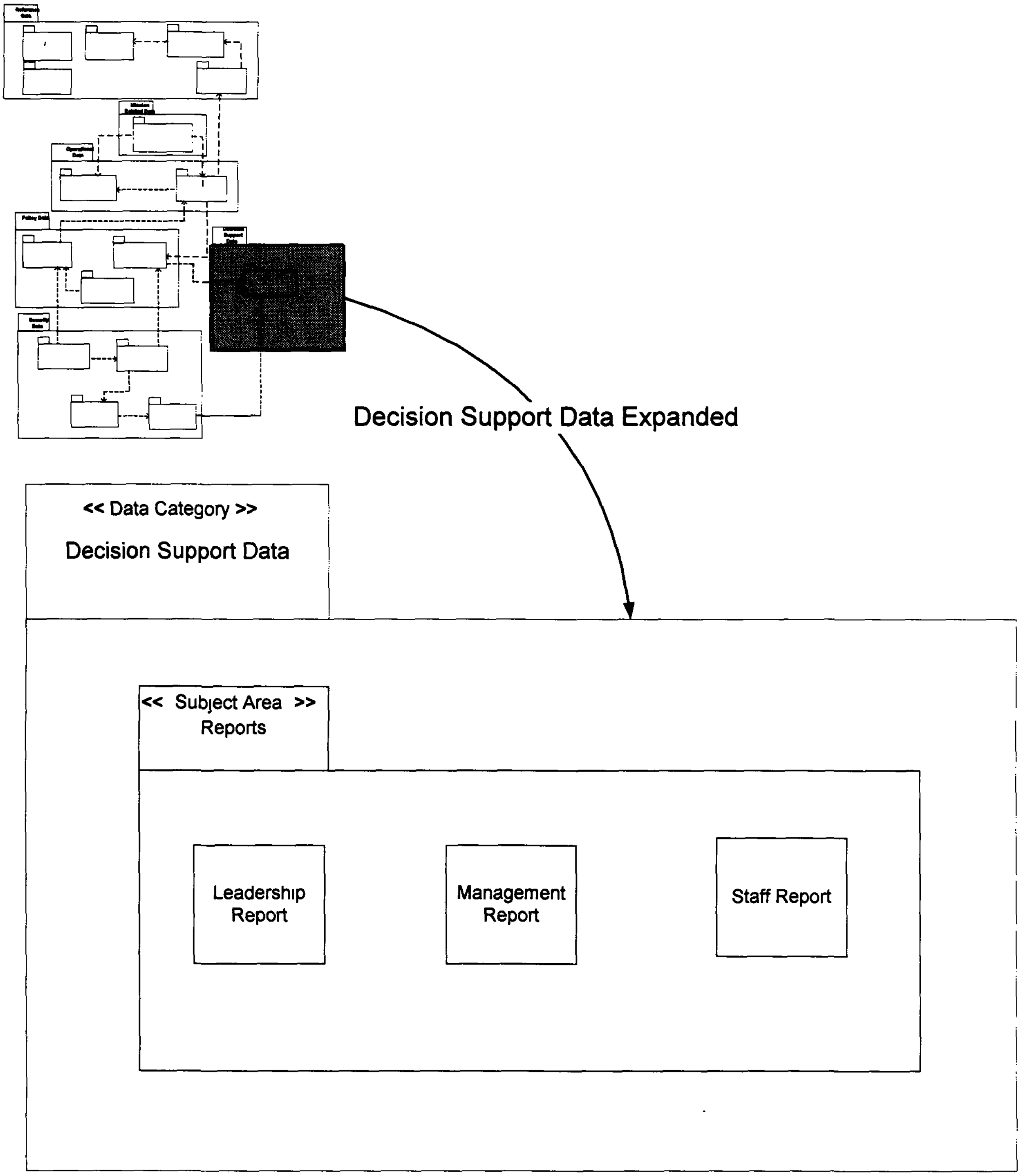
2.11.6.3.5 Decision Support Data Object Model View

The object view of this data category consists of one simple object, Reports, as listed in Table 53. Figure 38 illustrates the Decision Support data object model view.

Table 53 – Decision Support Data Object Model

Subject Area	Simple Objects	Simple Objects Description
Reports	Leadership Report	This simple object tracks the reports created for executives to assist in making leadership decisions.
	Management Report	This simple object tracks the reports created for managers to assist in making management decisions.
	Staff Report	This simple object tracks the reports created for staff to assist in making day-to-day operation decisions.

Figure 38 – Decision Support Data Object Model



ERA_ENG_034b

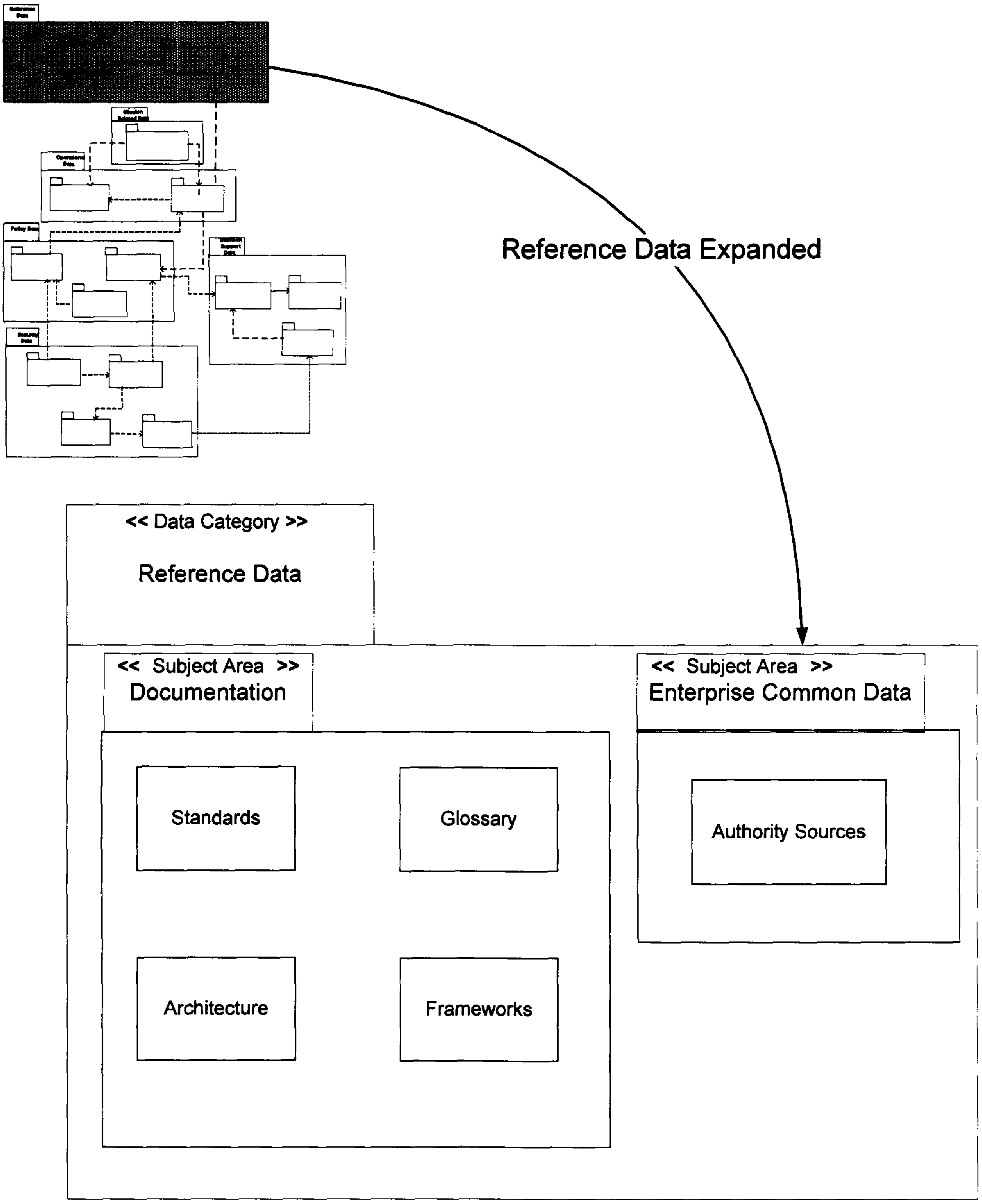
2.11.6.3.6 Reference Data Object Model View

The object view of this data category consists of the simple objects shown in Table 54. Figure 39 illustrates the Reference Data object model view.

Table 54 – Reference Data Object Model

Subject Area	Simple Object	Simple Object Description
Documentation	Standards	This simple object consists of classes to store the internal and external standards.
	Glossary	This simple object consists of a class to keep the glossary for the ERA System wide use to ensure consistency and uniformity.
	Architecture	This simple object consists of a class to keep the ERA System architecture information.
	Framework	This simple object consists of a class to keep the ERA System framework that will make it easier to find specific information. This framework is based around the records life cycle.
Enterprise Common Data	Authority Source	This simple object keeps track of the thesaurus containing standardized information.

Figure 39 – Reference Data Object Model



ERA_ENG_035b

This data model addresses only that data that is global to the ERA System, and is persisted. Data that is encapsulated within a given service and data that is transient are not included in this data model.

The ERA data modeling follows the methodology described in the NARA Data Architecture document. The methodology consists of a hierarchy of modeling steps each adding more detail than the previous:

- The conceptual data model, which defines data elements and their interactions at the real-world, domain level without particular regard for how this will be implemented. The NARA ERA Domain Model is the conceptual data model.
- The simple conceptual object model is then decomposed into a logical model, which states how the system will be developed at the application systems design perspective. Starting from the objects in the conceptual simple object model, a complex object model is developed.
- The logical model is further developed into a physical model, which states how the system will be implemented (e.g., as a relational database schema, XML schema etc.). This model is then subject to Critical Design Review (CDR).
- The physical model then forms the basis for the implementation.

The following sections describe the methodology and development of the logical model and its components.

2.11.7 Data Replication Architecture

The ERA System is a distributed system, and as such requires data replication among the Instances, and up/down from the central management suite, to ensure that all Instances have an available and current copy of mission, security, and operational data. This allows any Instance to operate, with limited degradation, when access to other Instances or to the ERA Management system-level package is unavailable. Specific data that require replication include:

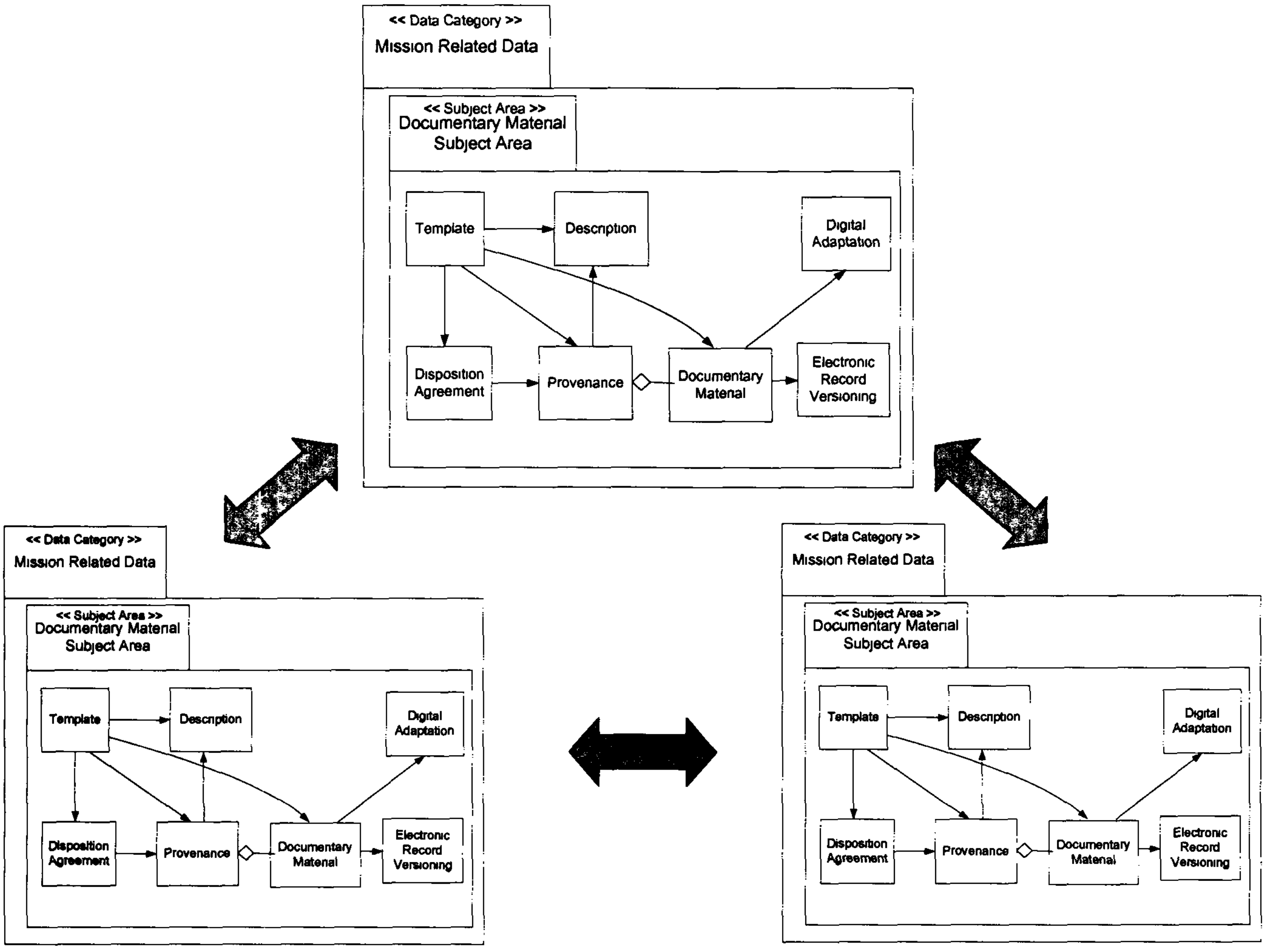
- Mission Data
  - Documentary Material Data
- Security Data
  - User, group, and access policy data
  - Accountability data
- Operational Data
  - Deployed Software
  - Deployed configuration data
  - System monitoring data
  - Inventory data
  - Business Rules
  - Portal Personalization Data
  - Subscription data

2.11.7.1 Replication of Mission Data - Documentary Material Data

The Mission data category's subject area of Documentary Material data is replicated from ERA Instance to ERA Instance, within a Federation at a single data classification (see Figure 40). It is important to note that the replication of Documentary Material data does not include replicating electronic records. The replication of electronic records is managed using the Active Safe-Store described in Section 2.9.1. Documentary Material data can be created or updated at any ERA Instance, and replication ensures that all Instances have the same, current data. This replication "on create" or "on change" limits the network traffic and ensures availability, versus requesting the same data from another Instance many times upon each access request. If more than one Instance makes a change to a datum, rules such as declaring the authoritative source to be the Instance at which entry was most recently updated will be used to resolve replication conflicts.

Archival records themselves, and the Archival Information Package of which they are a component, are not subject to this replication as they are managed using the Active Safe-Store.

Figure 40 – Replication of Documentary Material Data



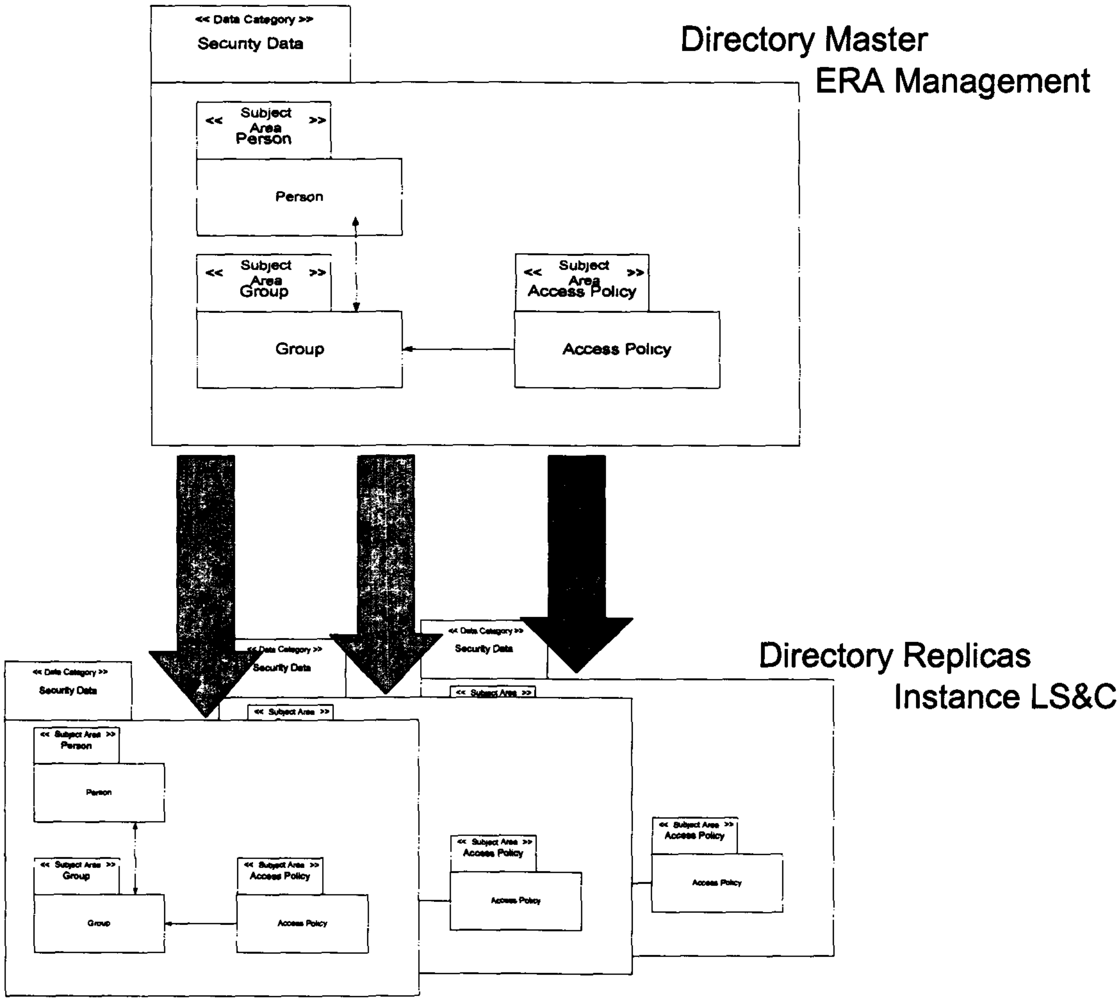
ERA ENG 036a

Note: In this figure, Documentary Material does not include electronic records.

2.11.7.2 Replication of Security Data

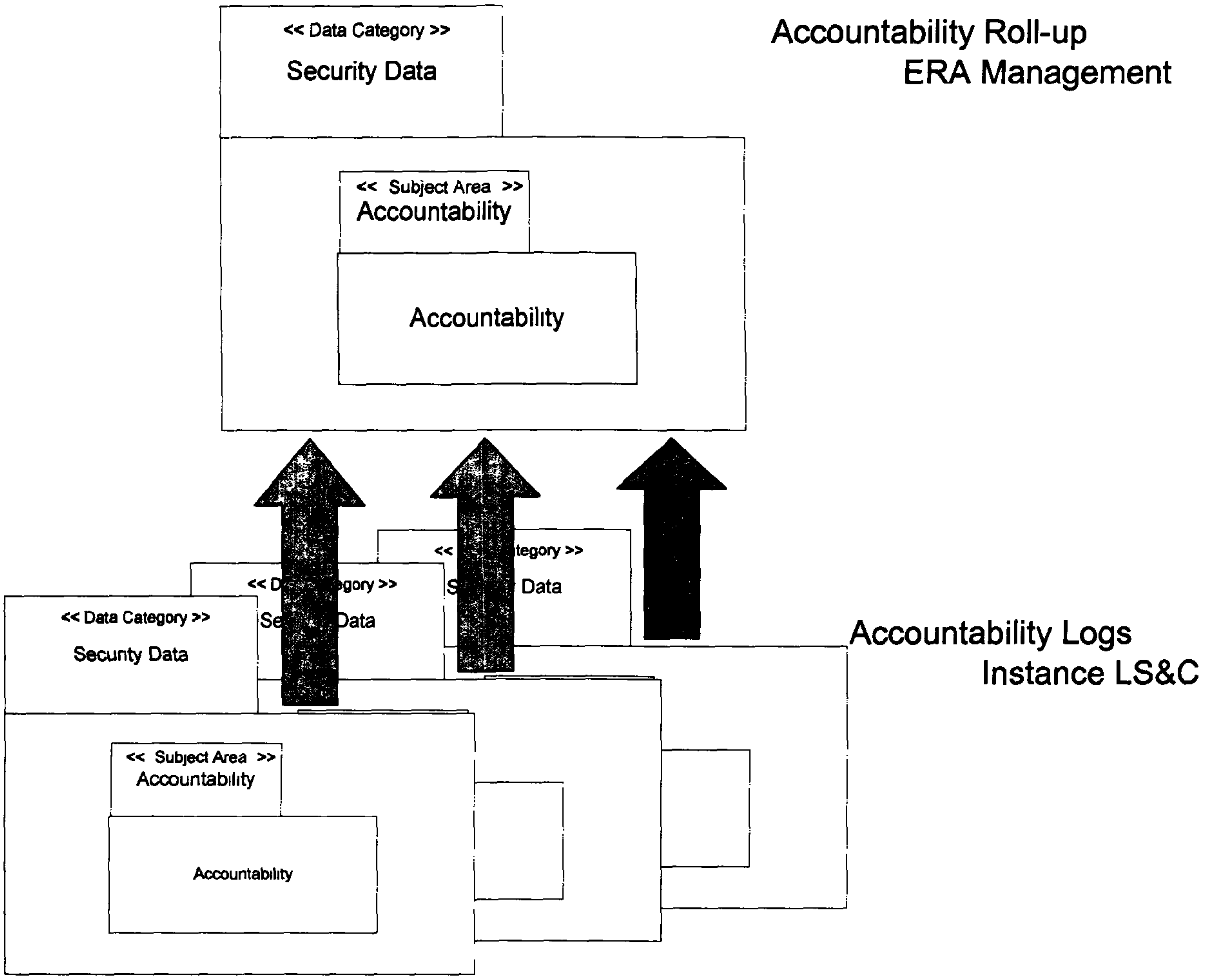
Security data, including authentication and authorization data, must be highly available. If access to authentication and authorization data is lost, user access to all ERA System services and assets is also lost. The authoritative source for all user data is the Directory Master at the ERA Management system-level package. Replication of user data is from this Directory Master to replica Directories located at each Instance (see Figure 41). This ensures that a local copy is available at each Instance. In the event that access from ERA Management to an Instance is lost, the Instance can continue to operate fully, but Directory updates including new account creation and password changes will not propagate to the Instance until connectivity is restored.

Figure 41 – Replication of User Security Data



Accountability data includes error, event, and audit logs. This data is created at each local Instance, and selected accountability data is replicated up the ERA Management system-level package (see Figure 42). ERA System-level audit and event reports are generated from the centralized, rolled-up data, but any detail not rolled-up from an Instance is available for drill-down on those occasions where detailed error or event logs are needed for problem diagnosis, or when audit logs are needed for security investigations.

Figure 42 – Replication of Accountability Security Data



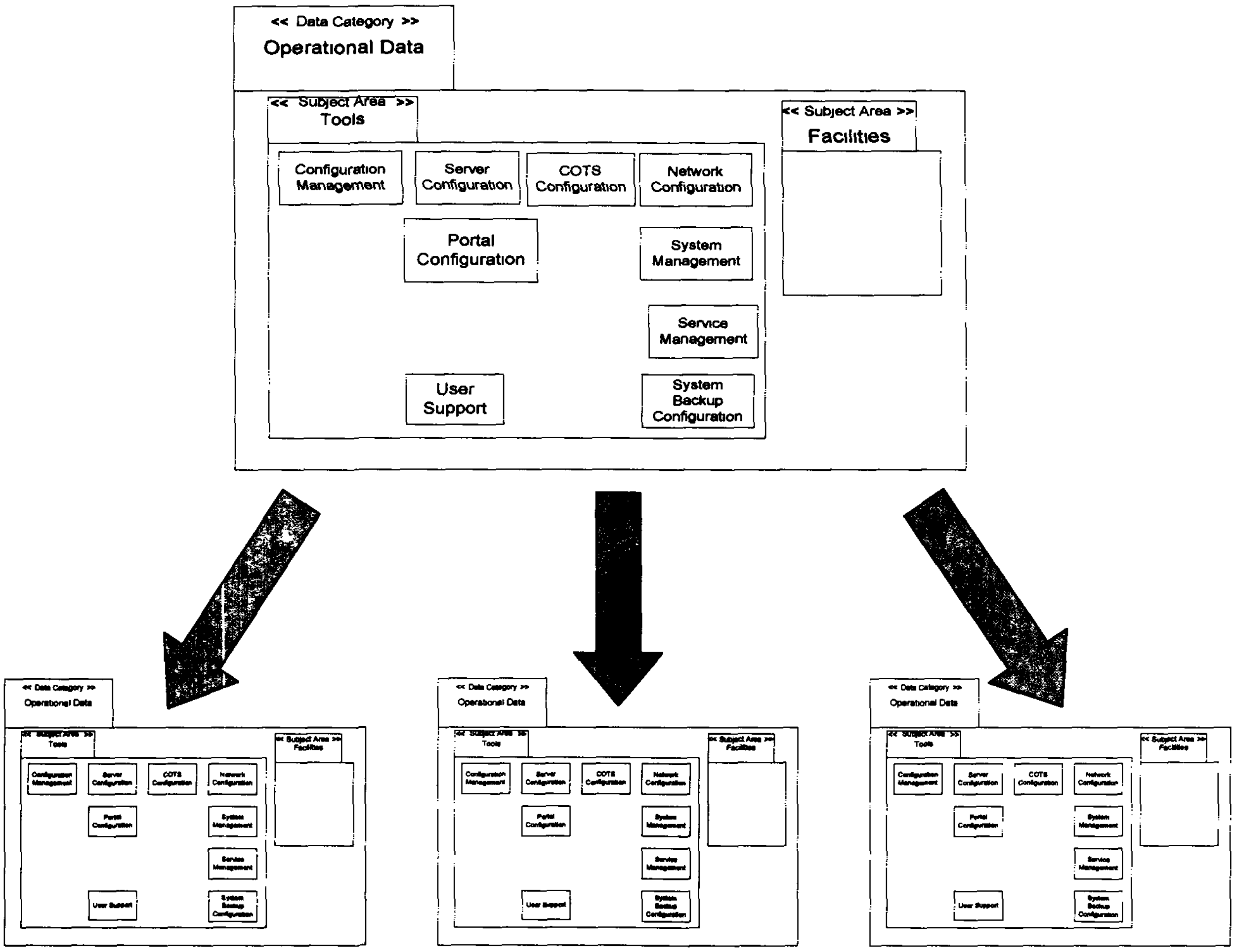
2.11.7.3 Replication of Operational Data

Operational data that must be replicated among the ERA Management system package and the distributed Instances comprises:

- Centrally generated, distributed data, including: Operating Systems, COTS, Global Configuration Data, Local Configuration Data, and Developed Code
- Locally generated, centrally used data, including: Operations Monitoring Data and Inventory Data
- Locally generated, distributed data, including: Business Rules, Portal Personalization Data, Subscriptions, and Service Management

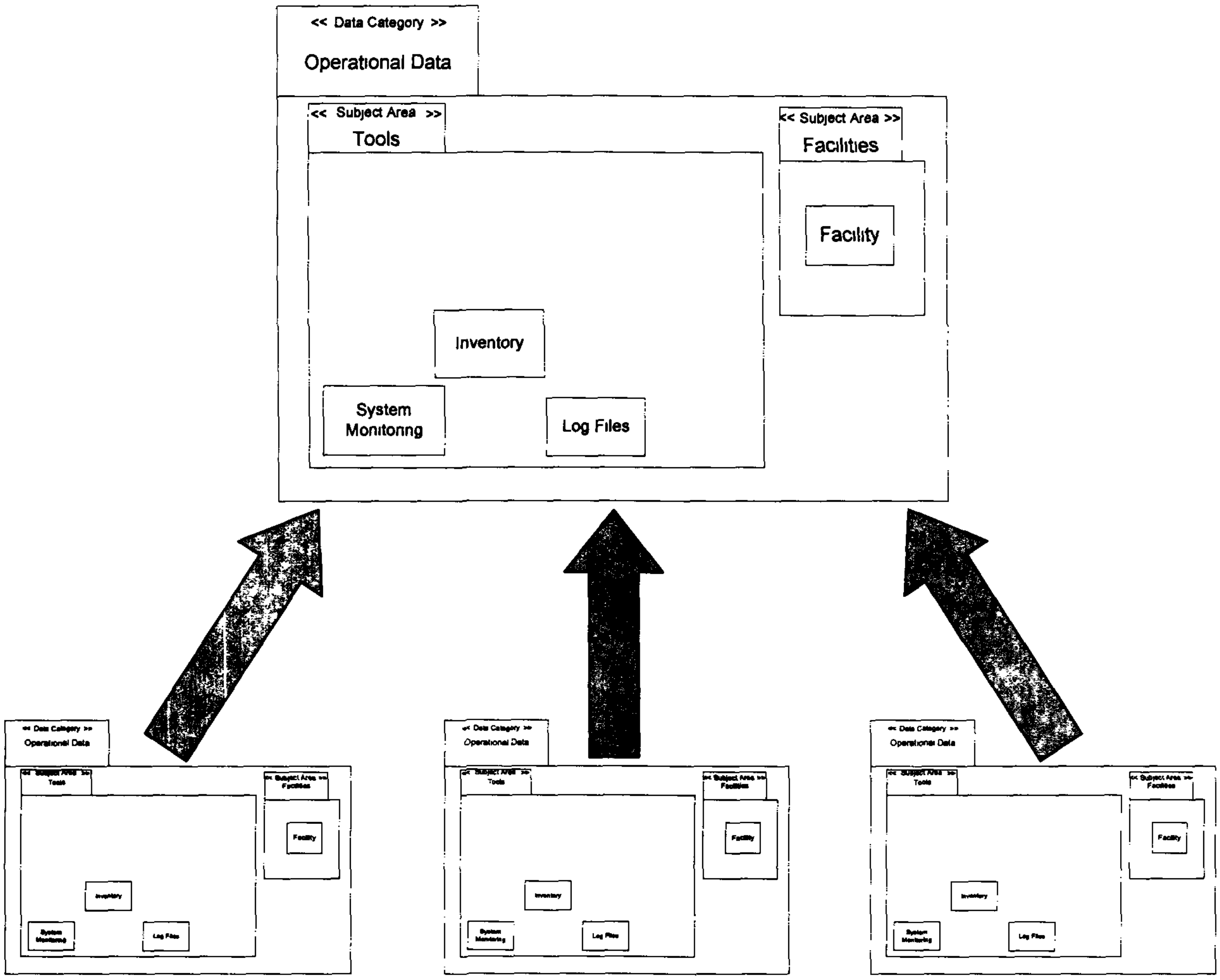
The authoritative source for Operating Systems, COTS, global configuration data, local configuration data, and developed code is at ERA Management. Operational data for system management is pushed from a master at the ERA Management system-level package to the Instances (see Figure 43).

Figure 43 – Replication of Centrally Generated Operational Data



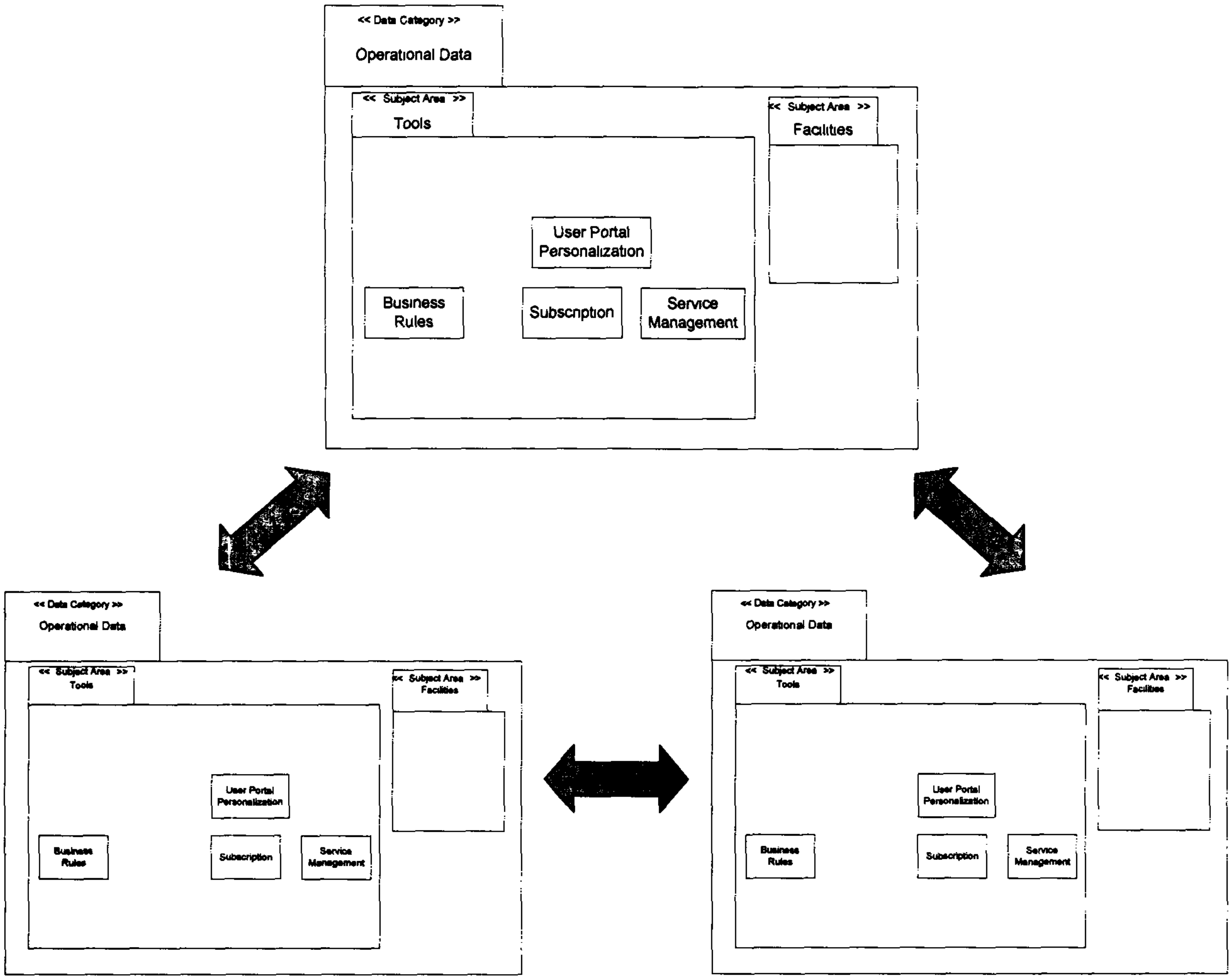
Operational data also include operations monitoring data and inventory data, which roll-up from the Instances to a master at the ERA Management system-level package (see Figure 44). The authoritative source is the LS&C system package at each Instance. System-level reports and detailed data are rolled-up from an Instance, and are available for alerting and for drill-down for problem diagnosis. Facility data are generated locally for each facility, and are rolled-up to ERA Management system-level package for centralized monitoring and management.

Figure 44 – Replication of Locally Generated, Centrally Used Operational Data



Operational data also include Business Rules, Portal personalization data, subscriptions, and service management. These data are generated locally at each Instance. They are replicated among all the distributed Instances at a given security classification level (see Figure 45) so that as a user is load-balanced among the different Instances for different sessions, his or her personalized data and interactions with the ERA System will remain the same.

Figure 45 – Replication of Locally Generated, Distributed Operational Data



3. RELATIONSHIP TO NARA ENTERPRISE ARCHITECTURE

As described previously in Section 2.3, the LM Team's approach is to develop a solution for the ERA System in the context of NARA's documented Enterprise Architecture (EA). NARA EA addresses NARA's information technology (IT) goals in support of NARA's strategic mission and agency-level strategic goals. The LM Team's approach to supporting NARA in achieving its mission and goals spans many domains, including initiatives beyond basic IT solution delivery such as, User Adoption and Human Factors Engineering. The ERA System architecture and design addresses the ERA System challenge with an enterprise architecture mindset. The LM Team has developed the ERA System's technical infrastructure within the context of NARA's Enterprise Architecture. At some point in the future, NARA may wish to leverage the ERA System's technical infrastructure to realize the NARA EA.

The NARA EA Overview identifies NARA's five Strategic IT initiatives:

1. Electronic Records Archives Initiative
2. Customer Service Initiative (a.k.a. GPEA[18])
3. Records Center Reimbursable Initiative (a.k.a. RCPOS[19])
4. Records Management Life Cycle Initiative
5. Support and Infrastructure Initiative

NARA's Strategic Information Resources Management (IRM) Plan provides further details on each initiative.

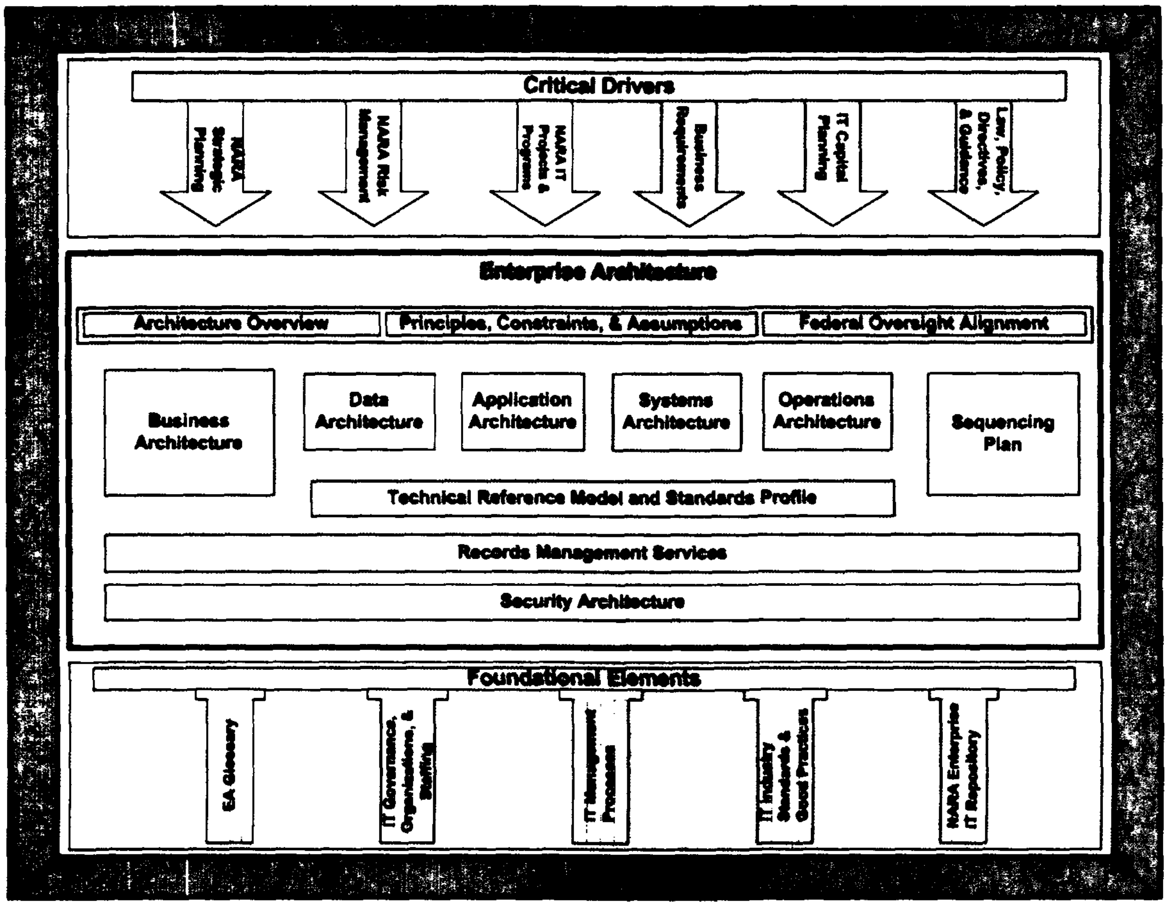
The deployed ERA System solution within the ERA initiative will be integral to fulfilling many of the EA objectives. The ERA System is just one of the multiple IT assets that will be deployed within NARA. The ERA System will enable a great deal of additional functionality that previously either has not existed, could not be integrated, or could not be achieved at such large scale; however, the ERA System is not intended to be a panacea for all the needs of the NARA enterprise. NARA will only be able to fully address its strategic goals via the implementation of the ERA System in concert with the efforts encompassed by the other four initiatives. The IT assets deployed across all of these initiatives will facilitate the overall transformation in parallel with NARA's business, organizational, and functional processes transformations outlined in the EA.

In the Business Architecture and the Application Architecture of NARA's EA, the ERA Initiative (along with the other initiatives) is mapped to constituent elements of the EA Framework. Figure 46 illustrates the NARA EA Framework. Some of these elements are mapped to multiple IT initiatives. These specific EA elements, along with the elements in the other primary EA framework components, can be further traced down to the ERA System modeling elements within the LM Team's ERA System solution as detailed in this SADD. These relationships provide visibility and traceability to how the ERA System solution fits within the context of NARA's EA. Table 55 provides references from each of the primary EA documents to the sections of the SADD that provide context reference.

[18] GPEA is referenced to the Customer Service Initiative in Footnote 8 of the EA Overview document, Sep. 13, 2004

[19] RCPOS is referenced as interchangeable with the Records Center Reimbursable Initiative in Footnote 8 of the EA Overview document, Sep. 13, 2004

Figure 46 – NARA Enterprise Architecture Framework



ERA_ENG_042a

Table 55 – EA Framework Descriptions and Documentation Mapping to SADD

Framework Element	Enterprise Architecture Components	SADD Section(s) for Context Reference
Architecture Overview	Enterprise Architecture Overview	Section 2.3.1
Principles, Constraints, and Assumptions (PCA)	Enterprise Architecture Overview	Section 2.5, Section 3
Business Architecture	NARA Business Architecture	Section 2.3.1, Section 2.4
Data Architecture	NARA Data Architecture	Section 2.11, Section 3.2
Application Architecture	NARA Application Architecture	Section 2.8, Section 3.3
Technical Reference Model (TRM)	NARA Technical Reference Model	Section 2.3.1, Section 3.7

Framework Element	Enterprise Architecture Components	SADD Section(s) for Context Reference
Technology Standards Profile	NARA Technical Standards Profile	Section 3.10
Systems Architecture	NARA Systems Architecture	Section 2, Section 3.4
Operations Architecture	NARA IT Operations Plan, NARA IT Operations Architecture	Section 2.4, Section 3.5
Sequencing Plan	NARA IT Sequencing Plan	Section 3.6
Records Management Services	NARA IT Records Management Services	Section 3.8
Security Architecture	NARA IT Security Architecture	Section 2.10, Section 3.9

The recent version of NARA's EA Overview states, "...many areas within the EA cannot be finalized until NARA's business needs are refined and business planning activities are complete." The demonstration of the LM Team's ERA System solution EA conformance addresses the available aspects in the EA's recent release, Version 3.2.

Throughout the EA, NARA has established corresponding but separate sets of Principles, Constraints, and Assumptions (PCA). Section 2.5 presents a PCA set that applies specifically to the LM Team's approach to the ERA System. The SADD PCA set is meant to stand alone, just as each of the EA PCA sets is intended to stand alone. Similarly, the SADD-presented PCA statements were developed in context with the EA-provided PCA sets.

However, several of the EA-Overview PCA elements directly relate to the LM Team's ERA System solution approach, as detailed in Table 56 below.

Table 56 – EA Overview Principles, Constraints & Assumptions (PCA) Mapping to ERA Solution

Selected NARA EA Overview PCA Elements	LM Team ERA Solution Context
Principle 2 – We will thoroughly understand, evaluate, and improve business processes before automating them.	The LM Team has based its solution on outputs from the ongoing NARA BPR efforts, NARA's ERA Concept of Operations document, the LM Team's Concept of Operations document developed with knowledge gained from direct interaction with NARA subject matter experts, and the LM Team's ongoing User Adoption efforts
Principle 4 – The IT infrastructure is a utility that must always be available, regardless of a customer's location.	The LM Team's SOA-based solution enables the delivery of the ERA System functionality utilizing the best available method among available service paths, within appropriate security constraints. Reliability, Availability and Maintainability analyses assure delivery and availability of the services within the proposed solution. The LM Team will utilize the LMTSS Human Factors and Usability Lab to excel in compliance with Section 508 and similar industry standards.

Selected NARA EA Overview PCA Elements	LM Team ERA Solution Context
Principle 5 – We will deploy IT capabilities in phases.	In addition to meeting NARA's specified delivery of services across multiple phased increments, the LM Team plans to continue prototyping new/updated services in the increments to reduce risk. Common infrastructure services are provided in the first increment to facilitate early service availability as well as system extensibility. The LM Team's architecture supports extending common infrastructure services across NARA's enterprise.
Principle 10 – We will acquire systems that are flexible and adaptable to change.	The SOA approach, high use of COTS HW/SW products, and conformance with industry-accepted standards assure solution flexibility, and adaptability, and simplifies evolvablity.
Constraint 4 – Our IT programs are constrained by on-going business operations and needs.	By integrating User Adoption into the LM Team's solution approach, the LM Team helps to mitigate the risk of loss of business service continuity
Assumption 1 – We will manage IT risk.	The LM Team's proposed ERA System solution demonstrates that NARA's goals are achievable with available and mature technologies, within a design that judiciously leverages COTS products. This evolution approach assumes a measured approach to the appropriate infusion of technology to avoid obsolescence and "vendor lock-in", and to assure continued successful operation.

Within the EA Overview, NARA provides a thorough mapping of its EA elements to the Federal Enterprise Architecture. Providing the context of the ERA System solution within NARA's EA facilitates NARA's demonstration of compliance with the requisite Federal statutes.

The following sections discuss the ERA System architecture and design within the context of each element of the NARA EA.

3.1 Business Architecture

The Business Architecture presented in NARA's EA defines the business needs, business organization and physicality, as well as the As-Is and potential To-Be business functions supported by the enterprise. From the standpoint of many of the referenced Framework Elements, the ERA System's role primarily will be one of facilitation and support of the business. By providing a solution that is flexible, scalable and extensible, the LM Team's ERA System solution will be able to adapt to meet the fluid needs of NARA's business processes, variety of locations, and organizational configurations.

The on-going BPR efforts capture and enhance understanding of NARA's business processes and functions. The BPR outputs also provide insight into what business needs can be satisfied by one or several of the planned IT initiatives, including ERA. Successful implementation of NARA's resulting Business Transformation Plan (BTP) will be facilitated through the combination of a planned User Adoption, optimized deployment of technology and resources to improve business performance, and technological evolution that is supported by logical business decisions, Within NARA's Business Context, the EA defines a set of core use cases that support the breadth of stakeholders in the execution of the Agency's business. Table 57 below provides a mapping between these use cases and the ERA System-level packages.

Table 57 – NARA EA Business Context Use Case Mapping to ERA Solution

EA Business Architecture Table 3-1 Business Context **Use Cases Name**	**ERA Initiative Involvement**	**ERA System-Level Packages**						
		Ingest	**Records Mgmt**	**Preservation**	**Archival Storage**	**Dissemination**	**LS&C**	**ERA Mgmt**
Maintain Documentary Material	Primary	X	X	X	X	X		
Support Records Management	Supporting		X					
Perform Archival Processing	Primary	X	X	X		X		
Determine Disposition	Primary		X					
Implement Disposition	Primary		X					
Provide Access to Archival Material	Primary					X		
Manage Party	Supporting					X		X
Manage Events	Supporting					X		
Manage Grants	N/A							
Manage Legal Publications	Supporting		X					
Manage Facilities	Supporting						X	X
Manage Tools	Supporting						X	X
Manage Finance and Accounts	Supporting						X	X

Table 57 above, maps the identified As-Is business functions to the ERA System-level packages. Table 58, demonstrates the relationships of the To-Be business functions. As the To-Be functionality continues to be developed and enhanced, the mapping of these relationships will be updated to assure the appropriate continuity of business needs coverage.

by ERA System functionality, as it is phased into operations. The mappings between the ERA System and the business functions in the Business Architecture provide a prospective To-Be view of the AA, as well as providing for the structural aspects of applications partitioning. The execution aspects of application partitioning are found in the Systems Architecture.

3.4 Systems Architecture

NARA's EA Systems Architecture (SA) provides several critical Framework elements of a successful EA. The present SA is self-described as a work in progress, which will provide significantly more details in future releases. The ERA System approach provided in this SADD replicates many of these elements, including the functional partitioning within the SOA, the utilization of an Enterprise Common Services approach, capacity and performance analyses to assure mission success, and finally, the definition of the Development and Test Environments necessary to support system creation, deployment, and ongoing support aspects.

3.5 Operations Architecture

NARA's EA Operations Architecture (OA) provides the recognition that an IT asset deployed within the enterprise (a system such as the ERA System) must not only achieve its required functionality, but must also continue to operate in a production environment.

The LM Team's approach to the ERA System recognizes and addresses these framework elements of the OA through the referenced sections in this SADD.

Table 59 – NARA EA Operations Architecture (OA) Elements Mapping to ERA Solution

Selected OA Framework Element	SADD Element
Disaster Recovery Planning	ERA Continuity of Operations Plan describes the LM Team's strategy, approach, plans, and processes for assuring operations support of ERA's core business services in the event of system(s) outages and disasters that affect the operating capabilities of ERA facilities or operating components.
Production Staging and Capacity Monitoring	Deployment and Transition Plan provides details of moving new system components from development/test into production. Section 2.4.4.2 describes the solution components that are used to evaluate and assess operations capacity and configurations prior to production acceptance and deployment.
Facilities Management	Deployment and Transition Plan describes the approach to support and manage the day-to-day operations of ERA System's hardware, networks, applications, and Help Desk within the ERA System infrastructure.
Systems Management	

NARA has also provided in the OA document a set of PCA statements that follow accepted best practices for providing modern data center operations support. The LM Team's ERA System operations approach fits well within the context of these statements. Of particular note are principles that address continuous operations support, centralization of support of deployment and management services, and optimized COTS vendor support; each of these principles is inherent in the ERA System solution.

The solution spans multiple operations architectural areas. The ERA System and Initiative cannot be successful if envisioned solely as an application within the Applications and Software Integration Area (Figure 10-1 of OA). The ERA System will provide communication channels between ERA Instances, necessary portal and Web services, Data Integration, Data Stores, and Integrated Security and Enterprise Systems Management. From the OA perspective, the ERA System could be a slice/layer of the enterprise.

3.6 Sequencing Plan

In conformance with enterprise architecture guidelines, NARA EA has a Sequencing Plan that allows the current state of the IT infrastructure to transition to the target state. In the case of the ERA Program, the technical activities within the program can be connected to the Sequencing Plan based on option years and increments. Based on the phased availability of services as manifested in the SyRS requirements baseline, the LM Team's phased solution over multiple increments and releases fits within the context of the Sequencing Plan provided in the EA current state and target state.

3.7 Technical Reference Model and Standards Profile

The NARA EA Technical Reference Model (TRM) provides a generic framework for addressing and conceptualizing the planned enterprise technologies. The TRM relies on the same basic principles and practices used by the LM Team in the approach to large-scale system integration (LSI) efforts such as the ERA System. The SOA-based solution supports multi-tiered solutions, with services partitioned to applications to provide loose coupling, increased modularity, and high reliability. Data integration in the ERA System solution is facilitated by a mediated data access service (mediation layer) in the context of the NARA preferred Mediated Virtual View.

The ERA Program has developed its own Technical Standards Profile that is reflected in Section 3.10 that reviews the current information within the NARA Technical Standards Profile. It then extends it to reflect the program necessities such as the transition to a SOA-based architecture, and the use of current hardware and software elements based on ERA technology evolution planning.

3.8 Records Management Services

The ERA System will be able to send data to and receive data from DoD 5015.2 compliant Records Management Systems, as well as other systems as dictated by NARA policy or other Federal mandates. As such, the ERA System will be developed in the context of the Records Management Services component of the NARA EA.

3.9 Security Architecture

The LM Team addresses security for the ERA System at all levels based upon the LM Team's experience working with the breadth of security classifications and protection methodologies reference by the Security Architecture (SecA) component of NARA's EA. Security architecture and design elements are address in the SADD in Sections 2.10 and 3.9, as well as in separate CDRLs as listed in Table 60 below.

Table 60 – NARA EA Security Architecture Elements Mapping to ERA Solution

Selected SecA Framework Element	SADD/ERA Program Supporting Elements
IT Security Program Elements	
IT Security Program Plan	Security Plan - The Security Plan provides an overview of the ERA System security requirements and describes the existing or planned controls needed to meet those requirements.
IT Security Policies	Security Plan
Compliance, Auditing, and Reporting Services	Certification and Accreditation (C&A) Plan
Security Monitoring & Remediation Services	Certification and Accreditation (C&A) Plan
Risk Management Services	Security Risk Assessment Report - Characterizes the release, and lists the potential threat-sources and associated threat actions applicable to the release.
Certification & Accreditation Services	Certification and Accreditation (C&A) Plan - The C&A plan is the roadmap or the "how" the C&A activities will be accomplished to satisfy the requirements and each of the steps set forth in the System Security Authorization Agreement (SSAA) required by DITSCAP. This plan also establishes the "who, what and when" of the certification activities.
IT System Security Planning Services	Security Plan and Certification and Accreditation (C&A) Plan
Security Awareness & Training Services	Technical Manuals - Describes the security mechanisms installed on the system, and how to use them, from a user's perspective.
IT System Continuity Planning Services	Continuity of Operations Plan - Identifies potential impacts that threaten the ERA System and provides a framework for building resilient and effective responses that safeguard the interests of its stakeholders.
IT Security Architecture Elements	
IT Security Risk Profile	Security Risk Assessment Report - Characterizes the release, and lists the potential threat-sources and associated threat actions applicable to the release.
IT Security Requirements	SADD Section 2.10.1

Selected SecA Framework Element	SADD/ERA Program Supporting Elements
IT Security Management Mechanisms and Specifications	Security Plan and SADD Section 3.9
IT Security Operational Mechanisms and Specifications	Security Plan, & and SADD Section 2.10.
IT Security Technology Mechanisms and Specifications	Security Plan

By infusing security throughout the architecture, design, and operations components, the ERA System architecture and design fully addresses the issues presented in NARA's EA SecA.

3.10 ERA Technology Standards Profile

The ERA Technology Standards Profile has been created based on a target NARA Enterprise Architecture. The standards profile is segmented based on an ERA Technology Classification Model created specifically to address the use of ERA's service-oriented architecture paradigm. The standards profile uses the technology structure provided by the classification model and offers technical standards that apply to each of the different components. The technology standards profile lists the following elements in a tabular format:

- **Technology Component** – lists the main heading and subheading of the items based on the above technology classification model.
- **Technical Standard** – lists the abbreviated standard.
- **Description** - provides a summarized description of the technical standard and its relevance to the technology component.
- **Recommended Products** – lists any recommended product by a vendor for the ERA System that abides by the technical standard.

Table 61 - ERA Technology Standards Profile

ERA Technology Standards Profile			
[illegible]	[illegible]		
[illegible]			
Web Browser	HTML	HTML, the HyperText Markup Language is a standard for defining document type within the Web.	Internet Explorer, Netscape

ERA Technology Standards Profile			
Communication Channels			
Transfer Protocol	HTTP	Web-based HyperText Transfer Protocol based messages for transfer of text graphics and images.	SUN Web Server
Mail Protocol	SMTP	Simple Mail Transfer Protocol (SMTP) for electronic mail transfer.	
Internet Protocol	TCP/IP	Transmission Control Protocol/Internet Protocol to conduct Internet-based communication.	
LAN/MAN Protocols	Ethernet; Gigabit Ethernet	IEEE 802.3 Ethernet standards and Gigabit Ethernet is defined by the IEEE 802.3z and 802.3ab standards.	
LAN/MAN Devices	10/100/1000 Base-T	Follows Ethernet and Gigabit Ethernet switch technology for all devices	Cisco Ethernet Switches
WAN Protocols	Frame Relay; SONET	Frame-relay service from external third-party carriers. SONET is a transport protocol for Fiber for offering OC-3 and OC-48 carrier lines.	
Portal Services			
Application Server	J2EE Server	JAVA 2 Enterprise Edition (J2EE) is an enterprise-level development environment for creating and deploying JAVA programming language and associated technologies.	BEA application server, SUN JES server
Portlet Specification	JSR-168	JAVA Specification Request (JSR) 168 establishes a standard API for creating portlets and enables interoperability between portlets and portals.	BEA WebLogic portal application
Message Format Specification	XML	XML is the current standard for message format and transmittal specification.	XML editors supporting BEA WebLogic platform
Text Message Format	RFC 822	RFC 822; Standard for the format of Internet text messages provides the text message format.	

ERA Technology Standards Profile			
Message Invocation Specification	SOAP	Simple Object Access Protocol (SOAP) used as an underlying protocol to send messages from one Application or Service to another within a Services Oriented Architecture.	SUN JES platform enabled for use of SOAP
Service Description Specification	WSDL	Web Service Description Language (WSDL) is an XML-based language for codifying services within a Services Oriented Architecture and offer web services for business functions.	BEA WebLogic platform enabled for use of WSDL
Locator Service Specification	UDDI	Universal Description, Discovery and Integration (UDDI) is an XML-based registry that allows web services to be listed and seen by external business entities. Use of UDDI has to be implemented at a high-level so multiple systems can access a common registry.	Bea WebLogic platform
Remote Portal	WSRP	Web Service for Remote Portals (WSRP) is a service specification published in UDDIs that allows remote portals and intermediary applications to integrate content and applications.	BEA portal server
[illegible]			
Business process and workflow specification	BPEL	Business Process Execution Language (BPEL) is an XML-based language that is currently emerging to enable sharing amongst multiple organizations.The BPEL 2.0 standard will be adopted when it is ratified.	BEA WLI
Interactive Web Application	WSIA	Web Services Language for Interactive Applications (WSIA) is to create an XML and web services centric framework for interactive web applications.	BEA application server
Style Sheet Integration	XSL	Extensible Style sheet Language (XSL) family allows XML transformation and presentation and acts as an integration adapter for web services.	BEA WebLogic Integration
Access Control	XACML	Use of eXtensible Access Control Markup Language (XACML) for implementing access control.	

ERA Technology Standards Profile			
XML Query	XQuery	W3C XML Query provides flexible query facilities to extract data from real and virtual documents and collections both locally and on the Web.	
[illegible]			
Integration Brokers	JAVA RMI	Java Remote Method Invocation (RMI) system allows an object running in one Java Virtual Machine (VM) to invoke methods on an object running in another Java VM, and provides remote communications between programs.	BEA WebLogic platform
Business Rules Engines	JSR-94	JAVA Rules Engine API (JSR 94) defines a Java runtime API for rule engines by providing a simple API to access a rule engine from a Java Platform.	Fair Isaac Blaze Advisor
Message Oriented Middleware	JMS	The Java Message Service (JMS) API is a messaging standard that allows application components based on the Java 2 Platform, Enterprise Edition (J2EE) to create, send, receive, and read messages.	Bea WebLogic platform
File Transfer & Transport	SecureFTP	SecureFTP is a file transfer client with great flexibility in configuration and transfer protocols. SecureFTP supports the secure SSH-1, SSH-2, and SSL/TLS protocols.	SUN Solaris
Database Connector	JDBC	Java DataBase Connectivity (JDBC) technology is an API (included in both J2SE and J2EE releases) that provides cross-DBMS connectivity to a wide range of SQL databases and access to other tabular data sources.	Bea WebLogic platform
[illegible]			
Data Access	JDO	Java Data Objects (JDO) API is a standard interface-based Java model abstraction of persistence, developed as Java Specification Request 12 JSR 12.	BEA WLI
XML Query Access	XQJ	XQuery API for Java (XQJ) is a standard API that implements XQuery for Java and coordinates with JDBC.	BEA WLI

ERA Technology Standards Profile

[illegible]			
Username/Password	NARA 804-02	Username and password is per the specification written within NARA IT Security Handbook – Technical Controls NARA 804-02.	
Digital Certificate Authority	X.509 PKI	X.509 is an ITU-T standard for public key infrastructure (PKI). Digital Certificate Authorities are X.509-based that is offered by government agencies or commercial third-party providers.	
Authentication Servers	IEEE 802.1-based	Authentication servers control authentication for enterprises via a centralized repository authentication information. IEEE 802.1-based authentication is used for Ethernet.	SUN JES Directory Server
[illegible]			
Access Control Lists	Windows-based ACLs, Solaris-based ACLs	The access control list (ACL) is a concept in computer security used to enforce privilege separation.	SUN JES Directory, BEA platform
Role & Policy Managers	NARA ERA-based	Role and policy management is a working-level activity within NARA and ERA to set the proper guidance.	SUN JEA Access Manager
Perimeter Protection Technology	Firewalls; IDS; Proxy Servers	Intrusion detection systems, firewalls, proxy servers and protection technologies are used to address this function.	CISCO firewall blades, IDS blades
Network Virus Scans	CERT	Computer Emergency Response Team (CERT) issues alerts and incident handling and avoidance guidelines.	F-PROT
Desktop Virus Protection	CERT	SUN and Windows-based desktop virus protection based on vulnerability alerts.	F-PROT
Directory Services	LDAP	Lightweight Directory Access Protocol (LDAP) is a "lightweight" version of a Directory Access Protocol (DAP) X.500 standard for directory services within a network.	SUN JES Directory Services
[illegible]			

ERA Technology Standards Profile

[illegible]	[illegible]	[illegible]	[illegible]
Secret Key Encryption	FIPS 197	FIPS 197 provides the Advanced Encryption Standard (AES) scheme for providing security encryption for ERA.	
Session Encryption	SSL	Secure Sockets Layer (SSL)-based session encryption is the current widely used standard.	CISCO SSL Accelerator cards
Secure Media Deletion	DoD 5220.22	This is the DoD NISPOM standard for media deletion that involves expunging data.	Data General Degausser
IPSec (Internet Protocol Security)	IPSec standards	A full set of IP Security standards that are present and are upcoming for use within the ERA System.	
Checksum & Hash Algorithm	SHA 256; SHA 512	Checksum is a count of bits in a transmission unit that enables the receiver to verify if the number of bits received matches the number sent. Secure Hash Standard (SHA) - 512 and SHA 256 will be used.	DECRU security module
[illegible]			
Intrusion Detection Systems		An Intrusion Detection System (or IDS) generally detects unwanted manipulations to systems.	CISCO IDS blades
Vulnerability Assessment Tools	CVE	Common Vulnerability and Exposures (CVE) - is a list of standardized names for vulnerabilities and other information security exposures.	WebInspect AMP, Internet Security Systems
Event Correlation	CoBIT	CoBIT is an IT governance framework and supporting toolset. For ERA we need to perform event correlation from the logs and alerts of multiple security technologies.	Intellitactics
[illegible]			
Backup/Restore	Standard Partition level Image	A Standard Partition Level Image is typically stored on tape, may contain multiple partitions and includes some overhead information in addition to the data being backed up.	Veritas NetBackup

ERA Technology Standards Profile

[redacted]	[redacted]	[redacted]	[redacted]
Remote Copy	PPRC	Peer to Peer Remote Copy or PPRC is the protocol to mirror a DASD volume in one Control Unit (the primary) to a DASD volume in the other Control Unit (the secondary).	
Processor Clustering Technology	RAC	Oracle Real Application Cluster (RAC) is a cluster database that works in Solaris environment with a shared cache architecture that overcomes the limitations of traditional shared-nothing and shared-disk approaches.	Oracle RAC
[redacted]	[redacted]	[redacted]	[redacted]
System Management tools		System management tools allow the ERA enterprise to monitor the runtime condition of computer hardware platforms, operating systems, and monitor capacity.	
Archival Standard	OAIS	Use of standard reference model for an Open Archival Information System (OAIS) provides archiving model for records preservation.	
Records Management Specification	DoD 5015.2	DoD 5015.2-STD, "Design Criteria Standard for Electronic Records Management Software Applications," provides implementing and procedural guidance on the management of records in the Department of Defense.	
Enterprise Modeling	Zachman Enterprise Framework	Zachman Enterprise Architecture framework follows the NARA Enterprise Architecture and Levels 1 to 5 provide a model for system architecture.	
System Modeling	UML	Unified Modeling Language (UML) is the industry-standard language for specifying, visualizing, constructing, and documenting the artifacts of software systems.	
Language Compilers	JAVA	JAVA Language Specification for Solaris and JAVA Community Process (JCP) provides the current J2EE programming environment.	SUN JES for Solaris
Scripting Language	JSP	Java Server Pages (JSP) is a Java technology that allows software developers to dynamically generate HTML, XML or other types of documents in response to a Web client	

ERA Technology Standards Profile

		request.	
Interactive Scripting	AJAX	Asynchronous JavaScript And XML, or its acronym, AJAX, is a Web development technique for creating interactive web applications.	
Configuration Management & Version Control	ANSI-EIA-649-1998	ANSI/EIA-649-1998 National Consensus Standard for CM and MIL Handbook-61 provides the latest CM guidelines to be followed for the government enterprise.	
Requirements Management	IEEE/ANSI 830-1993	ANSI 830-1993 covers the recommended practice for software requirements specifications.	
Testing Software	ANSI 1008-1987; ANSI 829-1983; ANSI 1012-1986	ANSI has several standards related to software testing: 1008 deals with unit testing, 829 deals with verification and validation and 1012 is the standard for software verification and validation plans.	Mercury QuickTest Pro
[illegible]	[illegible]	[illegible]	[illegible]
[illegible]			
Workstation	Windows XP	Operating system for desktop workstations.	Dell Precision 670; Precision 380
Midrange Servers	Solaris; Windows Server 2003; Linux ES4	Operating system for ERA mid-range servers.	SUN Fire T2000; PowerEdge 850
High-End Servers	Solaris	Operating system for high-end servers.	SUN Fire V890
Workstation DBMS	SQL 1999; SQL/CLI 1995	Desktop level standard for database operations.	MS-Access
High-End Server DBMS	SQL 1999; SQL 2003; SQL/CLI 1995	Enterprise level standard for database operations.	Oracle 10G
[illegible]			
Workstation - Solaris	Ultra SPARC, AMD x86	Use of SUN Fire workstations.	SUN Fire Blade 150

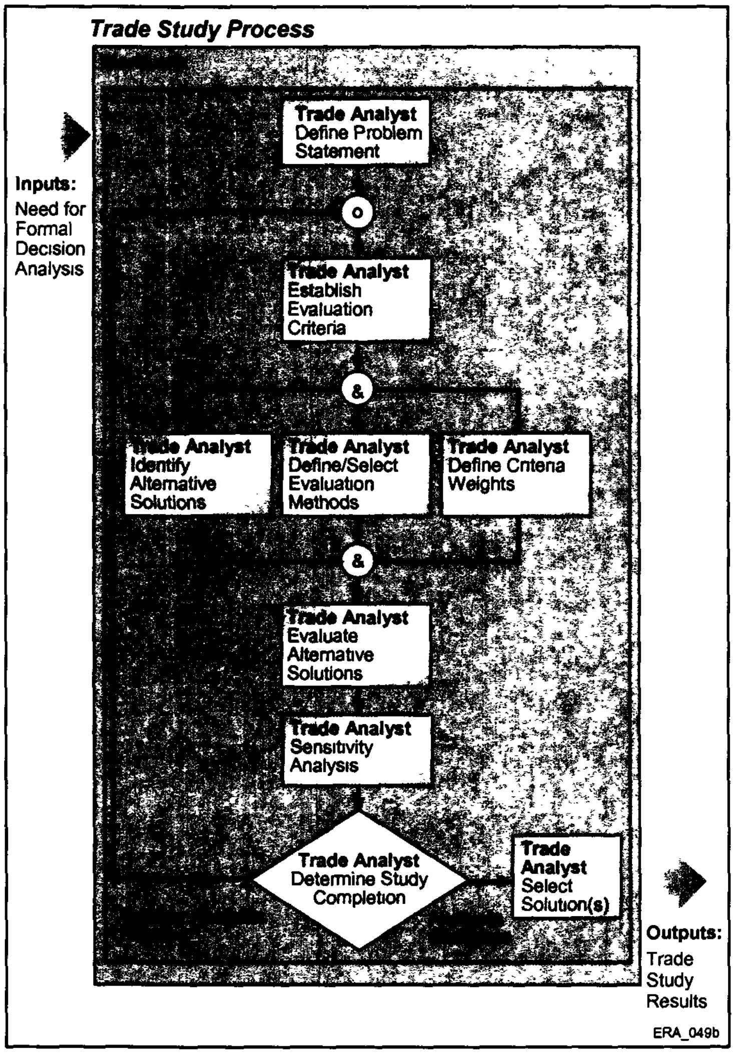
ERA Technology Standards Profile

[illegible]	[illegible]	[illegible]	[illegible]
Workstation - Windows	Pentium-based, AMD x86	Use of the latest Pentium or x86-based standard for use for new purchases.	Dell Precision 670; Precision 380
Mid-range Server - Windows	Pentium-based, AMD x86		Dell PowerEdge 850
Mid-range Server - Linux	Pentium-based, AMD x86	Use of latest Pentium or x86-based server.	SUN X2100 server SUN X4200 server
Mid-range Server - Solaris	Ultra SPARC	Use of SUN Fire T2000 server using the UltraSPARC T1 processor.	SUN T2000 server
Server Input/Output	PCI(e)	PCI Express, or PCI-E, is an implementation of the PCI computer bus, but bases it on a completely different and much faster serial physical-layer communications protocol.	Qlogic Sun PCI(e) cards
Cable Plant	100 TIA/EIA 568	100 TIA/EIA 568 is a standard for providing RJ-45 connectors to CAT5 cables.	
Fiber-optic cabling	100Base-FX	100Base-FX over Fiber provides the standard for fiber cables necessary for network carriers and third-party subscriber lines.	Cisco 100 FX over fiber
Storage Systems			
Storage Subsystems (SAN-based)	Fibre Channel	Fibre Channel ANSI X3.230-1994 is a technology standard for transferring data between computer devices.	Brocade 4100 SAN Fabric switch
Storage Subsystem (NAS-based)	Gigabit Ethernet	NAS is a way of attaching storage to standard networks, and a NAS appliance is a file server that runs on Gigabit Ethernet and uses a file-sharing protocol to let clients access the storage.	Net App NAS device
Redundant Disk	RAID-5, RAID DP	Redundant Array of Independent Disk (RAID) Level 5 has a rotating parity array that allows all read/write activities to overlap; RAID Double Parity allows further protection for use in ERA.	Net App disk cache

Criterion	Description
Risk Mitigation	The LM Team may recommend a COTS product that does not meet all of the criteria if the alternative is costly or requires time-consuming development.
Cost	Applies the engineering knowledge base from the life cycle cost model to the established cost objective to manage risk and reduce ownership costs.

These criteria provide the basis for the evaluation and are ranked so that the highest ranked criteria exert the most influence on the evaluation. Actual COTS and NDI recommendations are the result of formal trade study processes in LM's Process Asset Library. Figure 47 illustrates the trade study process.

Figure 47 - Trade Study Process



Define Problem – The Trade Analyst defines and documents the purpose, objective(s), constraints, and requirements of the trade study, including definition of the need, the user, and the availability of resources bounding the scope of the analysis. Without a clear statement, studies become costly and produce unclear results.

Establish Evaluation Criteria – The Trade Analyst establishes, documents, and maintains the criteria for evaluating alternatives, and the relative ranking of these criteria.

Identify Alternative Solutions – The Trade Analyst identifies and documents alternative solutions to the problem.

Define/Select Evaluation Methods – The Trade Analyst selects, defines, and documents the methods for evaluating the alternative solutions against the established criteria. The Trade Analyst also ensures that the selected evaluation methods are commensurate with the resources bounding the scope of the analysis.

Define Criteria Weights – The Trade Analyst defines and documents weighting factors for the evaluation criteria established in R-2.

Evaluate Alternative Solutions – The Trade Analyst evaluates alternative solutions using the established criteria and weighting, and documents these evaluations.

Sensitivity Analysis – The Trade Analyst determines the sensitivity of the solution ratings to small changes in input values.

Determine Study Completion – The Trade Analyst determines study completion by ascertaining whether the analysis is complete and sufficient to permit solution selection or whether further analysis is needed.

Select Solution(s) – The Trade Analyst selects a solution(s) from the alternatives based on the evaluation criteria, and documents the rationale for this selection.

This page is intentionally left blank.

APPENDIX A. GLOSSARY OF TERMS

[illegible]	[illegible]
Access	To make available (in accordance with all applicable access restrictions) records, copies of records or information about records through activities such as reference services, providing reproductions, and producing exhibitions and public programs.
Access Privilege	An identified authorization associated with a user that grants that user the right to access records that have the corresponding access restriction. Some access privileges, such as a security clearance, are hierarchical and grant the user access
Access Restriction	An identified restriction that controls how access can be provided to assets, and how assets can be stored. Restrictions may apply to all or part of the asset, and may be based on national security considerations, donor restrictions, court orders, Freedom of Information Act (FOIA) exemptions, or other statutory or regulatory provisions.
Access Review	The process of reviewing records to determine what records or parts of records must be withheld from a requestor because of access restrictions, and the process of implementing those decisions to release, redact, withdraw, or withhold materials. This includes systematic review, mandatory review, FOIA review, special access review, and review of records of concern.
Access Review Case	A collection of documents (a file) relating to a specific action, event, person, place, project or other subject, utilized in an access review
Accession (n)	As a noun, the body of records for which legal custody is transferred by one act of accessioning.
Accession (v)	As a verb, the processes supporting the transfer of legal custody of records to NARA from the creator (or the creator's legal representative, successor, or heir), including the generation, execution, and processing of deeds of gift, the standard forms, or other appropriate legal documents.
Accession Group	A body of documentary materials for which transfer of legal custody is authorized by the same legal transfer instrument. Also referred to as "an accession".
Ad Hoc NARA-Prepared Disposition Agreement	A generic NARA-prepared disposition agreement, which can be used to establish intellectual control of documentary materials, which are not Presidential records or potential donations.
Ad Hoc Report	A report with variable content generated by the system to satisfy a temporary need.
Adaptive Simulated Training	Computer based training which simulates user interaction with system functionality without instructor interaction or actual system functionality/connectivity. This method of training could be used for general user training, as well as for administrator training.
Aggregate	An intellectual aggregation of documentary material arising because they result from the same accumulation or filing process, the same function, or the same activity; have a particular form; or because of some other relationship arising out of their creation, receipt, or use; or because the aggregate was required for the purposes of archival arrangement.

Allocation	(1) The process of distributing requirements, resources, or other entities among the components of a system or program. (2) The result of the distribution in (1).
Amended Information	Privacy Act amendment information is the data provided by the requestor that describes the amendment, such as the date of request, requestor identification and the requested amendment itself.
Appraisal	The process of determining the value and thus the disposition of records (i.e., designating them temporary or permanent) based upon their current administrative, legal, and fiscal use; their evidential and informational value; their arrangement and condition; their intrinsic value; and their relationship to other records. (Society of American Archivists Glossary)
Appraisal Report	An analytical report that describes the records submitted on a schedule and their informational or evidential value, the organizational context within which they are generated, and whether the agency-proposed disposition instructions are appropriate.
Architectural Design	(1) The process of defining a collection of hardware and software components and their interfaces to establish the framework for the development of a computer system. (2) The result of the process in (1).
Archival Control Group	An intellectual grouping of documentary materials used to facilitate administrative control.
Archival Creator	The organization or person responsible for the creation, accumulation, or maintenance of a series of documentary material when in working (primary) use.
Archival Description	A kind of description that adheres to NARA standards for content and structure.
Archival Metadata Templates	Templates used to describe records in the Archive
Archival Processing	The activities of accessioning, arranging, describing, conducting access review, and properly storing records.
Archivally-Imposed Arrangement	An arrangement imposed on an aggregate in compliance with archival principles, for example to return the aggregate to its original order.
Archive object	Collection of assets in a self-describing modified ISO 9660 format.
Arrangement	The results of the intellectual and physical processes organizing records in accordance with the Archival Creator's business needs, accepted records management practices, or archival principals.
Arranging, (to arrange)	The intellectual and physical processes (and the results) of organizing records (documentary materials) in accordance with accepted archival principles (particularly provenance and original order. See also Hierarchical Description).(changes in parenthesis from Domain Model Draft)
Artifact	A three-dimensional object made, modified, or used by humans.
Asset Type	The archival, business, or system category to which an asset belongs, such as record, series, disposition agreement, business rule, event log, etc.
Assets (ERA-LM)	In the context of ERA, assets include the electronic records, descriptions, template data, records lifecycle data, and data which is a by-product of the production system.
Assets (ERA-PMO)	The complete set of information available within ERA.

Association class	Component of NARA Conceptual Data Model; describes the interaction between (or among) two or more object classes.
Attribute	Component of NARA Conceptual Data Model; Identifies the properties of object classes and association classes that have specific meaning with respect to the NARA CDM.
Attribute of Records	A data item containing a single piece of information about a record.
Audit	An independent examination of a work product or set of work products to assess compliance with specifications, standards, contractual agreements, or other criteria.
Audit Trail	Information stored in the system log that provides the capability to discover an action or series of actions taken by the system, including actions initiated by either the system or by an individual interacting with the system.
Authentic Copy	A copy of a record for which the official custodian attests to the authenticity.
Authentic record	A record that is what it purports to be and is free from tampering or corruption
Authentically Preserve	To maintain a record over time in such a manner that its identity is unquestionable and it is not corrupted.
Authenticity	(1) The property of a record that it is what it purports to be and has not been corrupted. (2) An authentic record is one that is proven to be what it purports to be and to have been created or sent by the person who purports to have created and sent it.
Authority Source	A list, file, pick list, or thesaurus containing standardized information (e.g., acronyms, abbreviations, names, and phrases) that is used to ensure that a person, place, thing, event, or concept is consistently referred to using the same terminology. Authority Sources provide a uniform method of creating consistent indexes or access points to records (documentary materials) and information about records (documentary materials).
Availability	The ratio of time that a system is available to the total time of system operation. As availability is a statistical calculation, mean times are used.
Backup	An alternate copy of a deployed asset. Assets (here) include deployed software (OS, COTS, developed code, and configuration files), data, and files. The alternative copy may be an original, or may be a copy made from the deployed asset.
Behavior (Digital Item)	(1) The variability in the manifestation of the content of a digital item. (2) The aggregate of the expressions of variability available in a digital item.
Bit Stream	A fixed octet-serialized encoding of an information model, independent of the physical medium underlying its manifestation.
Bit Sequence	A sequence of the integers 0 and 1, which is the binary, representation of intellectual content such as numbers or characters, or of specified digital encodings.
Canonical protocols	A standardized message format for exchanging information between two systems or sub-systems. In Service Oriented Architectures built on Web services, the canonical protocol is typically expressed in the Web Services Description Language (WSDL) XML standard.
Cardinalities	Component of NARA Conceptual Data Model; specify how many times an object class participates in a given association class.

Catastrophic Loss	A complete loss of a data center, a library, a significant amount of data in the data center, a single media, or a single electronic record.
Certificate Authority [CA]	As part of a public key infrastructure, an authority in a network that issues and manages security credentials and public keys for message encryption and decryption.
Certified Copy	A copy of a record signed and certified as an authentic copy by the official custodian of the original.
Check Pointing	Periodic recording of the state of the system, usually for purposes of being able to roll the system back to the state it was in prior to a problem.
Code	(1) In software engineering, computer instructions and data definitions expressed in a programming language or in a form output by an assembler, compiler, or other translator. (2) To express a computer program in a programming language. (3) A character or bit pattern that is assigned a particular meaning; for example, a status code.
Coding	(1) In software engineering, the process of expressing a computer program in a programming language. (2) The transforming of logic and data from design specifications (design descriptions) into a programming language.
Collaboration Object	An asset about which collaboration is being performed. Types of assets include, but are not limited to: templates, disposition agreements, transfer agreements, archival descriptions, and records. Business functions that collaborate on these objects include, but are not limited to: scheduling, transfer, description, access review, redaction, and user assistance. An asset on which collaboration is performed will have the same structure as any other asset of the same kind; in other words, the collaboration process does not alter the asset's structure.
Collection	A type of archival control group consisting of: (1) An artificial accumulation of documents brought together on the basis of some characteristic (such as means of acquisition, creator, subject, language, media, form, name of collector) without regard to the provenance of the documents. (2) The whole of the documents, regardless of form or media, organically created and/or accumulated and used by a particular person, family, or organization in the conduct of personal or organizational activity.
Complex Digital Item	A Complex Digital Item is a bitsequence with a defined representation and identification that includes its own content and other Digital Items. A word processing format that allows for embedded macros is an example of a complex digital item.
Composite Application	Composite application provides the end users with a complete set of business functions to perform business tasks such as managing a Disposition Agreement, processing a FOIA request, or submitting and statusing an order. A composite application allows for having several interactions between the application and the end user. It may interact with the Core Services and Business Application Services directly, or, for more complex applications, may interact through the Business Process Management service to orchestrate and mediate Service invocations.

[illegible]	[illegible]
Concept Based Searching	Concept search techniques automatically identify the most significant patterns (typically proper nouns, noun phrases and verb phrases, including stemming and thesaurus) in any text and use these compound terms to rank results based on an understanding of meaning rather than simply based on finding the required words. Concept search techniques use correlation filters such as Bayesian, Shannon, genetic algorithms, and other mathematical techniques.
Configuration Control	In configuration management, an element of configuration management consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification.
Configuration Identification	In configuration management: (1) An element of configuration management consisting of selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation. (2) The current approved technical documentation for a configuration item as set forth in specifications, drawings, associated lists, and documents referenced therein.
Configuration Management (CM)	In system/software engineering, a discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements.
Congressional Deposit Agreement	A deposit agreement between NARA and the U.S. Congress. (See also Deposit Agreement.)
Constant Unique Identifier	A unique, innate identifier for a digital item and elements of information within the system. These identifiers will be used both to identify entities and to bind entities to each other.
Content	The information that a document is meant to convey (Society of American Archivists Glossary). Words, phrases, numbers, or symbols comprising the actual text of the record that were produced by the record creator.
Content of a Record	The information conveyed by the record.
Context of a Record	The organizational, functional, and operational circumstances in which a record is created and/or received and used.
Control (Data)	To regulate. To control data means to regulate it in a manner that protects it against corruption or unauthorized access.
Controlled List Search	A search in which the user input is constrained to be a value contained in an authority source.
Copy	A duplicate or reproduction of a document.
Coupling	A measure of the extent to which interdependencies exist between system elements.
Creator	The organization or person responsible for the creation, accumulation, or maintenance of a series of records when in working (primary) use.
Current Owner	Current owner is the current owner of the legal right to the records.
Custody	Guardianship, or control, of records, including both physical possession (physical custody) and legal responsibility (legal custody), unless one or the other is specified.

Data	(1) In system/software engineering, a representation of facts, concepts, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automatic means. (2) Facts, ideas, or discrete pieces of information, especially when in the form in which it was originally collected and is unanalyzed.
Data Category	The highest level of conceptual representation of data within NARA from the business viewpoint. Each data category can be decomposed into multiple subject areas.
Data Content	Those parts of the bitsequence of a digital item on which behaviors act and which are not technical artifacts specific to the software and hardware environment in which the digital item was created. The data content will be invariable throughout the expression of any perceptual or functional behaviors. Logical behaviors may modify the data content of a digital item.
Data File	(1) A collection of data that is stored together and treated as a unit by a computer. (2) Related data (numeric, textual, or graphic information) and fields that are organized in a strictly prescribed form and format.
Data Structure (Digital Item)	The defined representation of the bitsequence of a specific data type. The data structure defines how each part of the bitsequence of the digital item is to be interpreted or processed by the software that uses it.
Data Type	The representation of information according to preset specifications (e.g., plain text files, fixed length text files, HTML, TIFF, etc.).
Data Type Descriptor	A registry entry that describes a data type, including identifying attributes, representation information, encodings, and software needed to parse/render the data type.
Deed Of Gift	A type of legal transfer instrument in which documentary material is donated (and legal custody transferred) to the National Archives by an individual, family, or organization.
Default Disposition Agreement	A NARA-initiated disposition agreement which contains only the mandatory information required for management purposes to be used when no other type of disposition agreement is applicable.
Default Records Schedule	A type of disposition agreement used for Federal records which have not yet received an approved specific records schedule.
Default Search	A standard search that has preselected criteria and values available to all ERA users.
Default Template	A template that specifies the minimal elements necessary for a document.
Demilitarized Zone (DMZ)	A neutral zone that also prevents outside access to the internal system data.
Deposit Agreement	A type of disposition agreement in which NARA agrees to accept physical custody of documentary materials without taking legal custody of them.
Deprecated Object	An object that has been outdated by newer constructs. Deprecated objects are maintained, but are clearly marked as deprecated. Deprecated objects may become obsolete in the future.
Description	(1) The process of analyzing, organizing, and recording information that serves to identify, manage, locate, and explain documentary material, and the contexts and record systems from which the material was selected. (2) The written representation or products of the above process.

Design	(1) The process of defining the architecture, components, interfaces, and other characteristics of a system or component. (2) The result of the above process.
Destruction	The process of eliminating or deleting records beyond any possible reconstruction.
Destruction Disposition Instruction	A type of disposition instruction that mandates the destruction of documentary materials.
Detected Effects	"Detected effects" will be discovered through comparing the results of the digital adaptation processor to a normative copy.
Digest	The computed result of applying a specialized algorithm to a sequence of bits that always creates another sequence of bits of pre-determined length that has an extremely high probability of being unique.
Digital Adaptation	The transformation or migration of an object from a source data type to a different target data type. See also "Digital Adaptation Processor".
Digital Adaptation Descriptor	A registry entry that describes a digital adaptation processor, including identifying attributes, version and other configuration information, and documented capabilities
Digital Adaptation Engine	See Digital Adaptation Processor
Digital Adaptation Processor	A processing capability that transforms a source data type to a different target data type. A generic data adaptation processor may use a template that provides the processing instructions specific to a target data type.
Digital Component	A bit stream which is necessary to reproduce documentary material and requires specific identification because it is stored separately or in a specific data type, or has a specific behavior or association with specific software.
Digital Container	A Digital Container is a bitsequence that includes one or more digital Items or complex digital items in an internal structure, which may be hierarchical.
Digital Item	A Digital Item is a bitsequence with a defined representation and identification. It is indivisible (cannot contain other digital items). There may be a many to 1 relationship between digital items and a data file.
Digital Medium	The physical material on which digital information may be encoded for eventual access. Digital medium may include, in addition to the physical material, the packaging and form factor that is utilized for that material.
Digital Resource	A resource is an individually addressable bitsequence within the system. The identification of a resource resolves to a bitsequence that represents informational content without a need to reference any other bitsequence.
Disaster Recovery	A complete state of restoration of a system component, Instance or facility.
Dispose	To carry out disposition instructions to destroy or donate temporary records after their retention period expires or other records without permanent value.
Disposition (n)	Those actions taken regarding records no longer needed for the conduct of the regular current business of the originator.
Disposition Agreement	A general term that includes all types of agreements (such as records schedules and deposit agreements) that contain disposition items with associated disposition instructions.

Disposition Agreement Package	A collection of assets related to a Disposition Agreement, such as a records schedule, an appraisal report, a Federal Register notice, Transfer Agreement, Preservation and Access Plan, etc.
Disposition Instruction	An instruction contained in a disposition agreement that mandates what is to be done with documentary materials at certain points in their lifecycle. Disposition Instructions may consist of: • Specification of the length of time material should be retained by their creator or custodian (a retention period) • Conditions under which the creator or custodian should terminate retention • Physical or legal transfer of material to another custodian • Destruction of records, or stipulation that the material is not to be destroyed
Disposition Item	A separate entry on a disposition agreement that pertains to one series or other body of documentary materials.
Document	A structured unit of recorded information, logical or physical, not fixed as a record.
Document Template	A set of specifications about a type of document that governs its format and behaviors.
Documentary Material	Records (temporary or permanent), non-record material, personal papers or artifacts that refer to all media containing recorded information, regardless of the nature of the media or the methods or circumstances of recording.
Documentation	(1) In archival usage, the creation or acquisition of documents to provide evidence of the creator, an event, or an activity. (2) In electronic records, an organized series of descriptive documents explaining the operating system and software necessary to use and maintain a file and the arrangement, content, and coding of the data which it contains.
Documented Effects	Each digital adaptation processor will have known and "documented effects", which are discovered through designing and testing the processor software itself.
DOD 5015.2	A DOD and NARA approved set of requirements for ERM applications.
Donated Historical Material	Documentary material that has been transferred into NARA's legal custody via a deed of gift from a person or non-Federal organization.
Donor Disposition List	A type of NARA-prepared disposition agreement that pertains to materials that are under consideration for donation prior to the execution of a deed of gift.
Dynamic	Pertaining to an event or process that occurs during computer program execution; for example, dynamic analysis, dynamic binding. Contrast with static.
Dynamically Persisted System Data	Important non-static data in the system like the Directory, Access Policies, user personalization data not addressed by deployed "configuration support files".
Electronic Document	A document that consists of information that is recorded in a form that only a computer can process.
Electronic Document Management (EDM)	Functionality to support the computerized management of electronic and paper-based documents. Associated components include a system to convert paper documents to electronic form, a mechanism to capture documents from authoring tools, a database to organize the storage of documents, and a search mechanism to locate the documents.
Electronic Record	A record in a form that only a computer can process.

[illegible]	[illegible]
Electronic Records Management (ERM)	Functionality to support record collection, organization, categorization, storage of electronic records, metadata, and location of physical records, retrieval, use, and disposition.
Electronic Records Preservation And Service Plan	A Preservation and Service Plan that applies to an aggregate of electronic records.
Electronic Signature	A technologically-neutral term indicating various methods of signing an electronic message that (a) identify and authenticate a particular person as the source of the electronic message; and (b) indicate such person's approval of the information contained in the electronic message (definition from GPEA, Pub.L. 105-277). Examples of electronic signature technologies include PINs, user identifications and passwords, digital signatures, digitized signatures, and hardware and biometric tokens.
Enterprise Content Management (ECM)	An automated system with the functionality to capture, manipulate, retrieve, and publish the entire inventory of digital assets (e.g., Web pages, office documents, databases, scanned images, e-mail) created by an organization.
Enterprise, Enterprise-Wide	Implementation of a service, function, or software application throughout all levels and components of an agency or organization.
Equity Holder	An entity (such as a Federal or Presidential organization, or an individual) that owns or has a stake in information found in a record, and therefore must participate in decisions relating to the release, redaction, and withdrawal of records during access review.
Error	(1) The difference between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. For example, a difference of 30 meters between a computed result and the correct result. (2) An incorrect step, process, or data definition. For example, an incorrect instruction in a computer program. (3) An incorrect result. For example, a computed result of 12 when the correct result is 10. (4) A human action that produces an incorrect result. For example, an incorrect action on the part of a programmer or operator.
Escalation	Taking some action when the allocated time for a process step is exceeded. Actions might include: • return to originator • forward to higher level approver • automatic approval
Essential Characteristics	Those properties/characteristics of electronic records that must remain unchanged through transfer, ingest, storage, and presentation or output of records.
Event Log	The recording of activities performed by ERA for the purpose of providing audit trails, accountability information, and the re-creation of events.
Execute	To carry out an instruction, process, or computer program.
Export - Media	Controlled removal of media from ERA archival assets.
Export - Record	To remove a record from ERA and provide it to another system or user. The exported record no longer exists in ERA at the conclusion of an export. Export may or may not include the records life cycle data pertaining to the exported record.

Expunge Record	Complete removal of a record and all related information such that no trace of the record's existence or its audit trail information remains in the system.
Facility	An actual physical location that contains one or more Instances, one or more Federations, and may also contain a SOC.
Fault Tolerance (Software Design And Software Design Concepts)	(1) The ability of a system or component to continue normal operation despite the presence of hardware or software faults. (2) The number of faults a system or component can withstand before normal operation is impaired. (3) Pertaining to the study of errors, faults, and failures, and of methods for enabling systems to continue normal operation in the presence of faults.
Federal Enterprise Architecture (FEA)	A strategic information asset base, which defines the business, the information necessary to operate the business, the technologies necessary to support the business operations, and the transitional processes necessary for implementing new technologies in response to the changing business needs. It is a representation or blueprint.
Federal Enterprise Architecture Framework (FEAF)	An organizing mechanism for managing development, maintenance, and facilitated decision making for federal information technology resources. The framework provides a structure for organizing federal resources and for describing and managing Federal Enterprise Architecture activities.
Federal Records Legal Transfer Instrument	A type of legal transfer instrument used specifically for the transfer of legal custody of Federal records. Note: This instrument is currently the SF 258.
Federation	A group of one or more Instances with the same data classification level.
Fee Bearing Service	An ERA capability for which a fee may be charged.
Fidelity	(1) A measure of the congruence between the renditions of two digital items when measured in terms of specified behaviors and attributes. In the ERA context this is generally a measure of the similarity of a human subject's experience of the rendition of a digital item in the technical environment for which it was created and the rendition of a different digital item, intended to be perceived from a human subject's point of view as the same, in its technical environment. (2) Accuracy of reproduction.
File Plan	(1) A plan designating the physical location(s) at which an agency's files are to be maintained, the specific types of files to be maintained there, and the organizational element(s) having custodial responsibility. (2) A document containing the identifying number, title, or description, and disposition authority of files held in an office.
File Unit	(1) A record aggregate made up of an organized unit of documentary materials grouped together either for current use or in the process of archival arrangement. A file unit is the intellectual grouping of the material, which may or may not equal the physical grouping. For example, a case file may be housed in several physical folders, but described as one file unit. (2) The middle level of hierarchical description as defined by NARA, which describes the above aggregate.
Final Operating Capability (FOC)	The complete set of ERA capabilities when the system is fully deployed and fully operational.
Foreign Language Extensibility	Designing the ERA System such that it may be enhanced to accommodate foreign (non-English) languages if needed without major rework to the system.

Framework	An abstract set of interactions, which define canonical protocols on how services interact with each other.
Free Text Search	A search in which the user input can be anything textual.
Freedom Of Information Act (FOIA) Request	A request, made based on the provisions of the Freedom of Information Act, for access to restricted information in Federal records held by NARA, including NARA operating records subject to the FOIA, or for access to Presidential records in the custody of NARA that were created after January 19, 1981 and are subject to the Presidential Records Act.
Functional Behaviors	Functionality in the software or hardware that originally manipulated a digital object which defined how the user could interact with the object in its original context. These behaviors are inherent in the software or hardware that created or materialized the digital item, not in the item itself. There is no reference to them in the digital item and it may be impossible to infer them from the digital item.
Functional Design	(1) The process of defining the working relationships among the components of a system. (2) The result of the process in (1).
General Records Schedule	(1) A type of records schedule issued by NARA which governs the disposition of specified Federal records common to several or all agencies. (2) A records schedule governing specified series of records common to several or all agencies or administrative units of a corporate body (Society of American Archivists Glossary). The NARA General Records Schedules (GRS) provide disposition authority for temporary administrative records common to several or all agencies of the Federal Government.
Geographic Information	The geographic area represented in the archival materials. Appropriate geographic information for the archival materials should be chosen from a Geographic Authority File.
Geospatial Identifiers	Information that identifies the geographic location and characteristics of natural or constructed features and boundaries on the earth. This information may be derived from, among other things, remote sensing, mapping, and surveying technologies. Contrast with geographic information, which specifies places by name.
Government Function	A government activity or program, possibly spanning more than one agency or organization.
Government Line of Business	A general area or subject in which the government works (internally or externally), such as education, national defense, or transportation. Lines of business are defined under the Federal Enterprise Architecture (FEA) Business Reference Model (BRM) at www.feapmo.gov/fea.asp.
Grammar	A formal definition of the syntactic structure of a language, normally given in terms of production rules which specify the order of constituents and their sub-constituents in a sentence (a well-formed string in the language). Each rule has a left-hand side symbol naming a syntactic category (e.g. "noun-phrase" for a natural language grammar) and a right-hand side that is a sequence of zero or more symbols. Each symbol may be either a terminal symbol or a non-terminal symbol. A terminal symbol corresponds to one "lexeme" - a part of the sentence with no internal syntactic structure (e.g. an identifier or an operator in a computer language). A non-terminal symbol is the left-hand side of some rule. One rule is normally designated as the top-level rule that gives the structure for a whole sentence.

Help Desk Tiers	The ERA help desk will use a three tiered structure. Customer service representatives staff Tier 1 and as the initial point of contact they will answer the majority of help questions for ERA users. Tier 2 are system administrators, and Tier 3 are other ERA development and maintenance technical staff. Help issues will be escalated to the tier required to resolve the issue.
Hierarchical Description	The principal of archival description in which records are described in aggregates at various prescribed hierarchical levels. At NARA these levels range from the largest grouping (series) to the intermediate level (file unit) to the smallest (item). Descriptions of records at the series level are also linked to one of two types of archival control groups: a record group or a collection.
Identical Copy	A copy of a document that has the same content, structure, and presentation as the original.
Identification	An assertion by the subject of who the subject is.
Identity And Rights Templates	Templates used to define the nature and rights of identities on records.
Identity authentication	Proof offered by the subject of the asserted identity.
Implementation	(1) The process of translating a design into hardware components, software components, or both. (2) The result of the process in (1).
Information	A collection of data, ideas, thoughts, or memories. Information and data are near synonyms. Where data connotes facts, ideas, or information in its most atomized form, information refers to more complex concepts made up of multiple data elements. Information may take many forms, including words, sounds, images, and formulas.
Informational Content	The meaning a human subject attributes to a specific manifestation of a digital item, or collection of digital items. That meaning will be inferred from the data content and the behaviors manifested with the data content of a digital item in a specific context and from any explicitly declared or inferred relationships between digital items manifested together. [Two digital items appearing together on the same screen, for example an advertisement on a Web page, may be perceived as related or not]. Informational content will likely change with a change in behaviors.
Ingest	The process of moving records into the ERA System.
Initial Operating Capability (IOC)	The set of ERA capabilities available for use upon completion of the initial deployment of ERA.
Inspections	A static analysis technique that relies on visual examination of development products to detect errors, violations of development standards, and other problems. Types include requirements inspections, code inspections; design inspections.
Instance	An Instance comprises the applicable security appliances (firewalls, intrusion detection devices), hardware (servers connected by routers and switches) and software (System-level Services) necessary to operate the ERA functionality within a specific Federation at an individual facility. An Instance only operates on one classification level.

Instrument of Transfer	A type of legal transfer instrument which can be used when neither a deed of gift nor Federal records legal transfer instrument is applicable, for example in the transfer of Presidential records.
Integrity	The integrity of a record refers to its being complete and unaltered.
Integrity Constraints	Component of NARA Conceptual Data Model; rules that the data must follow in order to participate in a given association.
Item	(1) The smallest intellectually indivisible archival unit (e.g. a letter, memorandum, report, leaflet, or photograph). (2) The lowest level of hierarchical description as defined by NARA, which describes the above material.
Layering	A form of cohesion in which the facilities for providing or accessing a set of services through a standard software API or hardware interface are logically kept together.
Legal Custody	To have legal control and responsibility for a specific group of records.
Legal Transfer Disposition Instruction	A type of disposition instruction that mandates the transfer of legal custody of the documentary materials to the National Archives.
Legal Transfer Instrument	An instrument, usually a document, which formally conveys the legal custody of documentary material to the National Archives.
Life Cycle Document Templates	Templates used to create documents that will become records in the Archives.
Location Transparent Access (To Assets)	A user, or a component of the system, will not need to know the location of a record within ERA in order to access that record. A search capability will locate requested records based on entered search criteria.
Logical Behaviors	Transformations to the content or presentation of the content of a digital item that could be optionally executed by a user in the original context that created that item. These logical behaviors are defined in associated processing instructions.
Losslessly	A term to describe the outcome of (hardware) compression that does not rely on removing data in order to reduce file size. With lossless compression, the results of the algorithm can be reversed to completely recover the original data. With lossless compression, every single bit of data that was originally in the file remains after the file is uncompressed.
Magnetic Remanence	A measure of the magnetic flux density remaining after removal of the applied magnetic force. Refers to any data remaining on magnetic storage media after removal of the power.
Maintenance	(1) The process of modifying a software system or component after delivery to correct faults, improve performance or other attributes, or adapt to a changed environment. (2) The process of retaining a hardware system or component in, or restoring it to, a state in which it can perform its required functions.
Material In Courtesy Storage	Documentary material which NARA stores at no charge as a courtesy to the owner, and for which the owner maintains legal custody of the material. Such material may or may not eventually be donated

Media Migration	The act of moving electronic records and related data from one piece of media to another, usually in response to improving media technology, to avoid the inability to access records on media that is becoming obsolete, or to move records from media that is deteriorating onto fresh media.
Mediated Search	A search for records or information about records during which the person searching is assisted by NARA personnel.
Mediated Search Request	A request for a search for documentary materials or information about documentary materials during which the person searching is assisted by NARA personnel
Medium	The physical material in or on which information may be recorded (e.g. paper, magnetic tape, film).
Metadata	Information about a digital item that provides the context necessary to establish its quality as a record, or to provide reference to the content. The contextual information may include provenance, the original order of objects in the record, lifecycle information, intellectual property rights, access restrictions, and information about the form of the digital object, its attributes and behaviors.
Metric	A quantitative measure of the degree to which a system, component, or process possesses a given attribute.
Model	An object representing data or even activity.
Model Template	A template created to be copied and modified for the creation of new templates.
Modeling	The process of gaining understanding about a system by creating representations that exhibit similar properties but in a more tractable manner.
NARA-Prepared Disposition Agreement	A type of disposition agreement which allows NARA to establish adequate intellectual control of documentary material for management purposes prior to their physical or legal transfer. Note: These agreements will allow NARA to ingest materials into the ERA System, and can be used (as appropriate) to inventory, track, and plan for the arrival and processing of materials. They may be created entirely by NARA without any participation by the Transferring Entity
Non-Electronic Document	A document that consists of information that is recorded in a form that can be understood without the aid of a computer.
Non-Electronic Record	Any information that is recorded in a form that can be understood without the aid of a computer and that satisfies the definition of a record.
Non-Electronic Records Preservation and Service Plan	A Preservation and Service Plan which applies to an aggregate of non-electronic records.
Non-Repudiation	Steps taken by an agency to provide assurance, via the use of an audit trail, that a sender or initiator of an activity cannot deny being the source of a message or the initiator of the activity, and that a recipient cannot deny receipt of a message.
Notice	For the purposes of this SyRS, any communication originating from ERA to a user or group of users of the system. Notices may inform users of scheduled system downtime, the availability of search results, or other information that needs to be conveyed to users.
Object (Digital)	A discrete Instance of data (i.e. a record, description, etc) intended to be managed by the ERA System.

Object class	Component of NARA Conceptual Data Model; defines as clearly distinguishable real world phenomena and are atomic, i.e., they cannot be decomposed further into other classes.
Object-Oriented Design (Software Design and Software Design Strategies and Methods)	A software development technique in which a system or component is expressed in terms of objects and connections between those objects. Contrast with functional design, data-structure design.
OC3	Fiber Optic connection capable of transferring data at 155.52 Mbps.
OC48	Fiber Optic connection capable of transferring data at 2.488 Gbps.
Offsite	An operational site which is physically separated from the site performing a particular operational activity.
Online Certificate Status Protocol [OCSP]	A draft Internet communications protocol of the IETF X.509 PKI Working Group that is useful in determining the current status of a digital certificate without requiring certificate revocation lists.
Online Form	Online Forms are software versions of physical forms (e.g. SF115, SF258, etc). The term "online form" is not envisioned to extend to all Web forms for each process step.
Orchestrations	Orchestrations invoke service methods in a specific order, based upon a defined business process.
Original Order	The arrangement of records established by the creator, preserved by NARA in order to preserve existing relationships, evidential significance, and the usefulness of finding aids supplied by the creator.
Output A Record	A means of making a record available outside of the system, such as copying files to digital media, printing records to paper, or transmitting copies over the internet. The record in ERA archival storage is not affected by being output.
Perceptual Behaviors	Data embedded within a digital item that represent values which, when processed by the software that interprets that data type, defines how a human subject would perceive the content of the digital item. These behaviors may include data that define all aspects of human perception, such as Visual (color, size number of dimensions, location in visual space, perspective, illumination, etc.), Audio (frequency, volume, acoustics, etc), and Movement (3 dimensional orientation, momentum, acceleration
Performance	The degree to which a system or component accomplishes its designated functions within given constraints, such as speed, accuracy, or memory usage.
Permanent Record	A record that has sufficient historical or other value to warrant its continued preservation by the Federal Government beyond the time it is needed for administrative, legal, or fiscal purposes.
Persistent Format	A data type, which may be simple or complex, that is independent of specific hardware or software, such that an object in this data type can be transferred from a source platform to an arbitrary target platform with no significant alteration of essential attributes or behaviors.
Physical Custody	To have physical control of and responsibility for a specific group of records.

Physical Media	The physical material in or on which information may be recorded (e.g. magnetic disks, magnetic tape, film).
Physical Transfer Disposition Instructions	A type of disposition instruction which mandates the transfer of physical custody of the documentary materials to a records center the National Archives, or another type of custodian.
Portal	A personalized user interface that contains an aggregate of tools relevant to a user's role.
Portlet	A Web-based component that will process requests and generate dynamic content. The end-user would essentially see a portlet as being a specialized content area within a Web page that occupies a small window in the portal page. The portlet provides users with the capability to customize the content, appearance and position of the portlet.
PRA Instrument of Transfer	A type of legal transfer instrument which references The Presidential Records Act to document the transfer of legal custody of Presidential records.
Present Electronically	The act of reproducing records on an electronic device, as opposed to producing hard copies, printing text or images to paper, or writing records to media. The records in ERA archival storage are not affected by being presented electronically.
Preservation	Processes and operations involved in ensuring the technical and intellectual survival of authentic records through time.
Preservation and Access Level (PAL)	The related services for preservation and access to a set of electronic records maintained in the ERA System. NARA will specify standard PALs for given record types and data types.
Preservation and Service Plan	A plan, based on the results of a preservation assessment, indicating the activities to be undertaken in preserving specific documentary material or sets of documentary material and the level of service NARA plans to provide for them.
Preservation Assessment	(1) The review of records to determine the records' current condition and potential need for preservation processing. (2) The results of this review.
Preservation Copy	A copy of a record used solely in the processes and operations involved in the stabilization and protection of the record against damage or deterioration.
Preservation Objective Model	A signature of the preservation requirements for a particular record type of given provenance.
Preservation Process	A process appropriate for ensuring the continued existence, accessibility, and authenticity of records over time.
Presidential Records Disposition List	A type of NARA-prepared disposition agreement which pertains to records which will be transferred from a Presidential administration.
Printable Assets	Electronic assets that can be rendered two dimensionally by a printing device.
Privacy Act Amendment Information	Privacy Act amendment information is the data provided by the requestor that describes the amendment, such as the date of request, requestor identification and the requested amendment itself.
Process	(1) A sequence of steps performed for a given purpose; for example, the software development process. (2) An executable unit managed by an operating system scheduler. (3) To perform operations on data.

Project Plan	A document that describes the technical and management approach to be followed for a project. The plan typically describes the work to be done, the resources required, the methods to be used, the procedures to be followed, the schedules to be met, and the way that the project will be organized, e.g., a software development plan.
Provenance	The organization or individual that created, accumulated, or maintained the records in the conduct of business, and/or maintained records in the conduct of business prior to their transfer to NARA.
Public Key Infrastructure [PKI]	An IT infrastructure that enables users of a basically unsecure public network such as the Internet to securely and privately exchange data through the use of a public and a private cryptographic key pair that is obtained and shared through a trusted authority.
Record	(1) A unit of recorded information created, received, and maintained as evidence or information by an organization or person, in pursuance of legal obligations or in the transaction of business. (2) All books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the U.S. Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them.
Record Behavior	For the purposes of this SyRS, the ability of a record presented or output by ERA to do essentially the same things it could do when in use by the transferring entity.
Record Creator	See Creator.
Record Group	A type of archival control group consisting of an administrative grouping of organizationally related records established by an archival agency after considering the organization's administrative history and complexity and the volume of its records.
Record Manifestation	A deliverable package.
Record Presentation	The process or the result of a process, of transforming an electronic record from a digital storage format into a form in which it can convey to a human the information it was intended to communicate.
Record Series	File units or documents arranged in accordance with a filing system or maintained as a unit because they result from the same accumulation or filing process, the same function, or the same activity; have a particular form; or because of some other relationship arising out of their creation, receipt, or use. (Society of American Archivists Glossary)
Record Structure	The relationships between digital items in a "complex digital item," a digital container, or an aggregate of containers and items that singularly or collectively make up a record. The record structure defines which items are associated to other items, and the nature of that association, such as child, parent, or sibling and whether items are embedded in other items, as in a complex digital item.
Record Type	The intellectual form of the records, such as letter, memo, greeting card, or portrait.

Records Center	A facility for the storage and servicing of records pending their disposal or transfer to the National Archives. Records centers include NARA-authorized agency records centers and NARA-operated Federal records centers.
Records Lifecycle	An archival concept that describes the lifespan of a record, from its creation or receipt to its final disposition. The records lifecycle is divided into the following stages or phases: creation/receipt, maintenance and use, retirement, final disposition, and continuing use.
Records Lifecycle Data	All data collected by NARA that pertains to the records throughout their lifecycle. This includes all data related to records lifecycle management processes, including data collected during scheduling, physical transfer, legal transfer, and description.
Records Lifecycle Transaction	Activity performed on records throughout their existence that changes their status in the records lifecycle. Such transactions include the scheduling and appraisal of government records, the development of deposit agreements, the retirement of records to NARA's physical custody, the transfer of permanent records to the National Archives and Presidential Libraries, destruction, and the review, redaction, and release of information subject to legal restrictions on access. Making a copy of a record is not a lifecycle transaction, because it does not change the status of the record being copied.
Records Schedule	A type of disposition agreement developed by a Federal agency and approved by NARA that describes Federal records (and non-record materials), establishes a period for their retention by the agency, and provides mandatory instructions for what to do with recurring or nonrecurring records when they are no longer needed for current Government business. The term refers to: (1) an SF 115, Request for Records Disposition Authority, which has been approved by NARA to authorize the disposition of Federal records; and (2) a General Records Schedule (GRS) issued by NARA.
Record-Type Specific Template	A template which specifies specific attributes for a specific type of record.
Redaction	The action of following instructions and/or guidelines from equity holders to create a copy of records, in which access restricted information is removed so that the non-restricted information in the record may be made available to the public.
Refreshment	Replacement of media that has: (1) degraded; (2) reached end-of-life based on age; or (3) reached end-of-life based on usage.
Registration Of A Template	Official approval of a template by NARA, and placement of the template in the ERA template repository. Once registered, the template can be used.
Related Materials	A broad variety of items with a perceived connection, relation, or reference to an archival asset or set of assets. Notes: "This glossary uses material as an encompassing, generic term to describe the broad variety of items that an archives might collect, regardless of medium, format, or type. It is used to avoid connotations carried by terms such as record, document, or object. In this sense, materials may be tangible (of matter) or virtual (electronic), and may be used to describe a collection of individual items. In the context of digital information, material is roughly synonymous with resource." (from http://www.archivists.org/glossary/index.asp)

Related Resources	Information and/or services, available for use through a network, with a perceived connection, relation, or reference to an archival asset or set of assets.
Release(Full Release, Partial Release)	A review determination that the record may be accessed by the public, either in full or in part. Full release indicates that the entire record is available for access. Partial release indicates that some information within the record has been withheld by performing redaction, or that a subset of records in a group of records has been withheld.
Reliability (of a Record)	A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities, or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.
Remote Triage	Remote triage is a process for sorting system problems into groups based on their characteristics and severity from a distant location. The steps that a technical team goes through can be considered as a triage of the system. The performance of remote triage will determine the seriousness of a problem and whether there are any steps that should be performed prior to getting more sophisticated help.
Removable Media	Storage media that is intended to be removable such as magnetic tape and optical disk.
Remove Record	Remove a record from the system but maintain its audit trail or other information about it.
Repository	The physical or logical identification of the location of the documentary material.
Representation Information	Information accompanying a digital object, or sequence of bits, that is used to provide additional meaning. It typically maps the bits into commonly recognized data types such as character, integer, and real, and into groups of these data types. It associates these with higher-level meanings that can have complex inter-relationships that are also described.
Requirement	(1) A condition or capability needed by a user to solve a problem or achieve an objective. (2) A condition or capability that must be met or possessed by a system or system component to satisfy a contract, standard, specification, or other formally imposed documents. (3) A documented representation of a condition or capability as in (1) or (2).
Retrieval of Records	The process of locating records, getting them from storage, and preparing them for presentation or output.
Re-validation (of an Electronic Signature)	Re-confirming the validation process for a previously validated electronic signature.
Review Determination	The decision in an access review regarding whether records will be fully released, partially released, redacted, withdrawn, or withheld.
Reviews	A process or meeting during which a work product, or set of work products, is presented to project personnel, managers, users, customers, or other interested parties for comment or approval. Types include code reviews, design reviews, formal qualification reviews, and requirements reviews, test readiness reviews.
Rollback	To reset a system or component back to the previous state. A rollback can include some or all of the operating system, patch, application software, databases, or files.

Routine Report	A report of standardized content and format that is automatically generated by the system on a pre-defined routine basis. Routine reports are under CCB and CM control.
Safe-Store	(1) Data backup approach used to ensure that archival data can survive a range of failures from a simple hardware fault to the catastrophic failure of an entire site. (2) Any (persistent) mechanism for storing data, including but not limited to: relational databases, XML databases, XML files, and text files.
Sample Records	Copies of a representative group of records provided by the creator or a custodian to NARA to support the review of a proposed disposition agreement, an inspection or evaluation of the agency's records management program, or the identification of preservation requirements.
Schedule (n)	As a noun, a synonym for records schedule.
Schedule (v)	As a verb, the processes carried out by a Federal agency to support the development of a records schedule.
SCIF	A facility that complies with a set of physical security standards governing the construction and protection of facilities for storing, processing and discussing Sensitive Compartmented Information (SCI) which requires extraordinary security safeguards.
Self-Describing	An entity whose data structure, format, or layout provides both definitions and values for the data or formats of the entity. A self-describing entity can be evaluated, with all its elements and formats understood, without the need of external references.
Sensorial Behaviors	Data preserved in a digital object that determined how a human would experience the object when rendered in its original context. These may include Visual, Audio, Movement (Orientation and Momentum), Touch, [in future Smell, Taste] behaviors. (See also Perceptual Behaviors.)
Series	(1) A record aggregate consisting of file units or items arranged in accordance with a filing system or maintained as a unit because they result from the same accumulation or filing process, the same function, or the same activity; have a particular form; or because of some other relationship arising out of their creation, receipt, or use. (2) The highest level of hierarchical description as defined by NARA, which describes the above aggregate.
Service	A function that is well defined, self-contained, and does not depend on the context or state of other services.
Service Architecture Templates	Templates used to orchestrate services and make the system self-describing.
Set Of Records	Records grouped together, either physically or virtually, for any purpose. Sets may be hierarchical in nature.
Software	Computer programs, procedures, and possibly associated documentation and data pertaining to the operation of a computer system.
Software Configuration Control	In configuration management, an element of configuration management consisting of the evaluation, coordination, approval or disapproval, and implementation of changes to configuration items after formal establishment of their configuration identification.

Software Configuration Identification	In configuration management, (1) An element of configuration management consisting of selecting the configuration items for a system and recording their functional and physical characteristics in technical documentation. (2) The current approved technical documentation for a configuration item as set forth in specifications, drawings, associated lists, and documents referenced therein.
Software Configuration Management	In system/software engineering, a discipline applying technical and administrative direction and surveillance to: identify and document the functional and physical characteristics of a configuration item, control changes to those characteristics, record and report change processing and implementation status, and verify compliance with specified requirements.
Software Quality Assurance (SQA)	(1) A planned and systematic pattern of all actions necessary to provide adequate confidence that an item or product conforms to established technical requirements. (2) A set of activities designed to evaluate the process by which products are developed or manufactured. (3) The set of activities specified in a Software Quality Assurance Plan, as developed based on IEEE-Standard-730.
Software Requirements Analysis	(1) The process of studying user needs to arrive at a definition of system, hardware, or software requirements. (2) The process of studying and refining system, hardware, or software requirements. (3) Reasoning and analyzing the customers and users needs to arrive at a definition of software requirements.
Software Requirements Specification	(1) A document that specifies the requirements for a system or component. Typically included are functional requirements, performance requirements, interface requirements, design requirements, and development standards. (2) A document that clearly and precisely records each of the requirements of the software system.
Software Tool	A computer program used in the development, testing, analysis, or maintenance of a program or its documentation. Examples include comparator, cross-reference generator, decompiler, driver, editor, flow-charter, monitor, test case generator, and timing analyzer.
Spatial Behaviors	The location in three dimensional space, real or perceived, and which is defined in relation to a specified reference point, at which the manifestation of a digital item is intended to occur, such as a sound that should be perceived to come from behind and above the listener.
Specific Records Schedule	A type of records schedule developed by a Federal agency and approved by NARA that describes Federal records, establishes a period for their retention by the agency, and provides mandatory instructions for what to do with them when they are no longer needed for current Government business. Also called records disposition schedule, records control schedule, records retention schedule, records retention and disposition schedule, or schedule. Note: Currently this process is supported by the SF 115, Request for Records Disposition Authority.
Specified Behavior	Behavior of a record that has been specified in advance of preservation by ERA to be of sufficient importance that it must be maintained through preservation and be available when the record is output or presented.
Standard Language Notice	A notice that is expected to be reused, as opposed to a one-time notice.

[illegible]	[illegible]
Standards – Software	Mandatory requirements employed and enforced to prescribe a disciplined uniform approach to software development
Structure	The physical and logical format of a record and the relationships among the data elements.
Structured Data	Data that resides in fixed fields within a record or file, and has an enforced composition to the atomic data types. Relational databases and spreadsheets are examples of structured data.
Subject	A subject is an entity that attempts to access ERA System resources. The subject may be a human user, a process acting on behalf of a human user, or another system attempting to access the ERA System.
Subject (Archival)	The topic(s) represented in archival material.
Subject area	A high-level classification of a major topic of interest within a data category and is an are of interest centered on a major resource, product or activity. It summarizes the things in which the enterprise is interested.
Subscription	For the purposes of this SyRS, a standing instruction stipulating a specific action to be taken by the system on behalf of the user at the occurrence of a trigger event.
Supplemental Descriptive Information	A type of description in which documentary materials are described in ways which do not meet NARA standards for content and structure.
Support Manual	A document that provides the information necessary to service and maintain an operational system or component throughout its lifecycle. Typically described are the hardware and software that make up the system or component and procedures for servicing, repairing, or reprogramming it.
Support Software	Software that aids in the development or maintenance of other software, for example, compilers, loaders, and other utilities.
Supreme Court Deposit Agreement	A deposit agreement between NARA and the U.S. Supreme Court. (Also see Deposit Agreement.)
System (ERA)	Includes all of the associated equipment, facilities, material, software, hardware, policy, technical documentation, services, and personnel required for operations and support at NARA [of the Electronic Records Archives].
System Metadata Templates	Templates used to process digital objects in the archive.
System Operations Center (SOC)	SOC is the location at which the network, security, and system monitoring and management is performed by a staff of administrators.
Systematic Review (re: Classification)	A complementary program to automatic declassification. Requires all agencies that originate classified information to establish and conduct a systematic declassification review program for classified permanently valuable records for the purpose of declassification after the records reach a specific age. Records exempted from automatic declassification are subject to the systematic review program.
System-high	System-high operation means that all users have the clearance to see all information on the IT system, but do not necessarily have the need to know.
Target Format Processor	A system element (e.g. software code) that takes as input a target data type and renders that data type within a target device.

Target Format Template	A set of instructions that when processed by a Digital Adaptation Processor in conjunction with a persistent object format of a digital item will produce the specified target format version of that item.
TEMPEST	The study and control of spurious electronic signals emitted by electrical equipment.
Template	A set of specifications about a type of record or a set of records.
Template Repository	The repository that contains all registered and deposited templates and template information and which provides services to support the creation and management of templates.
Temporal Behaviors	The sequencing in time of the manifestation of digital items, as in an Orchestration of sounds, the visualization of a sequence of images, or the intermittent appearance of an image.
Temporary Record	A record approved by the appropriate authority for disposal, either immediately or after a specified retention period.
Test Coverage	In Software Testing, the degree to which a given test or set of tests addresses all specified requirements for a given system or component.
Test Design	In Software Testing, documentation specifying the details of the test approach for a software feature or combination of software features and identifying the associated tests.
Test Documentation	In Software Testing, documentation describing plans for, or results of, the testing of a system or component. Types include test design specification, test case specification, test incident report, test log, test plan, test procedure, test report.
Transfer (n)	As a noun, the body of records for which physical custody is so transferred.
Transfer (v)	As a verb, the processes supporting the moving of records from one location to another. Usually used to refer to transfer of records from the creator or custodian to NARA (including Federal records centers).
Transfer Agreement	An agreement between NARA and a transferring entity which specifies how the documentary materials covered by a disposition item will be prepared and physically transferred to NARA.
Transfer Group	A body of documentary materials whose physical transfer is authorized by the same request to transfer. Also referred to as "a transfer"
Transfer Request	A request or offer from a transferring entity to transfer physical custody of documentary materials to NARA, either for archival or records center storage.
Transferring Entity	The individual, organization, Presidential administration, or Federal agency that transfers records to NARA for storage. The transferring entity is either the records creator, an agent of the record's creator, or a successor to the record's creator.
Transformation	The process or the results of a process, of reformatting or otherwise changing the way an electronic record is digitally encoded in order to reduce or eliminate dependencies on specific hardware or software, while preserving authenticity.
Uniform Resource Identifier (URI)	A compact string of characters for identifying an abstract or physical resource. The generic set of all names and addresses which are short strings which refer to objects (typically on the Internet). The most common kinds of URI are URLs andrelative URLs.

Uniform Resource Locator (URL)	An Internet address (for example, http://www.nara.gov/era/), usually consisting of the access protocol (http), the domain name (www.nara.gov), and optionally the path to a file or resource residing on that server (/era/).
Unit Of Work	A generic reference for jobs, and it is a trackable set of records running against a workflow process(es), and tracked as a whole. It is a view from the perspective of a NARA manager tracking assignments, status and completion.
Unscheduled Records	Federal records which are not covered by a disposition agreement.
Usable Record	A record which can be located, retrieved, presented and interpreted.
User Account	A user account is the collection of information about a user that the system uses for determining privileges, access rights, contact information, user ID, user name, etc. Some of the information is owned by the user and may changed by him/her. Other information is asserted by the user, but validated and permitted by NARA ERA administrators. This information cannot be directly changed by the user. The user can assert new information but administrators must verify and permit the assertions.
User Category	A general term used to distinguish types of registered users; including unregistered users.
User Class	A formal term used to differentiate the responsibilities of persons who interact with the ERA System. There are eight classes of users: Transferring Entity, Appraiser, Records Processor, Preserver, Access Reviewer, Consumer, Administrative User, and NARA Manager. Each of these classes typically consists of several user roles.
User Group	A user group is a collection of users, other groups, and rules for group membership that is recognized by the access control security mechanisms. Groups are used as a convenient way to administer a large number of users. Users may be assigned to one or more groups.
User Interface	An interface that enables information to be passed between a human user and hardware or software components of a computer system.
User Role	A user role corresponds to a job set of objectives within the ERA environment. Each role has a distinct set of access rights and privileges to data and to function. A role might be "preserver" or "administrator." Roles are ımplemented using groups; so that every user in the group has the rights and privileged required to perform achieve their job objectives.
User Type	A general term used to differentiate between users. Its exact meaning is contextual.
Validation (of a Record)	The process by which a message/record is confirmed to have originated from an authenticated network user, that is, one who has appropriately established his/her identity on the network.
Validation (System)	(1) The process of evaluating a system or component during or at the end of the development process to determine whether it satisfies specified requirements. Contrast with verification. (2) The process is used for determining whether the requirements and the final, as-built system or software product fulfills its specific intended use.

Verification (System)	(1) The process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. Contrast with validation. (2) The verification process is used for determining whether the software products of an activity fulfill the requirements or conditions imposed on them in the previous activities.
Verification and Validation (V&V)	The process of determining whether the requirements for a system or component are complete and correct, the products of each development phase fulfill the requirements or conditions imposed by the previous phase, and the final system or component complies with specified requirements.
Version	A copy of a document [or object] that has some variation from the original in content, structure, or presentation.
Version (Software)	(1) An initial release or re-release of a computer software configuration item, associated with a complete compilation or recompilation of the computer software configuration item. (2) An initial release or complete re-release of a document, as opposed to a revision resulting from issuing change pages to a previous release. See also: configuration control; version description document.
View	Some form of visualization of the state of the model.
Virus	The term 'virus' as used in the SyRS includes all malicious code which may infect itself into a system. This includes conventional viruses, worms, Trojan horses, adware, spyware, and similar types of malicious code.
Well-Formed	An object is well-formed if it complies with the grammar defined for the object.
Wildcard Character	Characters that can be used to represent one or many characters as a means of specifying more than one name or label during a search procedure.
Withdraw Record	To deny public access to records on the basis of an informed decision rather than in response to a formal access request. These informed decisions may be based on knowledge or assumption that the content of the record is exempt from release based on the FOIA, subject to restrictions placed on Congressional records, sealed court documents, or subject to prohibitions under deeds of gift, or is subject to other restrictions.
Withhold Record	To deny public access to records on the basis of a formal review and pursuant to the provisions of some controlling authority, such as the Freedom of Information Act.
Workbench	A set of end-user tools related to performance of a common role or job in the system. Each role/job has its own workbench that differs from another role/job workbench. The tools themselves are provided by a central authority and controlled under configuration management.

This page intentionally left blank.

APPENDIX B. LIST OF ABBREVIATIONS AND ACRONYMS

[illegible]	[illegible]
24x7	24 hours a day, 7 days a week
A&D	Analysis and Design
AA	(NARA) Application Architecture
AAD	Access to Archival Databases
ABD	Availability Block Diagram
ADRRES	Archives Document Review and Redaction System
AERIC	Archival Electronic Records Inspection and Control System
AMIS	Accessions Management Information System
ANSI/AIA	American National Standards Institute/Automated Imaging Association
APS	Archival Preservation System
ARC	Archival Research Catalog
BPEL	Business Process Execution Language
BPR	Business Process Reengineering
BTP	Business Transformation Plan
C&A	Certification and Accreditation
CAS	Commerically Available Software
CAT	Customer Acceptance Test
CATS	Control and Tracking System
CBT	Computer Based Training
CCB	Change Control Board
CD	Compact Disk
CDR	Critical Design Review
CDRL	Contract Data Requirements List
CDM	Conceptual Data Model
CMRS	Case Management Reporting System
CONOPS, ConOps	Concept of Operations
COOP	Continuity of Operations Plan
COTS	Commercial-Off-The-Shelf
CM	Configuration Management
CM	Common Mode
CRUD	Create, Read, Update and Delete
DAMS	Digital Asset Management System
DCID	Director of Central Intellegence Directive
DEMARC	Demarcation

DID	Data Item Description
DISA	Defense Information System Agency
DMZ	Demilitarized Zone
DNS	Domain Name System
DPRIS	Defense Personnel Records Information System
EA	Enterprise Architecture
ECM	Enterprise Content Management
EDM	ERA Domain Model
ERA	Electronic Records Archives
ERD	En Route Domain
ER	Entity-Relationship
FAQ	Frequently Asked Question
FAR	Federal Acquisitions Regulations
FEA	Federal Enterprise Architecture
FEAF	Federal Enterprise Architecture Framework
FMEA	Failure Modes and Effects Analysis
FMECA	Failure Mode Events and Criticality Analysis
FMO	Future Mode of Operations
FOIA	Freedom of Information Act
FR	Federal Register
FRC	Federal Records Center
FTP	File Transfer Protocol
FOC	Full Operational Capability
GENSER	General Service
GB	Gigabytes
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GPEA	Government Paperwork Elimination Act
GRS	General Records Schedule
GUID	Global Unique Identifier
HHS	U.S. Department of Health and Human Services
HR	Human Resources
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HW	Hardware
ICD	Interface Control Document
IDS	Intrusion Detection System
IDS	Instance Data Store
IE	Information Engineering
IEEE	Institute of Electrical and Electronics Engineers
I&A	Identification and Authentication

[illegible]	[illegible]
I/O	Input/Output
IOC	Initial Operating Capability
IOS	Internetwork Operating System
IPT	Integrated Product Team
IRD	Interface Requirements Document
IRS	Interface Requirements Specification
IRM	Information Resources Management
IT	Information Technology
IWS	Ingest Working Storage
J2EE	Java 2 Platform, Enterprise Edition
JCP	JAVA Community Process
JSP	JAVA Server Pages
JWICS	Joint Worldwide Intelligence Communication System
LAN	Local Area Network
LAR	Load Analysis Report
LCC	Life Cycle Cost
LDAP	Lightweight Directory Access Protocol
LM	Lockheed Martin
LMTSS	Lockheed Martin Transportation and Security Solutions
LSI	Large-Scale Integration
LS&C	Local Services and Control
LTP	Legacy Transition Plan
MDT	Mean Down Time
MIL-STD	Military Standard
MLR	Master Location Register
MILS	Multiple Independent Levels of Security
MLS	Multi-level Secure
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MVC	Model View Controller
NALDS	NWME Automated Log Data Sheet
NARA	National Archives and Records Administration
NCES	Net-Centric Enterprise Services
N/E	Not Established
NIPRNET	Non-Secure Internet Protocol Router Network
NMCI	Navy Marine Corps Intranet
NOIS	NWME Order Information System
O&S	Operations and Support
OA	(NARA EA) Operational Architecture
OAIS	Open Archival Information System
OFAS	Order Fulfillment and Accounting System

OJT	On-the-Job-Training
OMB	Office of Management and Budget
OS	Operating System
PA	Privacy Act
PB	Petabyte (1,024 terabytes)
PCA	Principles, Constraints, and Assumptions
PDF	Probability Density Function
PDR	Preliminary Design Review
PDU	Power Distribution Unit
PGS	Performance Goal Specification
PKI	Public Key Infrastructure
PL	Presidential Library
PM	Preventive Maintenance
PMO	Program Management Office
PMRS	Performance Measurement and Reporting System
POP	Point of Presence
PRA	Presidential Records Act
PWS	Performance Work Statement
QA	Quality Assurance
QMP	Quality Management Plan
RCPOS	Records Center Program Operations System
RD	Requirements Document
RFP	Request for Proposal
SA	(NARA EA)System Architecture
SADD	System Architecture and Design Document
SAML	Security Assertions Markup Language
SAP	Special Access Program
SAR	Special Access Required
SBA	System/Business Applications
SBU	Sensitive But Unclassified
SCI	Secure Compartmented Information
SCIF	Secure Compartmented Information Facility
SDE	System Development Environment
SDR	System Design Review
SecA	Security Architecture
SEMP	System Engineering Management Plan
SHA	Secure Hash Algorithm
SIPRNET	Secure Internet Protocol Router Network
SME	Subject Matter Expert
SNMP	Simple Network Management Protocol
SOA	Service Oriented Architecture

[illegible]	[illegible]
SOAP	Simple Object Access Protocol
SOC	System Operations Center
SOO	Statement of Objectives
SOP	Standard Operating Procedure
SSAA	System Security Authorization Agreement
SSL	Secure Sockets Layer
SSP	System Security Plan
SW	Software
SWIT	Software Integration and Test
SyRS	System Requirements Specification
TAR	Target Release Paper
TB	Terabytes (1024 gigabytes)
TEMPEST	Telecommunications Electronics Material Protected from Emanating Spurious Transmissions
TMO	Transition Mode of Operations
TPM	Technical Performance Measurement
TRM	Technical Reference Model
TS	Top Secret
UCD	Use Case Document
UML	Unified Modeling Language
URTS	Unclassified Redaction and Tracking System
U/SBU	Unclassified and Sensitive But Unclassified
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WFT	Work Force Transformation
WSDL	Web Services Description Language
WWW	World Wide Web
XML	Extensible Markup Language
.NET	Microsoft .NET

This page intentionally left blank.

APPENDIX C. DIAGRAM NOTATION

Overview

The system architecture and design material presented in this document includes diagrams to convey specific aspects of the system. The diagram types were chosen to share a significant amount of relevant information in a consistent format. This Appendix describes the diagram notation used throughout this document. This information is collected in this Appendix to provide readers a reference coincident with the source material. The specific items discussed are as follows:

- Functional Architecture Diagrams
- Class Diagrams
- Sequence Diagrams
- Availability Block Diagrams

Functional Architecture Diagrams

Functional Architecture Diagrams are typical representations of system functional components, system boundaries, external interfaces, and key internal interfaces. These diagrams can exist at any level of system decomposition in order to communicate the components, boundaries, and interfaces at the chosen level.

This ERA SADD includes a functional architecture diagram at the ERA System-level and for each system-level package.

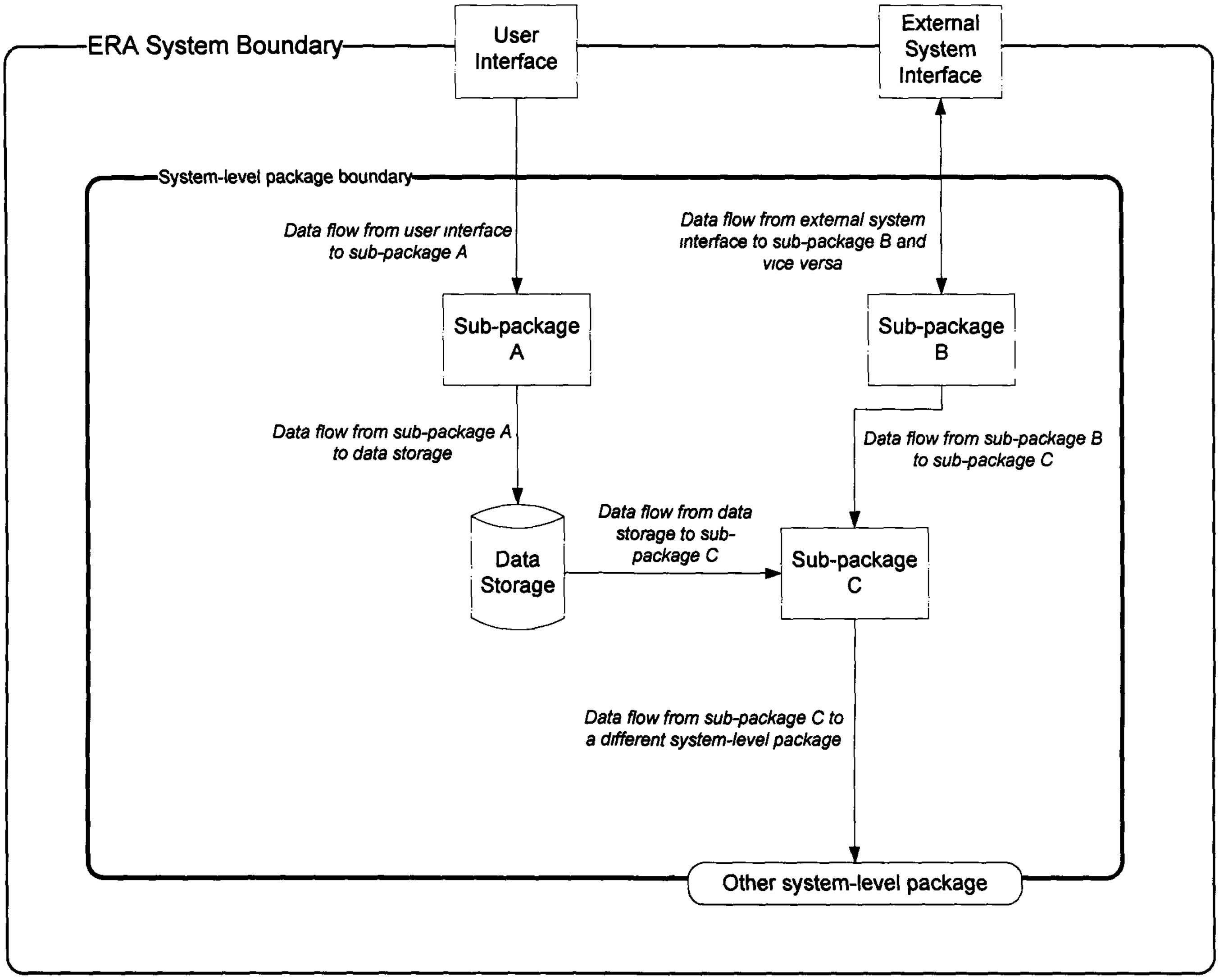
The intent of the functional architecture diagram is to provide a conceptual view of the system that:

- Delineates clearly what is part of the ERA System and what is external to the ERA System
- Identifies the systems and people with which the ERA System must interface
- Identifies the major functions the ERA System must perform
- Identifies the internal interfaces between the major functions in the ERA System
- Identifies the major persistent data stores associated with the major functions in the ERA System

In essence, the functional architecture diagram is a pictorial synopsis of the system requirements. The grouping of related functions and data is intended to provide the starting point for partitioning the system.

An example Functional Architecture Diagram and notation is shown in Figure 48.

Figure 48 – Functional Architecture Diagram Notation


ERA System Boundary
User Interface
External System Interface
System-level package boundary
Data flow from user interface to sub-package A
Data flow from external system interface to sub-package B and vice versa
Sub-package A
Sub-package B
Data flow from sub-package A to data storage
Data flow from sub-package B to sub-package C
Data Storage
Data flow from data storage to sub-package C
Sub-package C
Data flow from sub-package C to a different system-level package
Other system-level package

Class Diagrams

Class Diagrams are a kind of Unified Modeling Language (UML) model. UML is typically used for describing object-oriented software designs. A class diagram "describes the types of objects in the system and the various kinds of static relationships that exist among them. Class diagrams also show the properties and operations of a class and the constraints that apply to the way objects are connected."[20]

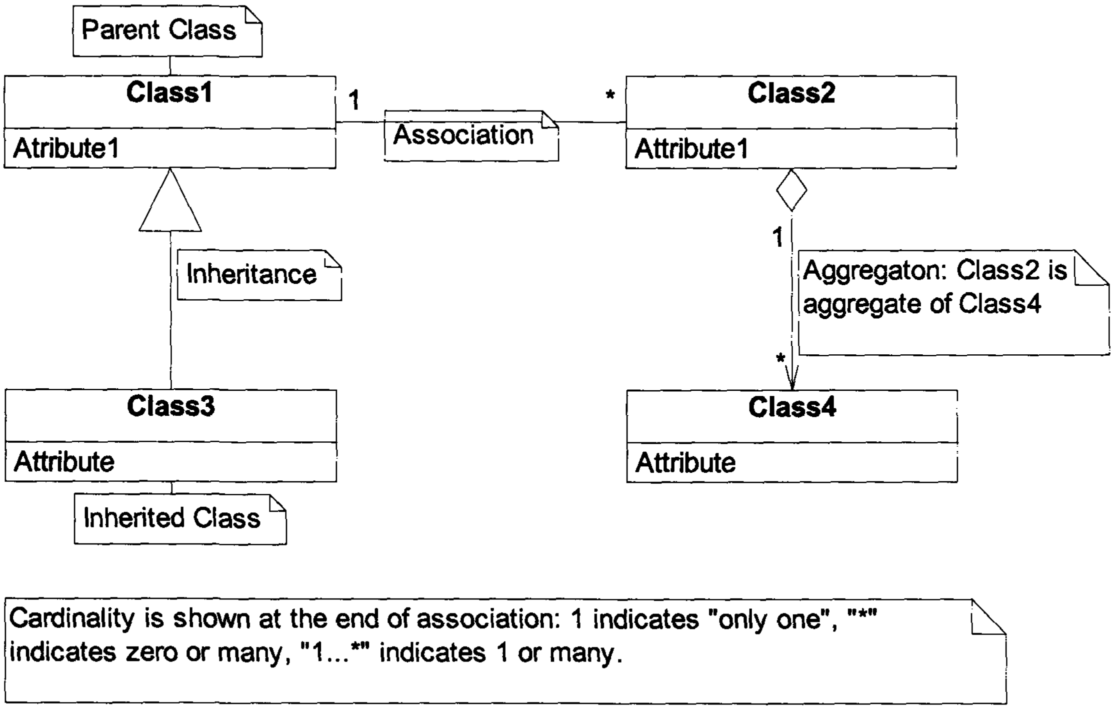
The LM Team has intentionally defined its data classes with only attributes and no operations. This stems from a design decision to keep all operations in the services in the Service Oriented Architecture, and the data classes limited to structural information to promote the concept of the persistent archives. The services can be thought of as classes with only operations and no attributes.

[20] UML Distilled: A Brief Guide to the Standard Object Modeling Language, Martin Fowler, p. 35

This too stems from a design decision to keep all services stateless; in other words, they have no persistent state that would normally be contained in attributes.

An example class diagram illustrating the notation is shown in Figure 49.

Figure 49 – Class Diagram Notation


Parent Class
Class1
Atribute1
1
Association
*
Class2
Attribute1
Inheritance
1
Aggregaton: Class2 is aggregate of Class4
*
Class3
Attribute
Class4
Attribute
Inherited Class
Cardinality is shown at the end of association: 1 indicates "only one", "*" indicates zero or many, "1...*" indicates 1 or many.

Each box in a class diagram represents a specific class. In Figure 49, 4 classes are shown ("Class1", "Class2", "Class3", and "Class4"). Each class box contains three compartments:

- The first compartment shows the class name in bold (e.g., "Class1")
- The second compartment shows the class attributes, which are the structural elements of the class (these roughly correspond to fields in a database table) (e.g., "Attribute1")
- The third compartment shows the class operations, which are the actions (or processes) that the class knows how to perform. Note: the LM Team's class diagrams do not include operations so the example does not show this.

The lines between the classes illustrate different kinds of relationships, including:

- **Association:** This indicates that the two classes are related. The cardinality of the relationship may be one-to-one, one-to-many or many-to-many. Some many-to-many relationships will be resolved into Association classes if this illustrates an important concept. Association is illustratated with a solid line.

- **Inheritance:** This relationship indicates that a sub-class is inherited from a super-class. The sub-class inherits all the attributes of the super-class and has additional attributes. Inheritance is illustrated with a solid line and a large hollow arrow.
- **Aggregation**: The relationship indicates that the aggregate class is made up of the other classes but the associated classes have an existence independent of the aggregate class. Aggregation is illustrated with a solid line and a hollow diamond.
- **Composition:** The relationship indicates that the dependent classes are a part of the composing class (i.e. the related classes have no existence independent of this class). Composition is illustrated with a solid line and a filled-in diamond.

Sequence Diagrams

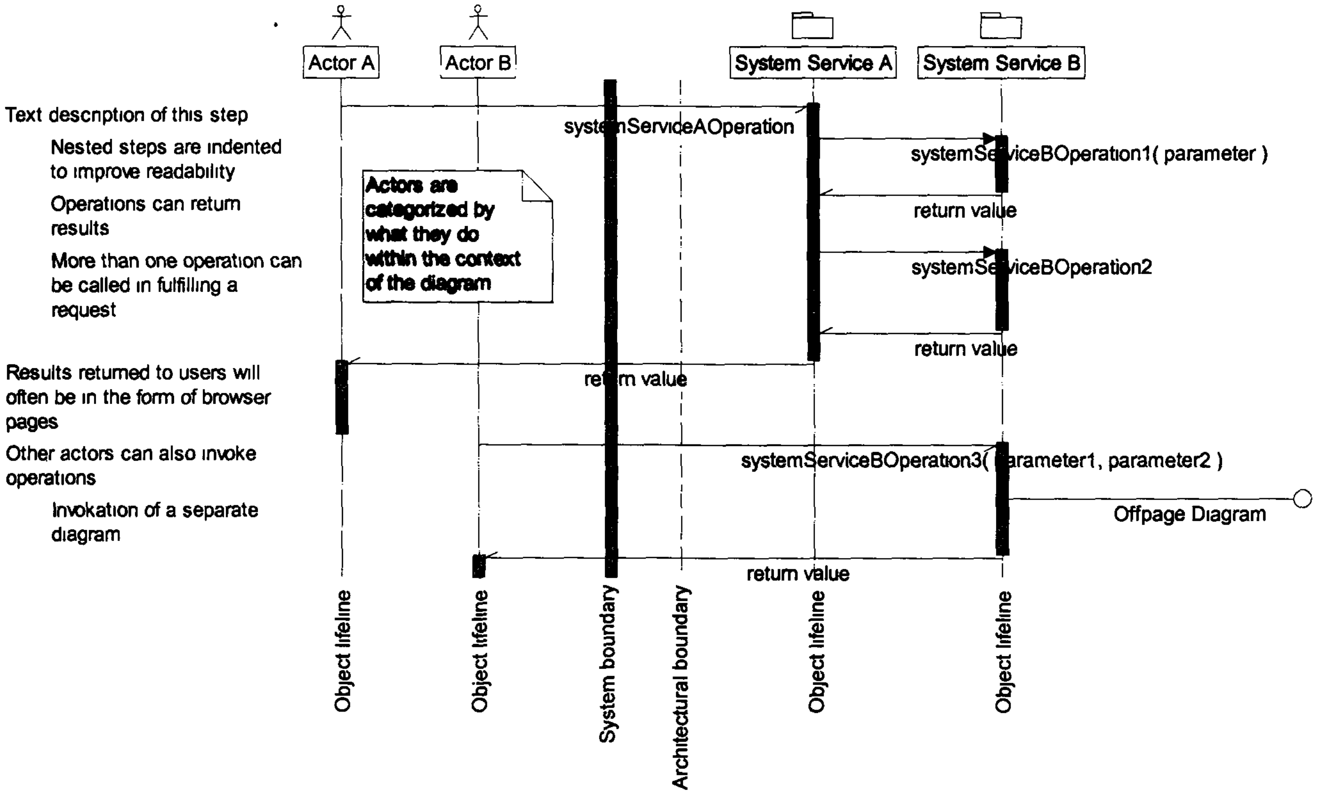
Sequence Diagrams are also a kind of UML diagram. For this document, sequence diagrams are used to illustrate the relative timing and interactions of the system services to achieve a specific action associated with an execution thread.

The primary component of the sequence diagram is the use of UML Objects that are specific Instances of UML Classes. The components, or objects, shown in the diagram include the external interfaces (actors), the system-level package from the software architecture, and significant data stores. The messages between components of the sequence diagram form the basis for a system data model of data interactions and operations in the lower level system specifications.

The LM Team has intentionally abstracted the sequence diagrams presented in this document. For example, every single service/method invocation requires security authorization based on the user's credentials, but including all of these steps would essentially double the size of the sequence diagrams while obscuring the business process. Other common operations, such as logging in, have been simplified and abstracted so that the business process is at the forefront.

An example sequence diagram illustrating the notation is shown in Figure 50.

Figure 50 – Sequence Diagram Notation


Actor A
Actor B
System Service A
System Service B
Text descnption of this step
Nested steps are indented to improve readability
Operations can return results
More than one operation can be called in fulfilling a request
Results returned to users will often be in the form of browser pages
Other actors can also invoke operations
Invokation of a separate diagram
Actors are categorized by what they do within the context of the diagram
systemServiceAOperation
systemServiceBOperation1(parameter)
return value
systemServiceBOperation2
return value
return value
systemServiceBOperation3(parameter1, parameter2)
Offpage Diagram
return value
Object lifeline
Object lifeline
System boundary
Architectural boundary
Object lifeline
Object lifeline

The Description identifies the information associated with each message activity on the diagram and provides additional information or insight into the value of the diagram.

The area between the Architectural boundary and the System boundary is optional and dependent on the type of sequence diagram being illustrated. LANs, VLANs, and user interfaces are good candidates for this area if the inclusion of this detail adds to the understanding of the picture. This may be the case if a number of LANs and VLANs are involved to complete a single related activity. Standard use of a common LAN and VLAN for interactions is left off of these diagrams.

A probe, also called an off-page connector, can be shown to indicate that another sequence diagram is referenced from the current sequence diagram. A probe appears as an off-page connector line with an open circle. The name of the referenced sequence diagram is shown with the probe. A note provides additional reference support for off-page connector references by indicating the figure number of the associated sequence diagram.

The sequence diagrams include several arrow styles to represent operations. Operations to or from and external interface ("actor") are shown with half, open-headed arrows (bottom half). Operations between internal components of the system are shown with closed-headed arrows. Most operations occur synchronously with a single thread of control shown on each diagram. Descriptive text to the left of the diagrams provides information for operations that are not strictly synchronous.

Sequence diagrams can include notes, which are indicated by a yellow box with a folded corner on the upper right side. The notes contain free text about the diagram and may be connected to a relevant portion of the diagram by a dashed line.