UNITED STATES GOVERNMENT PRINTING OFFICE (GPO)

REQUIREMENTS DOCUMENT
(RD V1.0)

FOR THE

FUTURE DIGITAL SYSTEM (FDsys)

Final
May 18, 2005

Document Change Control Sheet

Document Title: Requirements Document (RD)

Date	Filename/version #	Author	Revision Description
5/18/05	FDsys RD v1.0	Future Digital System Phase 3 Team	Preliminary System Requirements

FINAL

Table of Contents

List of Figures v
List of Tables........ v
1.0 Introduction 1
1.1 System Purpose 1
1.2 System Scope 1
1.3 Definitions, Acronyms and Abbreviations........ 1
1.4 References........ 4
1.4.1 Standards and Guidelines 4
1.4.2 GPO Documentation 5
1.4.3 Laws and Regulations 6
1.5 System Overview 6
2.0 General System Description 7
2.1 System Context........ 8
2.1.1 Proposed System Attributes........ 8
2.1 Major System Conditions 11
2.3 Major System Constraints 11
2.4 User Characteristics........ 11
2.5 Operational Scenarios........ 13
2.5.1 Content Originator Scenario........ 14
2.5.2 Content Evaluator Scenario 14
2.5.3 Service Specialist Scenario........ 15
2.5.4 Service Provider Scenario........ 17
2.5.5 Business Manager Scenario 17
2.5.6 Administration/Operations Manager Scenario........ 17
2.5.7 End User Scenario 19
2.5.8 Authentication Scenario 20
2.5.9 Content Rejected at Ingest Scenario........ 20
2.5.10 End User Access Scenarios........ 21
2.5.11 Hard Copy, End User Scenario 22
2.5.12 Electronic Presentation, End User Scenario 22
2.5.13 Hard Copy Quality Complaint, Content Originator Scenario 22
2.5.14 Preservation Process Scenario (Migration)........ 23
2.5.15 Preservation Process Scenario (Emulation)........ 23
2.5.16 Style Tools Scenario 23
2.5.17 Harvesting Scenario 24
3.0 Requirements........ 25
3.1.1 Assumptions........ 25
3.1.2 System Attribute Assumptions........ 26
3.1.1 System Interfaces........ 27
3.2 Requirements List 27
3.2.1 System Overarch (SYS 1.0) 28
3.2.2 Digital Standards........ 28
3.2.2.1 Preservation Standards - SIP (STD 1.0) 28
3.2.2.2 Preservation Standards - ACP (STD 2.0)........ 30
3.2.2.3 Archival Information Package - AIP (STD 3.0) 31
3.2.2.4 Preservation Standards - DIP (STD 4.0) 31
3.2.3 Metadata 32

3.2.3.1 Metadata - Types (MET 1.0)....32
3.2.3.2 Metadata - Core Capabilities (MET 2.0)....33
3.2.3.3 Metadata - Interoperability (MET 3.0)....34
3.2.3.4 Metadata - Collection & Storage (MET 4.0)....34
3.2.3.5 Metadata - Editing, Manipulation, Sharing (MET 5.0)....35
3.2.4 Style Tools....35
3.2.4.1 Style Tools – Capture (ST 1.0)....35
3.2.4.2 Style Tools – Composition (ST 2.0)....36
3.2.4.3 Style Tools – Collaboration (ST 3.0)....37
3.2.4.4 Style Tools – Approval (ST 4.0)....38
3.2.5 Deposited Content....38
3.2.5.1 Deposited Content – Standards (DEP 1.0)....38
3.2.5.2 Deposited Content - Verification and Validation (DEP 2.0)....39
3.2.5.3 Deposited Content – Metadata (DEP 3.0)....39
3.2.5.4 Deposited Content - System Administration (DEP 4.0)....40
3.2.5.5 Deposited Content – Preservation (DEP 5.0)....41
3.2.6 Harvested Content....41
3.2.6.1 Harvested Content – Core Capabilities (HAR 1.0)....41
3.2.6.2 Harvested Content - Harvester Tool Requirements (HAR 2.0)....42
3.2.6.3 Harvested Content - Metadata (HAR 3.0)....43
3.2.6.4 Harvested Content - Rules and Instructions (HAR 4.0)....44
3.2.6.5 Harvested Content - Validation and Authentication (HAR 5.0)....44
3.2.6.6 Harvested Content - System Administration (HAR 6.0)....45
3.2.7 Converted Content....45
3.2.7.1 Converted Content - Standards (CON 1.0)....45
3.2.7.2 Converted Content - Verification and Validation (CON 2.0)....46
3.2.7.3 Converted Content – Metadata (CON 3.0)....46
3.2.7.4 Converted Content - Systems Administration (CON 4.0)....47
3.2.7.5 Converted Content - Preservation (CON 5.0)....48
3.2.8 Content Originator Ordering (COO 1.0)....48
3.2.9 Content Ingest....50
3.2.9.1 Ingest - Core Capabilities (ING 1.0)....50
3.2.9.2 Ingest - SIP Validation (ING 2.0)....51
3.2.9.3 Ingest – Transformation (ING 3.0)....51
3.2.9.4 Ingest – Authentication (ING 4.0)....52
3.2.9.5 Ingest - Version Control (ING 5.0)....52
3.2.9.6 Ingest - Persistent Naming (ING 6.0)....52
3.2.9.7 Ingest - Unique ID (ING 7.0)....52
3.2.9.8 Ingest – Metadata (ING 8.0)....53
3.2.10 Unique Identifier....53
3.2.10.1 Unique ID - Digital Objects (UID 1.0)....53
3.2.10.2 Unique ID - Jobs Order Number (UID 2.0)....53
3.2.10.3 Unique ID - Content Packages (ACP, AIP) (UID 3.0)....54
3.2.11 Persistent Name....54
3.2.11.1 Persistent Naming - Core Capabilities (PN 1.0)....54
3.2.11.2 Persistent Naming – Resolution (PN 2.0)....56
3.2.11.3 Persistent Naming – Metadata (PN 3.0)....56
3.2.12 Authentication....56

3.2.12.1 Authentication - Certification of Content (AUT 1.0) 56
3.2.12.2 Authentication - Verification/Validation of Content (AUT 2.0) 57
3.2.12.3 Authentication - Re-authentication of Content (AUT 3.0) 57
3.2.12.4 Authentication – Credentials (AUT 4.0) 58
3.2.12.5 Authentication - Content Changes (AUT 5.0) 58
3.2.12.6 Authentication - Standards/Best Practices (AUT 6.0).................................59
3.2.12.7 Authentication - Integrity Marks (AUT 7.0) 59
3.2.12.8 Authentication - Records Management (AUT 8.0)......................................60
3.2.12.9 Authentication – Metadata (AUT 9.0) 60
3.2.13 Version Control...61
3.2.13.1 Version Control - Core Capabilities (VER 1.0) 61
3.2.13.2 Version Control - WIP Content Versions (VER 3.0)....................................63
3.2.14 Access...63
3.2.14.1 Access - Core Capabilities (ACC 1.0) 63
3.2.14.2 Search 64
3.2.14.3 Request 74
3.2.14.4 Cataloging and Reference Tools 79
3.2.14.5 Interface..84
3.2.14.6 User Support 87
3.2.14.7 Data Mining 92
3.2.15 Preservation Services 96
3.2.15.1 Preservation - Core Functionality (PRE 1.0) 96
3.2.15.2 Preservation - Preservation Processes (PRE 2.0)......................................96
3.2.15.3 Preservation – Assessment (PRE 3.0) 97
3.2.15.4 Preservation – Administration (PRE 4.0)..98
3.2.15.5 Preservation – Storage (PRE 5.0) 98
3.2.15.6 Preservation – Metadata (PRE 6.0)..99
3.2.15.7 Preservation – Security (PRE 7.0)..99
3.2.16 Content Delivery - Core Capabilities (CD 1.0)..100
3.2.16.1 Content Delivery - Service Provider Information (CD 2.0) 101
3.2.16.2 Content Delivery – Workflow (CD 3.0)...102
3.2.16.3 Content Delivery – Standards (CD 4.0) 102
3.2.17 Hard Copy Output (HC 1.0)...103
3.2.18 Electronic Presentation 104
3.2.18.1 Electronic Presentation - Core Capabilities (EP 1.0) 104
3.2.19 Digital Media..106
3.2.19.1 Digital Media - Overall (DM 1.0) 106
3.2.19.2 Digital Media - Data Storage Devices (CDs, DVDs) (DM 2.0) 106
3.2.19.3 Digital Media - Delivery Mechanisms (DM 3.0) 107
3.2.20 Workflow..107
3.2.20.1 Workflow - Core Capabilities (WF 1.0) 107
3.2.20.2 Workflow - Messaging and Notification (WF 2.0).......................................108
5.4.1.3 Workflow - Resource Requirements (WF 3.0)...109
3.2.20.4 Workflow - Definition Tool (WF 4.0)...109
3.2.20.5 Workflow - Control of Execution (WF 5.0) 110
3.2.20.6 Workflow – Interoperability (WF 6.0) 111
3.2.20.7 Workflow – Monitoring (WF 7.0) 111
3.2.20.8 Workflow – History (WF 8.0)...112

3.2.20.9 Workflow – Notification (WF 9.0) 112
3.2.20.10 Workflow – Status (WF 10.0) 113
3.2.20.11 Workflow - Monitoring Tool (WF 11.0) 113
3.2.20.12 Workflow – Security (WF 12.0) 114
3.2.21 Storage Management 114
3.2.21.1 Functional Data Storage (STO 1.0) 114
3.2.21.2 Storage System Standards (STO 2.0) 116
3.2.21.3 Operational Stores (STO 3.0) 117
3.2.21.4 Contingency Stores (STO 4.0) 119
3.2.21.5 Archival Stores (STO 5.0) 121
3.2.21.6 Storage Management (STO 6.0) 122
3.2.22 Security 124
3.2.22.1 Security - System User Authentication (SEC 1.0) 124
3.2.22.2 Security - User Access Control (SEC 2.0) 124
3.2.22.3 Security - Capture and Analysis of Audit Logs (SEC 3.0) 125
3.2.22.4 Security - User Privacy (SEC 4.0) 126
3.2.22.5 Security – Confidentiality (SEC 5.0) 127
3.2.22.6 Security – Administration (SEC 6.0) 127
3.2.22.7 Availability 128
3.2.22.8 Security – Integrity (SEC 8.0) 129
3.2.22.9 Security – Standards (SEC 9.0) 129
Appendix A – Glossary 132

List of Figures

List of Tables

Figure 1 – Functional Reference Model 7
Figure 2 – System Architecture – User Context 8
Figure 3 – Reference Model 9
Figure 4 – Storage Model 9
Figure 5 – User Classes 12

1.0 Introduction

This Requirements Document (RD) defines the requirements for the Future Digital System (FDsys) and is intended to communicate those requirements to the technical community who will specify and build the system. These requirements do not constitute design or implementation plans.

The following assumptions were made during the development of this RD:

- Readers of this document are expected to have a basic knowledge of the GPO mission and operations. Documents listed in Section 1.4, References, of this RD can provide information helpful in understanding FDsys and the contents of this document.
- IEEE standard 1233-1998 was used to provide guidance to the development of this RD, but it was adapted as appropriate to the GPO's situation.

1.1 System Purpose

The proposed system will ingest, preserve and provide access to electronic content from all three Branches of the U.S. Government. FDsys is envisioned as a comprehensive, systematic and dynamic means for preserving electronic content free from dependence on specific hardware and/or software. The system should automate many of the electronic content lifecycle processes and make it easier to deliver electronic content in formats suited to customers' needs.

1.2 System Scope

The proposed system, FDsys, is unparalleled in scope. GPO is responsible for the preservation and dissemination of information products generated by the entire Federal government, including current, legacy and future products in all conceivable formats. In order to meet GPO's obligations, FDsys must be able to accomplish the following goals:

- Support GPO's content, content management, and content delivery processes and continuing improvements with the efficiency, quality, effectiveness, and timeliness required by those processes;
- Provide access to descriptions of all types of content preserved by GPO;
- Accept/ingest content in a variety of complex formats;
- Accommodate future digital formats;
- Ensure the authenticity of the content that GPO preserves;
- Provide access to the content; and
- Support flexible services for content that GPO will manage on behalf of other Federal agencies.

1.3 Definitions, Acronyms and Abbreviations

The technical terms used in this document are defined in IEEE Std. 610.12-1990, *IEEE Standard Glossary of Software Engineering Terminology*.

See Appendix A, Glossary for Future Digital System and Information Dissemination Projects, for a complete set of definitions.

Table 1-1, Acronyms, provides a list of acronyms used herein.

ACRONYM	DEFINITION
ABLS	Automated Bid List System
ACES	Access Certificates for Electronic Services
ACSIS	Acquisition, Classification, and Shipment Information System
AIP	Archival Information Package
AP	Access Processor
ARK	Archival Resource Key
ASCII	American Standard Code for Information Interchange
BAC	Billing Address Code
BPI	Business Process Information
CA	Certification Authority
CCSDS	Consultative Committee for Space Data Systems
CD	Compact Disk
CD-ROM	Compact Disk Read Only Memory
CE	Content Evaluator
CFR	Code of Federal Regulations
CGP	Catalog of U.S. Government Publications
CMS	Content Management System
CP	Content Processor
CPI	Content Packet Information
CSV	Comma Separated Variable
DARD	Departmental Account Representative
DIP	Disposition Information Package
DO	Digital Objects
DOI	Digital Object Identifier
DoS	Denial of Service
DPI	Dots Per Inch
DVD	Digital Versatile Disc
ePub	Electronic Publishing Section
FAQ	Frequently Asked Question
FBCA	Federal Bridge Certificate Authority
FDLP	Federal Depository Library Program
FIFO	First In First Out
FOIA	Freedom of Information Act
FTP	File Transfer Protocol
GAO	General Accounting Office
GILS	Government Information Locator System
GPEA	Government Paperwork Elimination Act
GPO	Government Printing Office
HTML	Hypertext Markup Language
Hz	Hertz

FINAL

ACRONYM	DEFINITION
ID	Information Dissemination
IEEE	Institute of Electronics and Electrical Engineers
ILS	Integrated Library System
ISO	International Organization for Standardization
IT	Information Technology
JDF	Job Definition format
LOC	List of Classes
LPI	Lines Per Inch
MARC	Machine Readable Cataloging
MOCAT	Monthly Catalog of Government Publications
MPCF	Marginally Punched Continuous Forms
NARA	National Archives and Records Administration
NB	National Bibliography
NET	New Electronic Titles
NFC	National Finance Center
NIST	National Institutes of Standards and Technology
NLM	National Library of Medicine
OAIS	Open Archival Information Systems
OCLC	Online Computer Library Center
OCR	Optical Character Recognition
PCCS	Printing Cost Calculating System
PDA	Personal Data Assistant
PDF	Portable Data Format
PDI	Preservation Description Information
PICS	Procurement Information and Control System
PKI	Public Key Infrastructure
POD	Print On Demand
PPR	Printing Procurement Regulation
PURL	Persistent URL
RI	Representation Information
ROI	Return on Investment
RPPO	Regional Printing Procurement Office
SF	Standard Form
SIP	Submission Information Package
SGML	Markup Language
SMP	Storage Management Processor
SMS	Storage Management System
SPA	Simplified Purchase Agreement
SuDocs	Superintendent of Documents
URL	Uniform Resource Locator
U.S.C.	United States Code
USGPO	United States Government Printing Office
WAIS	Wide Area Information Servers
WAP	Wireless Application Protocol

ACRONYM	DEFINITION
WML	Wireless Markup Language
XML	eXtensible Markup Language

1.4 References

The standards, guidelines, and GPO and Future Digital System documentation used to support the *Future Digital System Requirements Document* are described in the following sections.

1.4.1 Standards and Guidelines

- American Library Association, *et. al. Anglo-American cataloging rules, second edition.* Chicago: American Library Association, 1978.

- Digital Library Federation Benchmark Working Group 2001-2002. *Benchmark for faithful digital reproductions of monographs and serials version 1, December 2002.* Washington, D.C.: Digital Library Federation, 2002. Available at http://www.diglib.org/standards/bmarkfin.htm

- Digital Library Forum. *A framework of guidance for building good digital collections.* Washington, D.C.: Institute for Museum and Library Services, 2001. Available at http://www.imls.gov/pubs/forumframework.htm

- *IEEE guide for information technology-system definition-concept of operations (ConOps) document. IEEE Std. 1362-1998* New York: Institute of Electrical and Electronics Engineers, 1998.

- Interagency Committee on Government Information. *Recommended policies and guidelines for federal public websites*. Washington, D.C.: Office of Management and Budget, 2004. Available at http:www.cio.gov/documents/ICGI/ICGI-June9report.pdf

- Interagency Committee on Government Information. *Requirements for enabling the identification, categorization and consistent retrieval of government information*. Washington D. C.: Office of Management and Budget, 2004. Available at http:www.cio.gov/documents/ICGI/ICGI-June9report.pdf

- Koyanl, Sanjay J., Robert W. Bailey, Janice R. Nall, Susan Allison, et al. *Research-based web design & usability guidelines*. Washington, D.C. [?]: U.S. Department of Health and Human Services, 2003. Available at http://usability.gov/pdfs/guidelines.html

- United States Government Accountability Office. *Government Printing Office: Actions to strengthen and sustain GPO's transformation.* GAO-04-830 Washington: U.S. General Accounting Office, 2004

- W3C. *Web content accessibility guidelines 1.0* Cambridge, MA [?]: W3C, 1999. Available at http://www.w3.org/TR/WCAG10/

- *The large-scale archival storage of digital objects*, Jim Linden, et al, The British Library, Digital Preservation Coalition Technology Watch Series Report 04-03, February 2005, http://www.dpconline.org/docs/dpctw04-03.pdf

- *Strategic Vision for the 21st Century*, U.S. Government Printing Office, December 1, 2004, http://www.main.gpo.gov/pub_print/STRATEGICPLAN.html

1.4.2 GPO Documentation

- *GPO Concept of Operations v2.0.*
- *Baseline Requirements for Digital Reformatting and Delivery of Legacy Federal Documents Collections,* prepared by the Center for Research Libraries, 11/29/04
- *Contract terms, quality assurance through attributes (QATAP).* GPO Publication 310.1, 2002
- *Federal document repositories: decision framework by tangible repository type,* prepared by the Center for Research Libraries, September 18, 2004*
- *GPO agency procedural handbook.* GPO Publication 305.1, 1998
- *Guide to Federal printing and publishing: what every Federal publisher should know about the publishing process.*, [2002?]
- *The Guidelines: best practices for preparing & submitting electronic design & prepress files* GPO Publication 300.6, 2001
- *Managing the FDLP Electronic Collection, Second Edition* , June 18, 2004 *
- *The National Bibliography of U.S. Government Publications: Initial Planning Statement,* June 18, 2004*
- *National Collection of U.S. Government Publications* - Revised June 18, 2004*
- *Printing Procurement Regulations.* GPO Publication 305.3, 1999
- *Report from the Meeting of Experts on Digital Preservation,* March 12, 2004*
- *Report from the Meeting of Experts on Digital Preservation: Metadata Specifications*, June 14, 2004*
- *Style manual.* Washington: U.S. Government Printing Office, 2000
- *U.S. Government Online Bookstore Replacement Proposal, January 2003* [unpublished]
- *U.S. Government Printing Office PKI Business Plan, October 28, 2003.* [unpublished]

*Reports available from http://www.gpoaccess.gov/about/reports/index.html

1.4.3 Laws and Regulations

- "Access to Federal Electronic Information" Title 44 *U.S. Code,* Chapter 41, 2000 edition
- "Depository Library Program" Title 44 *U.S. Code*, Chapter 19, 2000 edition
- "Distribution and Sale of Public Documents" Title 44 *U.S. Code,* Chapter 17 2000 edition
- "Production and Procurement of Printing and Binding" Title 44 *U.S. Code,* Chapter 5, 2000 edition
- "Vocational Rehabilitation and Other Rehabilitation Services--Rights and Advocacy"" Title 29 *U.S. Code* Chapter 16, Subchapter V", 2000 edition

1.5 System Overview

FDsys will be composed of the necessary technology and business practices that will enable GPO to ingest, manage, preserve, and provide access to content that is disseminated in hard copy and to content that is electronically stored.

GPO believes that management of both electronic and non-electronic content should be an integrated process that provides maximum efficiency and value for users. GPO has taken a lifecycle management approach to this data that promotes more effective and efficient processes by sharing relevant data and that promotes seamless transition from one phase to another. The proposed system should support GPO's end-to-end lifecycle management processes, including processes for the creation of content and for the transfer, ingest, management, and access of all electronic and non-electronic content.

The Future Digital System will ingest, preserve, and provide access to the information produced by the U.S. Government--including information produced by all three branches of Government -- and to the material currently in the custody of GPO and Federal depository libraries. The proposed system is envisioned as a comprehensive, systematic, and dynamic means for preserving any kind of content independently of specific hardware and/or software. When it becomes operational, FDsys will enable GPO customers to access and retrieve the content they want, and it will enable GPO to deliver that content in the formats its customers' desire. The system should automate many of the content lifecycle processes and make it easier to deliver the content in formats suited to the needs of GPO customers.

FDsys tools and content must be accessible. Accessibility is making tools and content available and usable for all users including those with disabilities. FDsys will follow established best practices and regulations for accessibility (e.g. Section 508, W3C, etc.)

2.0 General System Description

In order to meet GPO's strategic goals, the Future Digital System should be able to accomplish the following goals:

- Support GPO's content, content management, and content delivery processes and continuing improvements with the efficiency, quality, effectiveness, and timeliness required by those processes;
- Provide access to descriptions of all types of content preserved by GPO;
- Accept/ingest content in a variety of complex formats;
- Accommodate future digital formats;
- Ensure the authenticity of the content that GPO preserves;
- Provide access to the content; and
- Support flexible services for content that GPO will manage on behalf of other Federal agencies.

This will support a functional capability to submit, process and disseminate digitally within a framework of control structure that manages and administers the infrastructure as illustrated in Figure 1 – Functional Reference Model.

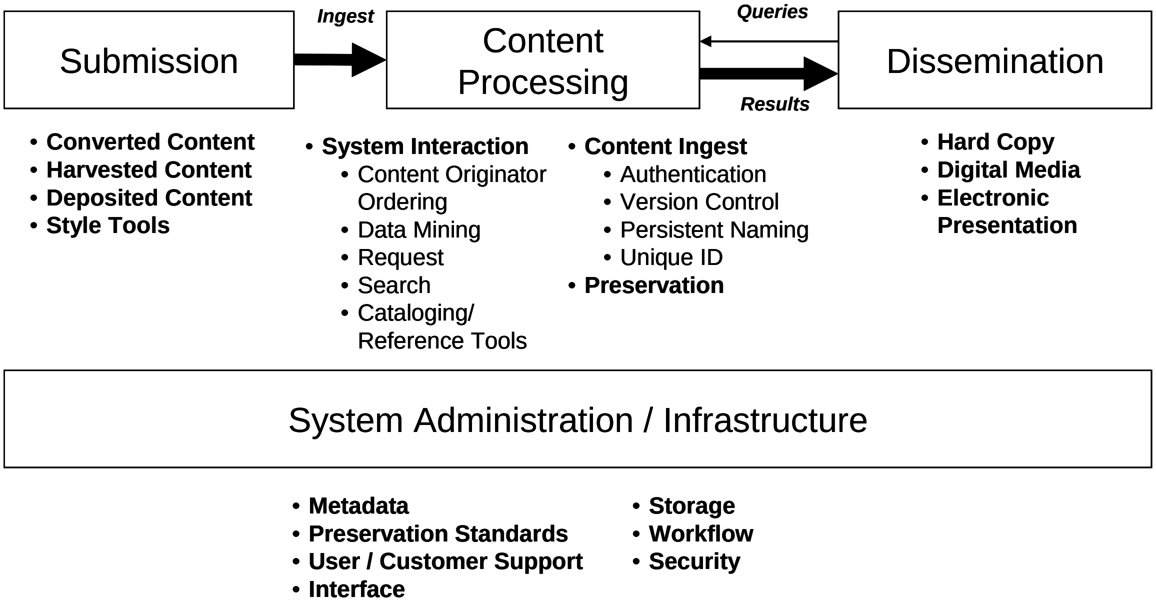

Figure 1 – Functional Reference Model

2.1 System Context

FDsys will be implemented in the context of GPO's strategic goals, existing GPO processes, and legacy systems. This architecture from a user's perspective is shown in Figure 2.

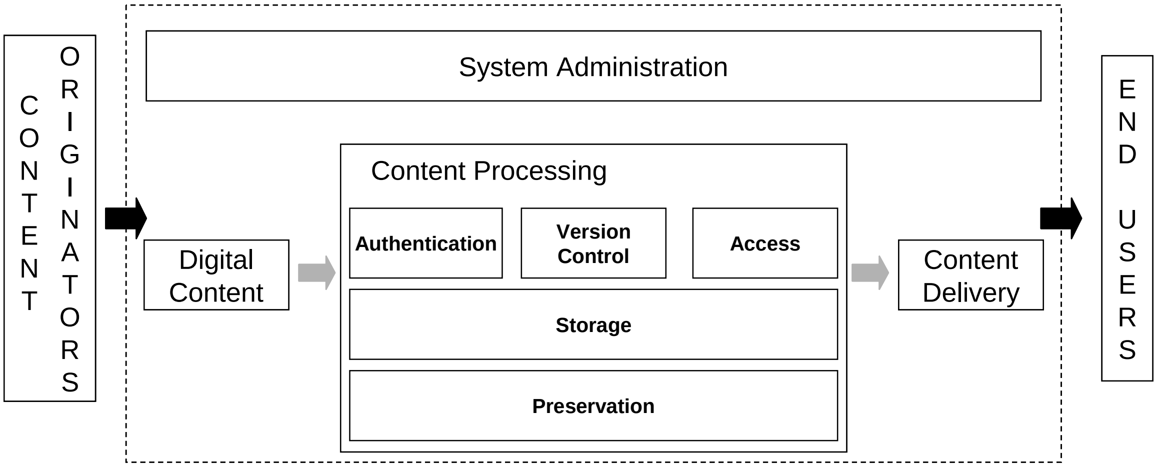

Figure 2 – System Architecture – User Context

2.1.1 Proposed System Attributes

From an overall system perspective, the system should possess the following attributes.

- *Infrastructure independence*: An architecture that allows preservation of content independent of any specific hardware and software that was used to produce them;
- *Modularity*: Ability to use plug-in components that can be replaced with minimal impact to remaining components as workload and technology change;
- *Scalability*: Capable of accommodating growth and managing differing sizes of repositories and ever increasing volumes of content;
- *Extensibility*: Be able to handle additional kinds of content over time, not limited to specific types that exist today;
- *Comprehensiveness*: Provide support for content management lifecycle processes for all types of records; and
- *Flexibility*: Enable GPO to tailor content-based services to suit its customers' needs and enable GPO to implement progressive improvements in its business process over time.

2.1.2 Proposed System Capabilities.

To meet strategic objectives, GPO must integrate its solution for preservation and long-term access to content with the lifecycle management of that content throughout the Federal Government. GPO has adopted the use of the OAIS reference model for an archival system that is dedicated to preserving and maintaining access to digital information.

Figure 3 – Reference Model shows functional model with an adaptation of the OAIS reference model.

Figure 4 – Storage Model shows the conceptual storage model that was created for the system, indicating the categories of storage that the system will utilize.

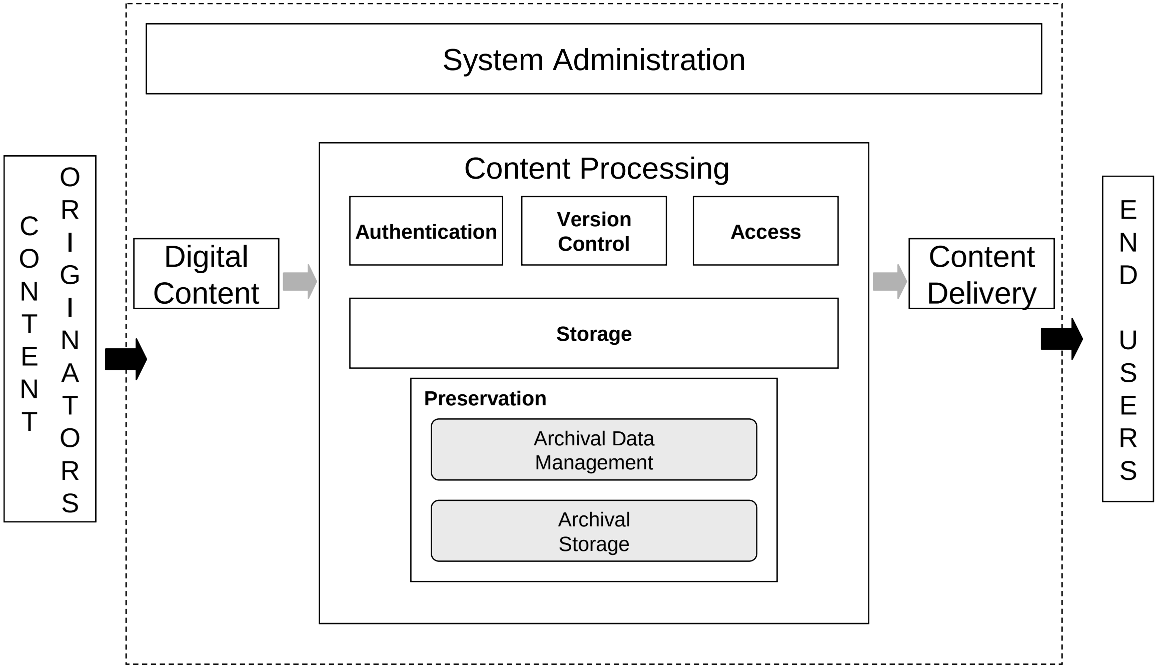

Figure 3 – Reference Model

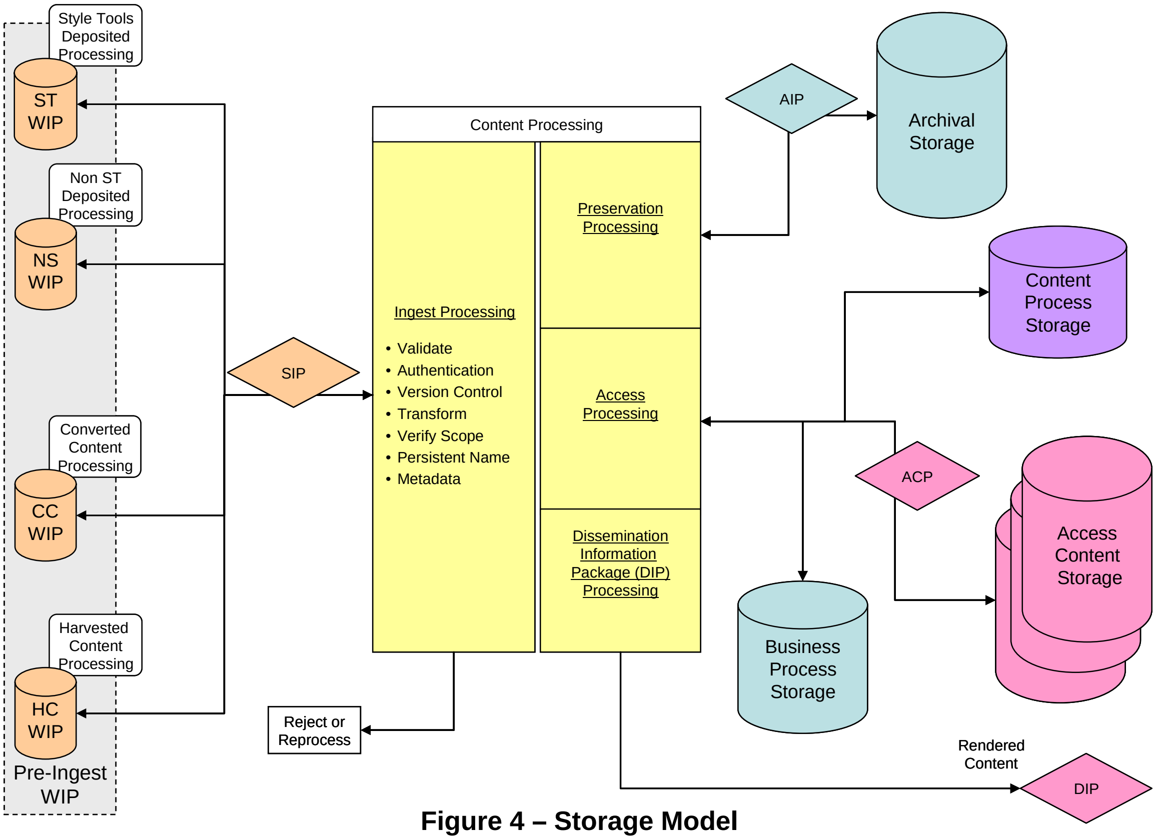

Figure 4 – Storage Model

To meet the challenges of today and the future, the system should be able to:

- Accept the transfer of content in a wide variety of formats as they were created or stored by their creators and the flexibility to easily adapt to future file formats;
- Ingest, preserve, and provide access to that content;
- Store content in a manner that is independent of any particular hardware and software component over long periods of time;
- Scale in order to store and preserve content based on the predicted digitizing of existing hard copy publications and the discovery and harvest of in scope Federal content from Web sites;
- Provide access to the content in electronic form for all users based on established user rights and privileges, thus ensuring that the system users are able to access all of the content that they are entitled to see;
- Provide access to the content in a manner that is consistent with current technology and the changing expectations of its diverse user communities;
- Adapt to changing technology in order to continue to provide access to and delivery of content desired by the user community; and
- Identify the essential characteristics of the content that is being preserved for the purposes of authentication and certification.

The proposed GPO system should provide the following capabilities in support of GPO content management lifecycle processes.

- Provide end-to-end automated work processes that streamline the content management lifecycle processes for all content;
- Manage the creation, review, and approval of content;
- Support the transfer process of all content (electronic and non-electronic) to GPO, FDLP, and other repositories;
- Support the Preservation Services;
- Ensure that content contained as part of service orders/requests, sales contracts, and/or other agreements that identify content that is to be transferred to GPO, specify the terms and conditions of such transfers that conform to GPO and other Federal standards and requirements as required;
- Support end-to-end tracking of all content during the process of transfer, maintenance in FDLP, processing, preservation, and continuing use;
- Accept transfers of content, check that the content conforms to terms and conditions of the service order specified transfer, and store them in the system;
- Ensure that the content transferred to GPO remains free from corruption and is accessible as GPO undergoes changes in IT;
- Support the description of content held by GPO so that it is clearly identified, discoverable, and retrievable;
- An automated tool must exist for any internal and external user to inform GPO of publications they become aware of in the future;
- Dispose of certain content (e.g., content out of scope for permanent preservation, or in-process work files) as stipulated by the service order or other agreement;
- Manage access rights;
- Provide access to electronic content;

- Output authentic and certified copies of the content;
- Output copies of the content as specified by customers;
- Monitor system performance;
- Maintain system security; and
- Provide audit trails of system activity.

2.1 Major System Conditions

A list of general high-level Conditions:

Anonymous default end user access
Responsiveness to User needs
System flexibility
System scalability
System interoperability
Support of legacy processes (e.g., Oracle, PKI, ILS, Microcomp)
Standards compliance

2.3 Major System Constraints

A list of general high-level Constraints follows:

Interface to Oracle (backend systems)
Oracle implementation schedule (2009)
Target implementation schedule
Funding/Timeline/Business Plan (cost)
Statute (e.g., accessibility, etc.) and regulations
No disruption of services
Standards bodies (existing)
Standards bodies (future)
Resources/workforce
Converted content condition
System security
Privacy
Multiple sites (preservation)
Legacy interfaces to content originators
Content originator practices and requirements related to content presentation and style (e.g., Agency style guides)
OMB's Federal Enterprise Architecture
Federal Agency Partner Work (NDIIP, ERA) on Content Packages

2.4 User Characteristics

A user can be defined as anyone who will interact with the system and are shown in Figure 5 – User Classes. A user class is determined by the ways in which the user interacts with the system.

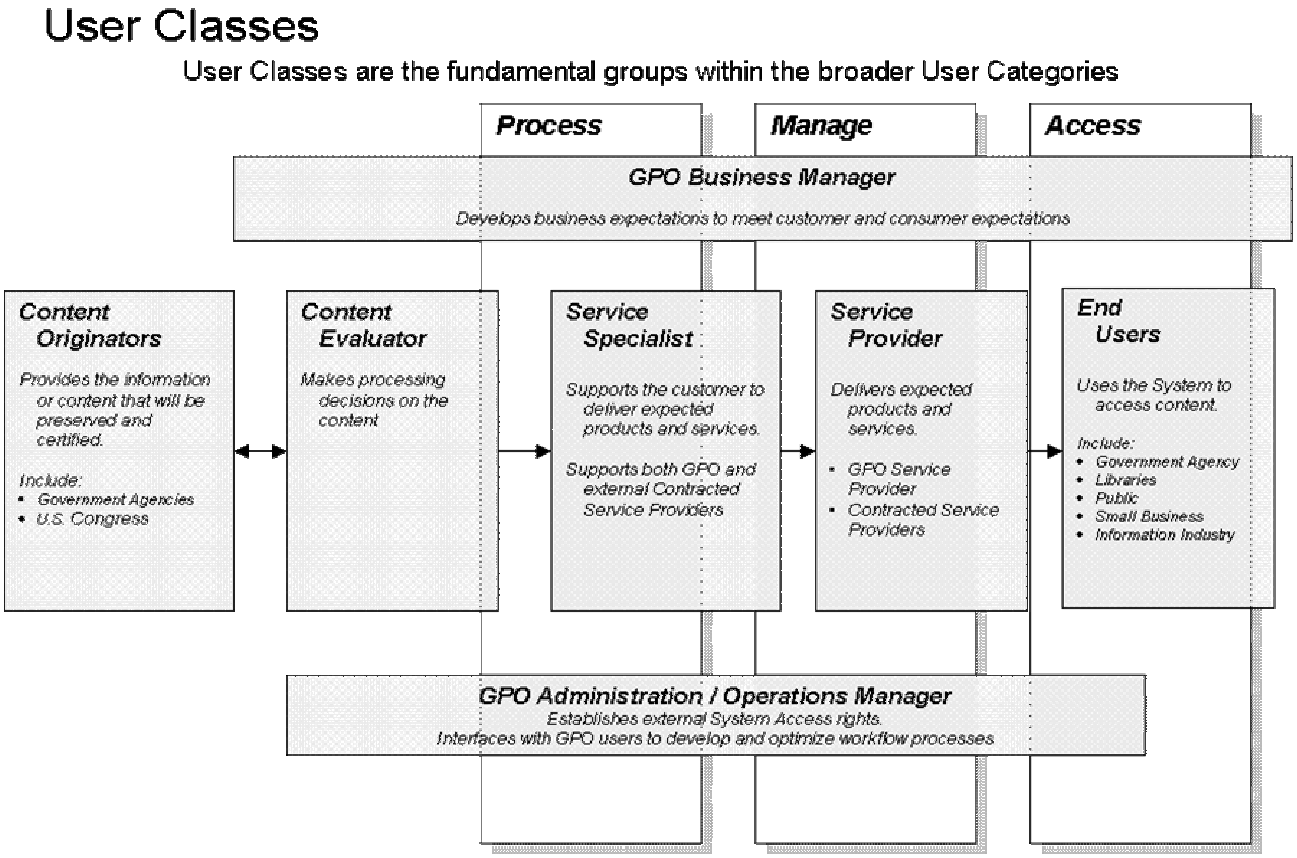
User Classes
User Classes are the fundamental groups within the broader User Categories
Process
Manage
Access
GPO Business Manager
Develops business expectations to meet customer and consumer expectations
Content Originators
Provides the information or content that will be preserved and certified.
Include:
• Government Agencies
• U.S. Congress
Content Evaluator
Makes processing decisions on the content
Service Specialist
Supports the customer to deliver expected products and services.
Supports both GPO and external Contracted Service Providers
Service Provider
Delivers expected products and services.
• GPO Service Provider
• Contracted Service Providers
End Users
Uses the System to access content.
Include:
• Government Agency
• Libraries
• Public
• Small Business
• Information Industry
GPO Administration / Operations Manager
Establishes external System Access rights.
Interfaces with GPO users to develop and optimize workflow processes

Figure 5 – User Classes

The major user classes identified for the system include:

- Content Originator – Develops information and content and generates requests for GPO services. The Content Originator works with the Content Evaluator to define the parameters of the Preservation and Dissemination Plan. Content Originator provides the content that will be transferred to the system for subsequent certification and preservation.

- Content Evaluator – Collaborates with the Content Originator to determine the content and if the content is in scope or not. The Content Evaluator establishes/defines the Preservation and Dissemination Plan and determines/makes decisions on what processing will occur, whether to use internal production or external contracting, and whether to include information in the Sales Program and/or FDLP.

- Service Specialist – Supports the customer and is expected to deliver the products and services as determined. The Service Specialist performs contracting, administrative, and preservation functions (e.g., creative services, contract writing and awarding, billing, quality control, cataloguing and indexing, preservation management, and dispute resolution.) The Service Specialist helps to describe the content and is involved with the creation of metadata and uses the system to preserve the content as required.

- Service Provider – The Service Provider delivers the expected services and products after receiving notifications. The Service Provider accepts print orders as an example and also certifies vendors as GPO vendors.

- Business Manager – Develop business expectations to meet Content Originator and End User expectations. Also works with GPO Sales Group to repurpose data in order to provide value added services.

- Systems Administration/Operations Manager – Systems Administration directly supports the overall operations and integrity of the system and its use and conducts such system activities as managing user access rights, monitoring system performance, and scheduling reports. The Operations Manager interfaces with GPO personnel and makes decisions, including approval of workflow processes. The Operations Manager reviews system recommendations and makes decisions on when and how lifecycle activities related to specific records occur and who will perform the work. The Operations Manager has ultimate responsibility for the completion of tasks and the quality of the products.

- End User – Uses the system to search for and access records, to submit data requests, request assistance via mediated searches, communicate with GPO, and invoke system services.

2.5 Operational Scenarios

The *Future Digital System* requirements document expresses what users want and envision in the proposed system. Scenarios convey these needs in simple non-technical language. Overlap occurs between different scenarios as a result of interaction between different users or due to similarity between different activities. All of the scenarios represented in the following sections describe one example of how users may interact with the system. Scenarios have purposely been made to be far reaching in an attempt to include all possible actors within a designated class (of users), but the scenarios are not intended to identify all possible situations for any given user class. Additionally, the steps in the scenarios should not be interpreted as a fixed sequence of events; instead they should be interpreted as an illustration of capabilities the system will offer (any user class).

A scenario is a step-by-step description of how the system should operate and interact with both its users and external interfaces under a given set of circumstances. Scenarios are described in a manner that enables readers to walk through them and gain an understanding of how all the principal parts of the system function and interact. The scenarios tie together all parts of the system, the users, and other entities by describing how they interact. Scenarios cover the user's concept of all the operational modes and all classes of users identified for the proposed system and illustrate all the business processes that the system will support.

2.5.1 Content Originator Scenario

Content originators are comprised of executive or judicial employees primarily consisting of authors, editors, and/or publication creators (Agency Customer*)*, and legislative or congressional employees who manage the information assets of the Congress (Congressional Customer). Content Originators are responsible for making content available to GPO for certification, preservation and dissemination. In some cases, content is created without using the Future Digital System, and/or without the knowledge of GPO, in those cases, the Content Evaluator may make the decision to use harvesting tools to begin the ingest of that content.

Content Creation

- Content Originator develops/creates content.
- Content Originator generates and submits order requesting GPO services.
- The system provides ingest aides for content creation, creative services, content management, and content validation, as applicable.
- Content Originator develops content and initiates workflow through an the system ingest aid that includes best practices guidelines for the creation and submission of the Content Package.
- Content Originator collaborates with GPO through the system to provide preprocessing information and specifications.
- Content Originator coordinates with Content Evaluator on the content service orders and the Preservation and Dissemination Plan and makes them available to Service Specialists and Service Providers.
- When GPO content creation services are fee-bearing, the system interfaces with the fee management system to determine fees and charge the Content Originator.

Content Validation and Ingest

- For deposited content ingest, text and/or other information is captured, managed, provided creative services as appropriate, and validated before the ingest toolset creates the SIP according to GPO-established best practices.
- For converted content ingest, converted content is made available, then is captured, managed, and validated before the ingest toolset creates the SIP according to GPO-established best practices.
- For harvested content ingest, content is harvested, then is then is captured, managed, and validated before the ingest toolset creates the SIP according to GPO-established best practices.

2.5.2 Content Evaluator Scenario

The Content Evaluator may work with the Content Originator to assist in content development and determines what processing occurs. Once the content is made available to GPO, the Content Evaluator makes decisions regarding scope and preservation of content. The Content Evaluator may also use tools to coordinate harvesting and format conversion of content. Service orders are pushed to Service Providers by the Content Evaluator.

Preprocessing of Content

- When requested, uses the system and the system tools to work with Content Originators to develop content that conforms to GPO standards.

Version, Scope, and Certification

- Determines if content is within the scope of GPO.
- The Content Evaluator then determines if the document is in scope for GPO Dissemination Program. Working with a Business Manager determines if the document is in scope for the sales program. An example of GPO dissemination program is the FDLP.
- The Content Evaluator uses the system to request certified content from the Service Specialist.
- The Content Evaluator determines if the content is new or a version of previously delivered content and confirms this with the Content Originator as appropriate.
- The system applies storage management rules as appropriate for the content.
- The system maintains audit trails that document the location of the material.
- Based on scope and input from Content Originators, the Content Evaluator uses the system to develop the Preservation and Dissemination Plan.

Harvesting and Format conversion

- The Content Evaluator uses the system locating tools to locate content that is within scope.
- When content is located, coordinates the harvesting by either using harvesting tools or creating a service order for Service Providers to use the harvesting tools to gather the content and its related metadata.
- Content is packaged for ingest into the system.
- As required by an Operations Manager or by business rules, the Content Evaluator sends service orders to Service Providers to use the system tools to digitize existing tangible content. When digitization is complete the Content Evaluator packages that content for ingest.

Service Ordering

- The Content Evaluator determines if the service should be done by GPO or by an external Service Provider.
- Service orders are sent to the Service Provider.

2.5.3 Service Specialist Scenario

After content arrives in the system and the Content Evaluator has determined its preservation status, the Service Specialist performs the following actions as needed to perform preservation tasks on content for as long as necessary.

Provides Special Services

- Uses the system to work with Content Originators to track and resolve disputes with Service Providers.
- Works with Content Originators to assist in content creation by providing expert advice.
- Works with Business Managers to repurpose content. This includes repackaging of content for new business needs, such as determining what digital content should be made available in hardcopy. For those documents that should be made available in hardcopy, a service order is sent to the Service Provider.

Metadata development

- The system populates initial metadata information package (e.g., bibliographic record) for the content. The Service Specialist confirms or updates that catalogue and index entry.
- If this is a version of existing content, the system documents the necessary relationships between this version and previous ones.
- The Service Specialist reviews that metadata and updates it appropriately.
- The system performs conformity checking to ensure that metadata has been recorded, and meets appropriate standards.

Preservation Processing

- When content arrives in the system, and after a preservation and dissemination plan has been established, the system executes any preservation processing required by that plan.

- The Service Specialist uses the system to review the original content and the processing applied to them to determine if preservation objectives are being achieved effectively and consistently.

- When problems occur in executing a preservation and service plan, the Service Specialist determines whether the exceptions should be accepted and documented "as is." Alternatively, the Service Specialist works with the Content Evaluator or Content Originator to determine appropriate corrective action or to modify the Preservation and Dissemination Plan. The system maintains an audit trail of activity.

- The Service Specialist ensures that the system captures and retains information about the digital content necessary to ensure its preservation, accessibility, and to certify whether it's authentic and/or official. The system will provide appropriate tools, techniques, and methods to enable faithful reproduction of all digital content in the system.

- When new content has been preserved, electronic versions will be available to the depository libraries through the system.

Content Maintenance

- The Service Specialist uses the system to examine samples of digital content being preserved to ensure that nothing is lost or corrupted in storage. In the event of corrupted content (e.g. either due to media degradation or media migration problems), the Service Specialist uses the system tools to assist in the recovery of the content.

- The Service Specialist works with administrative users to ensure that necessary changes, such as media migration, are implemented in the storage system. The Service Specialist reviews plans for, monitors, and evaluates updates or modifications of the storage system, including migration of digital content to new digital media.

Creation of the Collection of Last Resort

The system directs content to the appropriate storage location.

2.5.4 Service Provider Scenario

Service providers provide the system with their capabilities and pricing information, receive notification of service orders, accept service orders, and provide services.

Service Capability Update

- The Service Provider updates the system with their capabilities.
- The Service Provider updates the system with pricing information.

Providing Service

- For each service order, the Service Provider receives notification that an order is coming.
- External providers use the system to accept or deny orders and to provide quotations. When possible, the system provides quotations automatically to the service requestor based on capability and pricing information already available within the system.
- The system notifies Service Providers when jobs are ready for initiation.
- The system tracks the progress of orders and their completion.
- The Service Provider performs the service and notifies the system of status and completion.

2.5.5 Business Manager Scenario

The Business Manager is responsible for determining what content might be made available for sale and setting pricing levels for GPO services.

Repurposing Content

- Based on knowledge of content, the system provided data on content usage, and other business information, the Business Manager decides what content should be made available for sale. This may involve repurposing various content into documents or publications that will be made available for sale. It may also involve making non-tangible content into tangible publications.
- When a decision is made to make new content available, the Business Manager collaborates with the Service Specialist (via the system) to determine how to repurpose the content.

Set Pricing Levels

- Based on business knowledge and the system data, the Business Manager uses the system tools to set pricing levels for GPO services and products.

2.5.6 Administration/Operations Manager Scenario

Administration/Operations Manager users handle such activities as assigning user rights and privileges, scheduling reports, monitoring the system, modifying workflow, and ensuring system availability. This scenario is included to demonstrate some of the capabilities that would be included in the system for the administrative user of the system as well as the Operations Manager of the system. Not all capabilities are described in the scenario and many of the system functions will be done without user involvement.

Assign user rights and privileges

- Using GPO predefined roles (which includes information regarding permissions granted and job roles), the administrative user creates the user account establishing requested access rights and privileges in the system (i.e., user profile is created). The user is granted appropriate access rights (e.g., access to data that may be restricted by certain access privileges or administrative access) and systems capabilities (e.g., ability to edit, input data, check security, produce user reports). Note that not all users will require accounts.

Schedule Reports

- This user logs on to the system and uses any data available in the system to create new reports or modify existing reports. The request for reports could be based on a specific requirement from GPO or from a system monitoring need. The reports could provide metric data for such activities as system usage, system capacity, performance, and workflow statistics.
- The reports are scheduled for regular distribution to the appropriate people or are created on as needed basis.

Monitor System

- The system provides this user with the ability to monitor system performance and security using system tools. These tools provide for monitoring storage, performance, space, load, security-related indicators, etc.
- This user, with help from support staff, diagnoses and troubleshoots problems implementing intrusion detection systems and virus control procedures. In parallel, the system is recording these events in system logs and establishing an audit trail.
- Once the problem has been corrected the user ensures that the system's operations are secure from intrusion, viruses, unauthorized access, etc.

Modify Workflow

- In some instances this user will be able to modify workflow. The user will be able to modify work flowing through the system at a point in time when problems within the system arise.
- When this user is alerted to a potential problem within the system (e.g., a problem with a server has occurred), the user notifies the appropriate support staff who diagnoses and troubleshoots the problem, and temporarily modifies system workflow(s) to ensure continued service.
- This user notifies the appropriate operation of the temporary modification to workflow. The user tracks the resolution of the problem for audit trail purposes and the modified system workflow(s) will exist in the system until the problem can be corrected.
- When notified by the system that identified steps are not occurring as scheduled, this user has the capability to examine the system in an attempt to understand and/or determine the nature of the problem. Possible problems could be related to bottlenecks in the system or due to inability of the Content Evaluator, Service Specialist or Service Providers to complete tasks.
- This user may recommend possible solutions (if due to a bottleneck in the system) or interface with GPO staff to determine the nature of the problem and recommend solutions.
- This user has the authority to implement an agreed upon solution in order for the tasks to continue.

Job Pending

- This user logs onto the system and receives a notification from the system that a specific task is ready to be performed. The system, using predefined GPO business process rules is able to determine what activities need to occur. Based on these rules, the system can decide to create a task, assign tasks to staff, assign due dates, and provide relevant information about the task.

Review System Assignments

- This user reviews the assignments identified by the system and selects from the options that are presented:

  - Confirm Assignments
    - Upon confirmation the system notifies staff of their assignments including milestones and begins to track the task, which includes capturing performance statistics.
    - As the task proceeds, the system is able to send notifications, collect approvals, detect when processing has been suspended, make additional assignments, or notify this user that the job is complete.
  - Modify Assignments
    - Upon inspection of the task, the manager has the capability to modify the steps, adding or removing steps, or changing the order of the steps to be performed to process the job as a candidate workflow.
    - The system will either confirm the modification or may determine that additional steps are necessary requiring this user to make additional modifications.
    - Upon approval, notifications are sent to staff alerting them of their assignments.

Approval and Closure of Tasks

- As the task progresses through the system, there are various junctures when approval may be required by this user. The manager will inspect tasks on a periodic basis and provide approval as appropriate, including final approval that the job has successfully been completed.
- Upon final approval, the system captures this information and stops tracking the job.

2.5.7 End User Scenario

The End User will undertake the following steps in using the system to obtain content. (The steps listed below should not necessarily be interpreted as a sequence of events.)

Search

- All End Users will have the ability to search for and access content within the system. Access to content may be dependent on End User rights and privileges.
- The End User searches descriptive metadata and/or content within documents. Within the End User’s given access rights and privileges, the End User may use available functions and features. The system provides the capability for the End User to view and/or sort the results of the search, modify the search, and refine or save search results. If needed the user may interact with GPO to receive help.

Retrieve/Receive Content

- From search results that identify relevant content, the system allows the End User to view and access available content. The End User may request the system to deliver content to an available medium.
- If content is located that is not available electronically, the system provides the End User with bibliographic and location information, and options for accessing the tangible content.

Assisted Access

- The End User may request help from GPO while using the system. Assisted access may include such activities as answering questions, conducting and handling searches, processing special requests, expediting requests, and similar issues. This may also include online help tools or referrals to libraries, etc. the system tracks the communication and information about the Assisted Access. Some of these services may involve fees.

Fee for Service

- End users may request products or services that require them to pay a fee. If a fee must be collected, the system tracks, reports upon, and routes any required financial transaction information to all appropriate billing/accounting systems, and provides the requested product or service on authorization by the billing/accounting system.

2.5.8 Authentication Scenario

GPO receives digital content for deposit already authenticated by the content originator.

1. SIP is ingested with integrity mark from CO (thousands per day)
2. AIP and ACP created by ingest. (thousands created per day)
3. Existing authentication is detected, verified and passed on to AIP and ACP if possible.
   a. If authentication cannot be verified, a decision must be made on how it is further processed.
4. AIP and ACP are authenticated by GPO.
   a. The AIP and ACP will be certified as official and authentic (as required).
   b. GPO will re-authenticate content that has already been authenticated by the content originator.
   c. Certification will produce an integrity mark that includes a GPO integrity mark and a digital certificate.
   d. Authentication information already available from the content originator will be retained and will be referenced in the metadata.
5. DIP created from ACP (millions per day)
   a. Integrity mark is passed on to DIP
   b. The GPO integrity mark may be displayed on the DIP--visible or invisible dependent upon business rules.

2.5.9 Content Rejected at Ingest Scenario

Content in the form of a SIP is provided to the Ingest function and is subsequently rejected. As a result, the content cannot be processed into ACP, AIP or DIP.

Activities that need to take place:

1. Workflow provides the SIP to the Ingest Processor. (thousands per day)
2. The Ingest Processor determines that the SIP cannot be processed and why.
3. System provides notification to Content Evaluator that content has been rejected.
4. Content Evaluator determines next steps
    a. Deposited content: contact with CO for GPO or CO to resolve the problem.
    b. Converted content: contact with Service Provider for GPO or Service Provider to resolve the problem.
    c. Harvested content: contact with Service Provider for GPO or Service Provider to resolve the problem.
5. Rejected content is:
    a. Fixed by GPO
    b. Fixed or replaced by CO
    c. Fixed or replaced by Service Providers
6. Content is re-submitted to Ingest Processor.

2.5.10 End User Access Scenarios

Background: All End Users will have the option to be authenticated (e.g., security log-in) so that they can customize Access tools. Anonymous Public End Users will have access to default Access tools (Interface, Search, Reference Tools, and Request/Delivery options) as defined by GPO business rules.

Note: Currently 37M web views and downloads per month on GPO Access.

Scenario: Anonymous Public End User Access Scenario.

1. User access to system (greater than 1M/day)
2. User not Authenticated
3. System provides a default Interface containing default Search, Reference Tools, Request/Delivery options.
4. Public End User submits a query against ACPs.
5. System returns relevant results and available Request/Delivery options to Public End User.
6. A decision is made by the Public End User: Is this what I want?
    a. If yes, process Request.
    b. If no, the Public End User may restate or refine query until satisfactory results are obtained or query is abandoned.
7. Public End User requests Delivery of selected information.
8. System creates DIP from ACP and delivers DIP to Public End User.

Scenario: Authenticated Public End User Access Scenario.

1. User access to system (greater than 1M/day)
2. User Authenticated
3. System provides an Interface that allows user to customize Search, Reference Tools, Request/Delivery options.
4. Public End User submits a query against ACPs.
5. System returns relevant results and available Request/Delivery options to Public End User.

6. A decision is made by the Public End User: Is this what I want?
   a. If yes, process Request.
   b. If no, the Public End User may restate or refine query until satisfactory results are obtained or query is abandoned.
7. Public End User requests Delivery of selected information.

2.5.11 Hard Copy, End User Scenario

1. A public End User accesses the system via a default interface.
2. Default tools used to search and request delivery (including User credentialing) of 4 hard copies of a publication.
3. System determines the most effective method of output (in this case, POD).
4. DIP is created.
5. System selects Service Providers based on user input (e.g., user location, vendor capability).
6. System notifies Service Provider of job.
7. System allows Service Provider access to the DIP, or pushes the DIP to the Service Provider.
8. Job progress is tracked.
9. The order is fulfilled as requested.
10. Notification of fulfillment is provided to GPO and user

2.5.12 Electronic Presentation, End User Scenario

1. A public End User accesses the system via a default interface.
2. Default tools used to search and request a publication.
3. ACP is retrieved.
4. DIP is delivered to End User.

2.5.13 Hard Copy Quality Complaint, Content Originator Scenario

1. Hard copy output of a publication is deemed unacceptable to the Content Originator.
2. The Content Originator completes an electronic complaint form and submits it electronically to GPO.
3. Form is routed to the appropriate department and assigned to a Service Specialist.
4. Service Specialist analyzes the DIP provided to Service Provider to respolve complaint.
5. Service Specialist may request printed copies for evaluation.
6. Service Specialist communicates with Content Originator and Service Provider to resolve complaint.
7. Service Specialist may edit the Service Provider's information to indicate non-compliance, revise equipment and capabilities, etc.
8. Notification is electronically submitted to the Service Provider if the Service Specialist makes changes to their profile.
9. Service Specialist's evaluation and notification of complaint resolution is electronically submitted to the Content Originator (and Service Provider, if applicable).
10. If a reprint is required, DIP is provided to a Service Provider.
11. Job progress is tracked.

12. Service Specialist checks with Content Originator to ensure acceptability of reprinted product.

2.5.14 Preservation Process Scenario (Migration)

Assumptions: Content free of proprietary restrictions, successfully ingested into the FDSys

1. Ingest produces AIP
2. AIP is stored
3. AIP is kept refreshed
4. AIP is selected for preservation process from archival store
5. Content object is transformed from its stored form to the new, migrated form in content processing
6. Metadata is updated to record the transformation
7. New ACP is generated as needed
8. AIP is returned to archival store

2.5.15 Preservation Process Scenario (Emulation)

Assumptions: Content free of proprietary restrictions, fully self-describing, and successfully ingested into FDSys

1. Ingest produces AIP
2. AIP is stored
3. AIP is kept refreshed
4. FDSys registry of viable formats indicates that AIP exists in a no-longer-supported format
5. ACP is generated based on emulation of functionality derived from metadata

2.5.16 Style Tools Scenario

A content originator will use Style Tools in order to create and subsequently provide content to the system. (The steps listed below should not necessarily be interpreted as a sequence of events.)

Capture

- All Content Originators will have the ability to provide content to and/or create content within the system.

Compose

- The system will ensure that content adheres to appropriate guidelines and/or standards for aesthetics, layout and other key determining characteristics.
- The Content Originator uses the system to edit, re-work and finalize content.
- The Content Originator may use available functions and features to search for additional possible content or previously stored elements of related content.

Collaborate

- The Content Originator may designate other Content Originators as project collaborators.

- These content collaborators will be given access rights as necessary, with full functionality being an available option. Collaborators will have the capability to contribute and/or create content, edit content and change content presentation.

Approval

- Prior to ingest into the system, an authorized user must approve the content. This may include various levels of approval. Including, but not limited to the content itself, and content presentation. Approvals are typically from the same agency as the Content Originator.

Other Uses

- The system may be made available to other system users who have the need to compose and create unique aggregations of content. This may include end users who have searched for and compiled multiples segments of independent content and who want this independent content made into a single delivered package (e.g., a custom book made from segments of different books).

Sequence

1. The CO creates 100 pages of content including digital objects - e.g. photos, charts and graphs (200 per day)
2. A unique ID is created for each granular piece of content as well as all digital objects (40,000 per day)
3. Content and digital objects are stored within the system (1 terabyte per day)
4. The CO and collaborators search for additional content and digital objects within the system from prior content submissions as well as content submitted by different originating agencies (10,000 digital objects per day)
5. The CO and collaborators include that content within this unique project (2,000 per day)
6. CO and collaborators edit and re-work the content using design guides designated by the originating agency or GPO (four month process, 800 users working daily)
7. CO content approval is granted by an authorized user (200 per day)
8. A SIP is created and ingested (200 per day)

2.5.17 Harvesting Scenario

1. Harvester is targeted to locate publications on Federal Agency Web site
2. Harvester locates a publication
3. Harvester uses business rules to determine whether the publication is in-scope for GPO dissemination programs
4. Harvester gathers the digital object and metadata (including integrity marks, if available)
5. Harvested content is processed in WIP storage to form a DIP
6. SIP is submitted to ingest
7. SIP is validated
8. Scope is verified
9. Dissemination plan created
10. Content is authenticated
11. Authentication function determines how existing integrity marks should be used, if they are present
12. Content is versioned (based on any version information provided in the harvested metadata or content)
13. Metadata is updated

14. Content is transformed into an access content package (ACP) and archival information package (AIP)
15. Unique ID is assigned
16. Persistent name is determined and assigned

3.0 Requirements

3.1 *Assumptions and Constraints*

3.1.1 Assumptions

The following form the assumptions as currently known for the Future Digital System.

1. GPO will evolve into a Content Originator (a publisher) in addition to its historic role as a Service Provider.

    a. GPO will repurpose and repackage content to create new versions for its dissemination and access programs.

2. Deposited or born digital content will be the primary method of ingest. Conversion of documents is expected to be a transitional activity. Furthermore, Harvesting will continue to be available as required.

3. Agency customers will have more direct control over buying and publishing information products and services. For example, direct electronic ordering for any good or service.

4. GPO will collect and preserve in scope content of the Federal Government for public access.

    a. GPO will amass a comprehensive collection of Government publications from all three branches of Government.
    b. GPO will provide access to that content in a variety of forms and formats.
    c. GPO will preserve that content for access over time.
    d. GPO will receive that content in a variety of forms and formats.

5. The information that flows through GPO can be systematically evaluated and determinations about inclusion can be made by the system. If process and scope are properly identified and defined, a system can be built to make the inclusion/no inclusion determination.

6. Repurposing content for specific user groups (e.g., small business) or markets is a potential new revenue opportunity for GPO. Content granularity will be a key component of repurposing content.

7. Capturing content is essential to the success of the system.

   a. Missing content (known as fugitive documents for hard copy output) can be minimized, if GPO provides effective toolsets that aid in capturing content.
   b. Capturing all content will give GPO the richest collection possible.

8. The system will process all GPO work, including work that has no preservation or access value provided it meets agency business needs.

9. System concept should not be constrained by statutory limitations.

10. The volume of print will continue to decline.

11. Digital Media will still be required as an output vehicle for delivering content.

12. .The system will address usability and accessibility requirements and best practices.

13. Storage Management will adhere to best practices for data management.

14. The system must be flexible, extensible, and adaptable.

15. Tools and processes may include human interactions into the foreseeable future.

16. User requirements regarding specific needs for content ingest are not identified. GPO must be able to interface with various agency level content management systems (CMSs), manual processing of orders, etc.

17. GPO must create best practices for Content Ingest into the system and update GPO Style Manual.

18. Customer confidence with GPO administering and managing the agencies content. The system must demonstrate leadership in accepting and managing content to build customer confidence.

3.1.2 System Attribute Assumptions

The following form the assumptions as that will define the system aspects of Future Digital System (These aspects will defined in the next release of the RD):

- Physical
  - Construction
  - Durability
  - Adaptability
  - Environmental Concerns
- System Performance Characteristics
- System Security
- System Operations
  - System Human Factors
  - System Maintainability

  - System Reliability
- Policy and Regulation
- System Sustainment

3.1.1 System Interfaces

FDsys will be capable of interfacing with other applications and systems throughout the Federal Government..

FDsys will provide access to Users.

Interfaces to FDsys will be accommodated including legacy system (as they are updated or replaced) and Oracle.

3.2 Requirements List

The requirements listed in this section are the result of a thorough analysis of the ideas proposed in the *Future Digital System ConOps.* The requirements are organized by system capability in the same order as in the *ConOps* Section 5.3: Description of Proposed System. This RD should be reviewed together with the *ConOps* for a complete understanding of the proposed system.

The requirements are grouped into the major system capabilities discussed previously. There are several levels of system requirements in each major system capability. Each subsection is displayed in a table containing the properties and attributes of individual requirements.

The requirements were developed in compliance with IEEE Standard 1233-1998 and feature the following properties:

- Capability: feature or function of the system needed or desired by the customer;
- Condition: measurable qualitative or quantitative attributes and characteristics that are stipulated for a capability;

At this time, not all requirements are final and some properties such as specifications and testable conditions must be developed before the acquisition process begins. Such requirements are so noted.

Within each subsection, the requirements are ordered by the alphanumeric ID code assigned during the requirements development process. Many subsections are hierarchical in nature; these relationships are reflected in the ID codes. Frequently, a higher-level requirement refers to a lower-level requirement as a condition.

Each requirement also features the attributes of Criticality.

- Criticality (1, 2 or 3): how essential the requirement is to the operation of the system.

3.2.1 System Overarch (SYS 1.0)

ID	Criticality	Capability	Spec. Required
SYS 1.1	1	The system must provide for the use of open Interfaces	
SYS 1.2	1	The system shall employ interoperable programming interfaces which are compliant with open standards, including, but not limited to, Extensible Markup Language (XML)	Yes
SYS 1.3	1	The system shall have the ability to manage files expressed in interfaces which are compliant with open standards (including but not limited to XML)	Yes
SYS 1.4	2	The system shall have the capability to apply GPO Quality Assurance standards (to be developed).	Yes
SYS 1.5	1	The system shall have the capability to communicate with back office applications (e.g., finance, inventory).	
SYS 1.6	1	The system shall have the capability to replicate content for transfer to an alternate location (e.g. based on National Archives specifications)	

3.2.2 Digital Standards

3.2.2.1 Preservation Standards - SIP (STD 1.0)

ID	Criticality	Capability	Spec. Required
STD 1.1	1	SIP - Deposited Content	
STD 1.1.1	1	The SIP Deposited Object shall consist of the Digital Object	

STD 1.1.2	1	Metadata in the SIP shall consist of fundamental representation information, any necessary DTD's or style sheets, and the GPO submission level of descriptive metadata (as applicable): Unique ID; Title/Caption; Author/Creator; Publisher/Authority; Rights Owner; Version Info; Relationship; Provenance; Structural Information; Format, environment, file type; Packaging Info; Hardware/Software environment; Administrative Info (intended output, billing/payment, contacts); Preservation Processes/Events; Dates in Life-Cycle.	
STD 1.2	1	SIP - Harvested Content	
STD 1.2.1	1	The SIP Harvested Object shall consist of Digital object as harvested	
STD 1.2.2	1	The SIP Harvested Metadata shall consist of representation information and documentation of harvest & transformation(s); GPO submission level	
STD 1.3	1	SIP - Converted Content	
STD 1.3.1	1	The SIP Converted Object shall consist of digital object as obtained by scanning or other method, without compression or other modification.	
STD 1.3.2	1	The SIP Converted Metadata shall include full technical information on the conversion, using NISO Z 39.87-2002 as a guideline, in addition to the submission level descriptive metadata.	Yes

3.2.2.2 Preservation Standards - ACP (STD 2.0)

ID	Criticality	Capability	Spec. Required
STD 2.1	1	ACP - Deposited Content	
STD 2.1.1	1	The ACP Deposited Object shall consist of Digital object in XML	
STD 2.1.2	1	The ACP Deposited Metadata shall consist of SIP metadata + Descriptive metadata, packaging metadata, for access, content transformation, content management, derivation, etc	Yes
STD 2.2	1	ACP - Harvested Content	
STD 2.2.1	1	The ACP Harvested Object shall consist of Digital object as harvested and file(s) as converted to XML	
STD 2.2.2	1	The ACP Harvested Metadata shall consist of SIP metadata + Descriptive metadata, packaging metadata, for access, content transformation, content management, derivation, etc	
STD 2.3	1	ACP - Converted Content	
STD 2.3.1	1	The ACP Converted Object shall consist of Files created from converted object and/or other derivatives intended for access (e.g. text, JPEG)	Yes
STD 2.3.2	1	The ACP Converted Metadata shall consist of GPO submission level + metadata for access, content transformation, content management, derivation, etc	Yes

3.2.2.3 Archival Information Package - AIP (STD 3.0)

ID	Criticality	Capability	Spec. Required
STD 3.1	1	AIP - Deposited Content	
STD 3.1.1	1	The AIP Deposited Object shall consist of Digital object in XML	
STD 3.1.2	1	The AIP Deposited Metadata shall consist of SIP Metadata + PDI for deposited content	Yes
STD 3.2	1	AIP - Harvested Content	
STD 3.2.1	1	The AIP Harvested Object shall consist of Digital object as harvested and file(s) as converted to XML	
STD 3.2.2	1	The AIP Harvested Metadata shall consist of ACP Metadata + PDI for harvested content	
STD 3.3	1	AIP - Converted Content	
STD 3.3.1	1	The AIP Converted Object shall consist of digital object as obtained by scanning or other method, without compression or other modification.	Yes
STD 3.3.2	1	The AIP Converted Metadata shall consist of SIP + PDI for converted content	Yes

3.2.2.4 Preservation Standards - DIP (STD 4.0)

ID	Criticality	Capability	Spec. Required
STD 4.1	1	DIP - Deposited Content	
STD 4.1.1	1	The DIP Deposited Object in the DIP shall consist of a faithful copy of the digital object in the ACP, rendered for dissemination	

STD 4.1.2	1	The Deposited Object metadata in the DIP shall consist of all relevant ACP metadata plus additional descriptive and packaging information to facilitate access and dissemination (e.g., bibliographic description)	
STD 4.2	1	DIP Harvested Object	
STD 4.2.1	1	The Harvested Object in the DIP shall consist of a faithful copy of the converted object in the ACP, rendered for dissemination	
STD 4.2.2	1	The Harvested Object metadata in the DIP shall consist of all relevant ACP metadata plus additional descriptive and packaging information to facilitate access and dissemination (e.g., bibliographic description)	
STD 4.3	1	DIP - Converted Object	
STD 4.3.1	1	The Converted Object in the DIP shall consist of a faithful copy of the files archived from the digital object, rendered for dissemination	
STD 4.3.2	1	The Converted Object metadata in the DIP shall consist of all relevant ACP metadata plus additional descriptive and packaging information to facilitate access and dissemination (e.g., bibliographic description)	Yes

3.2.3 Metadata

3.2.3.1 Metadata - Types (MET 1.0)

ID	Criticality	Capability	Spec. Required
MET 1.1	1	The system shall employ metadata which captures representation and technical information related to the target digital object	

MET 1.2	1	The system shall employ metadata which relates the structure of the target digital object	
MET 1.3	1	The system shall employ metadata which relates the context of the target digital object and relationship to other objects	
MET 1.4	1	The system shall employ metadata which relates the provenance, fixity, and authority (ie.: official, certified, etc) of the digital object and its associated content packages	
MET 1.5	1	The system shall employ metadata which describes and provides reference information about the digital object and its associated content packages	
MET 1.6	1	The system shall employ metadata which describes administrative processes or conditions (e.g., Business Process Information)	

3.2.3.2 Metadata - Core Capabilities (MET 2.0)

ID	Criticality	Capability	Spec. Required
MET 2.1	1	The system shall have a central functionality which collects, edits, and shares metadata among the broad functions of the system	
MET 2.2	1	The broad functions include but are not limited to workflow, access, preservation, ingest, system administration, business processes, metadata dissemination	
MET 2.3	1	The system shall provide for centralized or distributed storage of metadata according to the requirements of particular functions	

3.2.3.3 Metadata - Interoperability (MET 3.0)

ID	Criticality	Capability	Spec. Required
MET 3.1	1	The system shall employ interoperable programming interfaces which are compliant with open standards, including, but not limited to, Extensible Markup Language (XML)	
MET 3.2	1	The system shall recognize multiple standards (schema and input standards) for expressing metadata, including, but not limited to MARC 21 for bibliographic data, PREMIS working group for preservation metadata, the Dublin Core Metadata Scheme, ONIX for publisher and bookseller data, according to the requirements of particular functions	
MET 3.3	2	The system shall provide a registry of schema and standards in use	
MET 3.4	2	The system shall provide "crosswalks" or other mechanisms to share data and provide linkages between schema and input standards	

3.2.3.4 Metadata - Collection & Storage (MET 4.0)

ID	Criticality	Capability	Spec. Required
MET 4.1	1	The system shall have the capability to acquire existing metadata from sources external to the system	
MET 4.2	1	The system shall have the ability to create metadata meeting the requirements of multiple schema	

3.2.3.5 Metadata - Editing, Manipulation, Sharing (MET 5.0)

ID	Criticality	Capability	Spec. Required
MET 5.1	1	The system shall have the ability to edit and delete metadata regardless of its source	
MET 5.2	1	The system shall have the ability to export metadata compliant with multiple standards	

3.2.4 Style Tools

3.2.4.1 Style Tools – Capture (ST 1.0)

ID	Criticality	Capability	Spec. Required
ST 1.1	1	The tool must accept deposited content	
ST 1.2	1	The tool must accept converted content	
ST 1.3	1	The tool must provide the ability for users to develop content (e.g., content that doesn't exist already)	
ST 1.4	2	The tool shall provide the capability to assign 13 Digit ISBN Numbers to content	
ST 1.5	1	The tool must accept content with specialized character sets (e.g., non-Roman, scientific notations)	
ST 1.6	3	The tool must accept content in multiple languages	
ST 1.7	1	The tool must assign Unique ID's to digital objects that were created by style tools.	

3.2.4.2 Style Tools – Composition (ST 2.0)

ID	Criticality	Capability	Spec. Required
ST 2.1	1	The tool must compose content	Yes
ST 2.2	3	The tool shall have the capability to compose based on content analysis.	Yes
ST 2.3	2	The tool shall have the capability to compose content and place graphical elements in locations using guidelines (GPO or Agency) and be optimized for understanding of information	Yes
ST 2.4	1	The tool shall have the capability to compose content based on content originator preferences	
ST 2.5	2	The tool shall have the capability to prompt users to define layout parameters from best available or system presented options.	
ST 2.6	1	The tool shall have the capability to allow users to compose content based on pre-defined design rules	Yes
ST 2.7	1	The tool shall have the capability to provide templates based on GPO or agency style guidelines	Yes
ST 2.8	1	The tool shall have the capability to allow users to select output methods for viewing preliminary composition (ie. Preparatory representation of content format or structure)	
ST 2.9	1	The tool must allow for viewing a localized presentation (ie. Temporary representation of layout or structure on a users local presentation device) of content	
ST 2.10	1	The tool shall have the capability to provide proofs of content and presentation.	

ST 2.11	1	The tool shall allow management of content based on the user's level of access	
ST 2.12	1	The system must provide tracking of all activities associated with work in progress	
ST 2.13	1	The tool shall provide the capability to modify content based on specified design parameters (e.g., GPO style manual, Agency style guide, user preferences)	Yes
ST 2.14	1	The tool shall create and pass SIP for ingest	
ST 2.15	1	The tool shall provide the capability to replicate any existing style of content received from Content Originators.	
ST 2.16	3	The tool shall provide the capability to revert to prior versions (e.g., History pallette)	

3.2.4.3 Style Tools – Collaboration (ST 3.0)

ID	Criticality	Capability	Spec. Required
ST 3.1	1	The tool shall allow for multiple users working collaboratively on the same content	
ST 3.2	1	The tool shall allow authorized users to approve/reject content changes made by collaborators based on access rights and permissions	
ST 3.3	1	The system shall provide the capability to store work in progress	
ST 3.4	1	The tool shall manage work in progress using GPO records management practices	Yes

ST 3.5	1	The system shall provide search and retrieval capabilities for WIP content (e.g., to allow CO's to pull unique digital objects into the creative process)	
ST 3.6	2	The system shall provide search and retrieval capabilities for content stored within FDsys (e.g., to allow CO's to pull unique digital objects into the creative process)	

3.2.4.4 Style Tools – Approval (ST 4.0)

ID	Criticality	Capability	Spec. Required
ST 4.1	1	The tool shall provide an approval process based on access rights and permissions.	
ST 4.2	1	The tool shall allow for approval of SIP submission to ingest.	
ST 4.3	1	The tool shall allow for approval of content presentation (e.g., is it pretty).	
ST 4.4	1	The tool shall allow for approval of content (e.g., proof approval).	

3.2.5 Deposited Content

3.2.5.1 Deposited Content – Standards (DEP 1.0)

ID	Criticality	Capability	Spec. Required
DEP 1.1	1	The system shall accept digital content provided by CO's	
DEP 1.2	1	The system must check provided digital file(s) (e.g., Virus Check, checksum) prior to ingest	Yes
DEP 1.3	1	The digital content may be sent through style tools before ingest.	

DEP 1.4	1	The system shall accept version information from deposited content	Yes
DEP 1.5	1	The system shall assign a Unique ID	Yes

3.2.5.2 Deposited Content - Verification and Validation (DEP 2.0)

ID	Criticality	Capability	Spec. Required
DEP 2.1	1	The system shall accept integrity marks at submission	Yes
DEP 2.2	1	The system shall ingest digital files that comprise a publication(s) approved for release by the content originating agency.	Yes
DEP 2.3	2	The system may process encrypted files through an alternate workflow to obtain key information to allow the file to be opened.	
DEP 2.4	2	The system shall provide notification to the submission agency/authority that the content has been received.	

3.2.5.3 Deposited Content – Metadata (DEP 3.0)

ID	Criticality	Capability	Spec. Required
DEP 3.1	1	The system shall accept files which contain all agency processing information with the deposited content, including billing information, jacket number, agency reference information, etc.	Yes
DEP 3.1.1	1	The system shall provide the capability to record (1) Title or caption of the content	Yes
DEP 3.1.2	1	The system shall provide the capability to record (2) Unique Identifier (persistent locators, filenames, ISNs, etc) of the content	Yes

DEP 3.1.3	1	The system shall provide the capability to record (1) Author / Creator of the content	Yes
DEP 3.1.4	1	The system shall provide the capability to record (2) Publisher / Authority of the content	Yes
DEP 3.1.5	1	The system shall provide the capability to record (3) Rights Owner of the content	Yes
DEP 3.1.6	1	The system shall provide the capability to record (1) Version information of the content	Yes
DEP 3.1.7	1	The system shall provide the capability to record (2) Relationship to other version or manifestations of the content	Yes
DEP 3.1.8	1	The system shall provide the capability to record (3) Structure Information of the content	Yes
DEP 3.1.9	1	The system shall provide the capability to record (1) Intended Output of the content	Yes
DEP 3.1.10	1	The system shall provide the capability to record (2) Intended Audience of the content	Yes

3.2.5.4 Deposited Content - System Administration (DEP 4.0)

ID	Criticality	Capability	Spec. Required
DEP 4.1	1	The system shall identify excepted files (e.g., encrypted files, usage restrictions) upon submission.	Yes
DEP 4.2	1	The system shall accept digital files that have rights limitations if they are in scope for GPO dissemination programs (e.g., controlled sales list, cooperative pubs, tangible electronic products with software rights issues).	Yes
DEP 4.3	1	The system shall provide data security for deposited content	Yes

DEP 4.4	1	The system must provide audit logs for deposited content processing.	

3.2.5.5 Deposited Content – Preservation (DEP 5.0)

ID	Criticality	Capability	Spec. Required
DEP 5.1	1	The system shall provide storage for deposited content.	
DEP 5.2	1	The system shall have the ability to convert the content to files expressed in interfaces which are compliant with open standards (including but not limited to XML)	Yes

3.2.6 Harvested Content

3.2.6.1 Harvested Content – Core Capabilities (HAR 1.0)

ID	Criticality	Capability	Spec. Required
HAR 1.1	1	The system shall accept content delivered by the harvesting function into WIP Storage.	
HAR 1.2	1	The system shall accept all metadata delivered by the harvesting function into WIP Storage.	
HAR 1.3	1	The system shall create a SIP (Harvested Content Package) from the harvested content and metadata.	Yes
HAR 1.4	1	The system shall have the ability to transform harvested content and metadata into interfaces which are compliant with open standards (including but not limited to XML).	Yes
HAR 1.5	1	The system shall have the ability to discern whether harvested content or metadata needs to be ingested (e.g., is it already in the system?).	Yes
HAR 1.6	1	The system shall allow for removal of duplicate harvested content.	Yes

3.2.6.2 Harvested Content - Harvester Tool Requirements (HAR 2.0)

ID	Criticality	Capability	Spec. Required
HAR 2.1	2	The harvester shall provide the capability to discover, assess and characterize content from Federal agency Web sites that fall within the scope of GPO dissemination programs.	Yes
HAR 2.2	2	The harvester shall determine if the discovered content is within the scope of GPO dissemination programs.	Yes
HAR 2.3	2	The harvester shall collect the in-scope discovered content and available metadata.	
HAR 2.4	2	The harvester shall deliver all in-scope content and metadata to WIP storage for processing.	
HAR 2.5	2	The harvester shall have the ability to locate and collect all file types that may reside on Content Originator Web sites (e.g., PDF, HTML, audio, video, proprietary word processing software, dynamic content, rich media, XML, etc).	Yes
HAR 2.6	2	The harvester shall have the capablity to collect content in the exact form that the content was resident on the agency Web site.	
HAR 2.7	2	To harvester must be able harvest to deep Web information.	Yes
HAR 2.7.1	2	The harvester must be able to harvest content contained in query-based databases.	Yes
HAR 2.7.2	2	The harvester must be able to harvest content contained in agency content management systems.	Yes
HAR 2.7.3	2	The harvester must be able to harvest content contained on dynamically generated Web pages.	Yes

HAR 2.7.4	2	The harvester must be able to harvest content contained on FTP servers.	Yes
HAR 2.7.5	2	The harvester must be able to harvest content contained behind proxy servers.	Yes
HAR 2.7.6	2	The harvester must be able to harvest content contained behind firewalls.	Yes

3.2.6.3 Harvested Content - Metadata (HAR 3.0)

ID	Criticality	Capability	Spec. Required
HAR 3.1	2	The harvester shall have the ability to locate and collect all metadata associated with harvested content, including identity, responsibility, reference information, version/fixity, technical, administrative and life cycle dates	Yes
HAR 3.2	2	The harvester shall have the ability to locate and collect Unique ID and title/caption information.	Yes
HAR 3.3	2	The harvester shall have the ability to locate and collect author/creator, publisher/authority, and rights owner information.	Yes
HAR 3.4	2	The harvester shall have the ability to locate and collect topical information and bibliographic descriptions.	Yes
HAR 3.5	2	The harvester shall have the ability to locate and collect version, fixity, relationship, and provenance information.	Yes
HAR 3.6	2	The harvester shall have the ability to locate and collect technical, structural, file format, packaging and representation information.	Yes

HAR 3.7	2	The harvester shall have the ability to locate and collect administrative metadata.	Yes

3.2.6.4 Harvested Content - Rules and Instructions (HAR 4.0)

ID	Criticality	Capability	Spec. Required
HAR 4.1	2	The harvester must accept and apply rules and instructions that will be used to assess whether discovered content is within the scope of GPO dissemination programs	Yes
HAR 4.2	2	The harvester shall have the capability to identify official Federal publications on Web sites	
HAR 4.3	2	The harvester shall provide a user interface to accommodate workflow management and scheduling of harvesting activities.	Yes

3.2.6.5 Harvested Content - Validation and Authentication (HAR 5.0)

ID	Criticality	Capability	Spec. Required
HAR 5.1	2	The harvester shall have the ability to collect integrity marks associated with content as it is being harvested.	
HAR 5.2	2	The harvester shall be able to determine the accuracy of harvesting.	Yes

3.2.6.6 Harvested Content - System Administration (HAR 6.0)

ID	Criticality	Capability	Spec. Required
HAR 6.1	2	The harvester shall provide quality control functions to test accuracy/precision of rule application and to incorporate results into rule creation/refinement.	
HAR 6.2	2	The harvester shall have the capability to produce reports on harvesting activities (discovered content and its location, scope assessment decisions, locations visited within a Web site, failures or errors, content discovered not in scope, etc.)	Yes
HAR 6.3	2	The discovery and harvesting tools shall have the ability to identify GPO as the owner of the tools.	

3.2.7 Converted Content

3.2.7.1 Converted Content - Standards (CON 1.0)

ID	Criticality	Capability	Spec. Required
CON 1.1	1	The system shall have the capability to accept digital content created by conversion processes (e.g., scanning, text encoding).	Yes
CON 1.2	1	The system shall provide the capability to check provided digital file(s) (e.g., Virus Check, checksum) prior to ingest	Yes
CON 1.3	2	The digital content may be sent through style tools before ingest.	
CON 1.4	1	The system shall accept version information from converted content	Yes
CON 1.5	1	The system shall assign a Unique ID	

3.2.7.2 Converted Content - Verification and Validation (CON 2.0)

ID	Criticality	Capability	Spec. Required
CON 2.1	1	The system shall accept integrity marks at submission	Yes
CON 2.2	1	The system shall ingest digital files that comprise a publication(s) approved for release by the content originating agency.	
CON 2.3	2	The system may process encrypted files through an alternate workflow to obtain key information to allow the file to be opened.	Yes
CON 2.4	2	The system shall provide notification to the submission agency/authority that the content has been received.	

3.2.7.3 Converted Content – Metadata (CON 3.0)

ID	Criticality	Capability	Spec. Required
CON 3.1	1	The system shall accept files which contain all agency processing information with the converted content, including billing information, jacket number, agency reference information, etc.	Yes
CON 3.1.1	1	The system shall provide the capability to record (1) Title or caption of the content	
CON 3.1.2	1	The system shall provide the capability to record (2) Unique Identifier (persistent locators, filenames, ISNs, etc) of the content	
CON 3.1.3	1	The system shall provide the capability to record (1) Author / Creator of the content	
CON 3.1.4	1	The system shall provide the capability to record (2) Publisher / Authority of the content	

CON 3.1.5	1	The system shall provide the capability to record (3) Rights Owner of the content	
CON 3.1.6	1	The system shall provide the capability to record (1) Version information of the content	
CON 3.1.7	1	The system shall provide the capability to record (2) Relationship to other version or manifestations of the content	
CON 3.1.8	1	The system shall provide the capability to record (2) Structure Information of the content	
CON 3.1.9	1	The system shall provide the capability to record (1) Intended Output of the content	
CON 3.1.10	1	The system shall provide the capability to record (2) Intended Audience of the content	

3.2.7.4 Converted Content - Systems Administration (CON 4.0)

ID	Criticality	Capability	Spec. Required
CON 4.1	1	The system shall identify excepted files (e.g., encrypted files, usage restrictions) upon submission.	Yes
CON 4.2	1	The system shall convert tangible titles that have rights limitations if they are in scope for GPO dissemination programs (e.g., controlled sales list, cooperative pubs, tangible electronic products with software rights issues).	Yes
CON 4.3	1	The system shall provide data security for converted content	
CON 4.4	1	The system must provide audit logs for converted content processing.	

3.2.7.5 Converted Content - Preservation (CON 5.0)

ID	Criticality	Capability	Spec. Required
CON 5.1	1	The system shall provide storage for converted content.	Yes
CON 5.2	1	The system shall convert the content to files expressed in interfaces which are compliant with open standards (including but not limited to XML)	Yes

3.2.8 Content Originator Ordering (COO 1.0)

ID	Criticality	Capability	Spec. Required
COO 1.1	1	The system shall provide the capability for Content Originators to specify Content Delivery options (hard copy, electronic presentation, digital media).	
COO 1.2	1	The system shall provide the list of approved external service providers.	
COO 1.3	2	The system shall provide the capability for Content Originators to select from GPO's approved external Service Providers	
COO 1.4	1	The system shall acquire content related to specific orders.	
COO 1.5	1	The system shall provide the capability to create, acquire, and store metadata elements specific to ordering functions, preservation needs, version, and job specifications (e.g., SF1, 952, 2511, 3868, etc.)	
COO 1.6	1	The system shall provide the capability for GPO users to augment C.O. order and job specifications (e.g., riders).	

COO 1.7	1	The system shall inform the Content Evaluators that a new order has been placed by a Content Originator.
COO 1.8	1	The system shall provide security for processing transactions.
COO 1.9	2	The system shall provide response back to an order request within a timeframe established by GPO business units responsive to C.O. need.
COO 1.10	1	The system shall provide context specific help and support.
COO 1.11	1	The system shall accept quotes from Service Providers.
COO 1.12	1	The system shall log financial and security activities associated with C.O.O.
COO 1.13	1	The system shall provide static and dynamic summary reports for various components of the system including Service Provider performance, Content Originator activity, response times, product types, dollar values/totals, number of jobs awarded to individual Service Providers.
COO 1.14	2	The system shall provide C.O. specific static and dynamic summary reports for various components of the system including Service Provider performance, Content Originator activity, response times, product types, dollar values/totals, number of jobs awarded to individual Service Providers.
COO 1.15	1	The system shall provide the capability to request re-orders based on previous orders.
COO 1.16	1	The system shall provide estimated costs to Content Originators for content and order information.

COO 1.17	1	The system shall provide actual costs to Content Originators based on job specifications.	
COO 1.18	1	The system shall be able to generate SIP for ingest.	
COO 1.19	1	The system must provide a unique id when content is initially submitted.	

3.2.9 Content Ingest

3.2.9.1 Ingest - Core Capabilities (ING 1.0)

ID	Criticality	Capability	Spec. Required
ING 1.1	1	The ingest processing function shall have the capability to accept SIPs	
ING 1.2	1	The system must have the capability to provide a graphical user interface to support ingest activities	
ING 1.2.1	1	The ingest processing function shall provide a prompt to confirm that the user intends to submit the SIP to ingest.	
ING 1.3	1	The ingest process shall make scope determinations on SIPs as defined by GPO business units (e.g. GPO, FDLP, National Bib., Sales Program, etc.)	
ING 1.3.1	1	The system shall record scope determination in metadata	
ING 1.4	1	The system shall process content based on GPO business rules (e.g., scope determination)	
ING 1.5	1	The system shall process non-conforming SIPs.	
ING 1.5.1	1	The system shall provide the capability to reject non-conforming SIPs.	

3.2.9.2 Ingest - SIP Validation (ING 2.0)

ID	Criticality	Capability	Spec. Required
ING 2.1	1	The ingest processing function shall validate SIPs against standards for content based on GPO best practices or rules	
ING 2.2	1	The ingest processing function must check each SIP to assure that metadata meets minimum submission level requirements	
ING 2.3	1	The ingest processing function shall have the capability to create a log entry notifying non-compliance with standards for content	

3.2.9.3 Ingest – Transformation (ING 3.0)

ID	Criticality	Capability	Spec. Required
ING 3.1	1	The ingest process shall transform SIPs into ACPs	
ING 3.2	1	The ingest process shall transform SIPs into AIPs	
ING 3.3	1	The system shall transfer AIPs to archival storage	
ING 3.4	1	The system shall transfer ACPs to access content storage	
ING 3.5	1	The ingest process shall transform content compliant with GPO specified open standards	

3.2.9.4 Ingest – Authentication (ING 4.0)

ID	Criticality	Capability	Spec. Required
ING 4.1	2	The ingest process shall have the capability to accept and transfer external integrity marks	
ING 4.2	1	The system shall authenticate SIPs at ingest	

3.2.9.5 Ingest - Version Control (ING 5.0)

ID	Criticality	Capability	Spec. Required
ING 5.1	1	The ingest process shall have the capability to accept and transfer version identifier information	
ING 5.2	1	The system shall perform version control on SIPs at ingest	

3.2.9.6 Ingest - Persistent Naming (ING 6.0)

ID	Criticality	Capability	Spec. Required
ING 6.1	2	The system shall have the capability to assign a persistent name at ingest	

3.2.9.7 Ingest - Unique ID (ING 7.0)

ID	Criticality	Capability	Spec. Required
ING 7.1	1	The ingest process shall have the capability to accept (from style tools) and transfer unique IDs at ingest.	
ING 7.2	1	The system shall assign unique IDs to digital objects at ingest	

3.2.9.8 Ingest – Metadata (ING 8.0)

ID	Criticality	Capability	Spec. Required
ING 8.1	1	The system shall record ingest processes in metadata	

3.2.10 Unique Identifier

3.2.10.1 Unique ID - Digital Objects (UID 1.0)

ID	Criticality	Capability	Spec. Required
UID 1.1	1	The system shall organize file(s) into digital objects at a level of granularity appropriate to the content and as defined by GPO business rules.	
UID 1.2	1	The system must create and assign an alphanumeric identifier (ANI) for each unique digital object	
UID 1.3	1	The system shall have the ability to assign a unique ID to a related or continuous piece of content in context	
UID 1.4	1	The DO unique ID must not be re-used	
UID 1.5	1	The system must record DO unique ID's in metadata	

3.2.10.2 Unique ID - Jobs Order Number (UID 2.0)

ID	Criticality	Capability	Spec. Required
UID 2.1	1	The system must create and assign an alphanumeric identifier (ANI) for each unique Job	
UID 2.2	1	The system must provide the capability for GPO to assign a Unique ID to each Job as defined by GPO Business rules.	

UID 2.3	1	The JOB unique ID must not be re-used	
UID 2.4	1	The system must record JOB unique ID's in metadata	

3.2.10.3 Unique ID - Content Packages (ACP, AIP) (UID 3.0)

ID	Criticality	Capability	Spec. Required
UID 3.1	1	The system must create and assign an alphanumeric identifier (ANI) for each unique Content Package	
UID 3.2	1	The system must provide the capability for GPO to assign a Unique ID to each Content Package as defined by GPO Business rules.	
UID 3.3	1	The Package unique ID must not be re-used	
UID 3.4	1	The system must record PACKAGE unique ID's in metadata	

3.2.11 Persistent Name

3.2.11.1 Persistent Naming - Core Capabilities (PN 1.0)

ID	Criticality	Capability	Spec. Required
PN 1.1	2	The system shall assign persistent names	
PN 1.1.1	2	The system shall assign persistent names to content packages during Ingest	
PN 1.1.2	2	The system shall comply with standards and best practices pertaining to persistent naming (e.g., URN RFC1737 and RFC2141, emerging Federal standards)	

PN 1.1.3	2	The system shall support interoperability across different naming systems to allow one system to access a resource within another
PN 1.1.4	2	The system shall accommodate OpenURL syntax to enable federated searching
PN 1.1.5	2	The system shall arbitrate between content origniator naming and global naming standards
PN 1.2	2	The system shall assign persistent names to all versions
PN 1.3	2	The system shall assign persistent names that are location independent
PN 1.4	2	The system shall assign persistent names that are permanent
PN 1.5	2	The system shall have the capability to assign persistent names that are human readable
PN 1.6	2	The system shall have the capability to log persistent name transactions
PN 1.7	2	The system shall have the capability to create reports about persistent name transactions (e.g., assignments, link checking)
PN 1.8	2	The system shall associate persistent names to existing legacy GPO naming schemes (e.g., PURLs)
PN 1.9	2	The system shall be scalable in terms of persistent name assignment and resolvability
PN 1.10	2	The system shall have the capability to support distributed persistent naming and resolution

3.2.11.2 Persistent Naming – Resolution (PN 2.0)

ID	Criticality	Capability	Spec. Required
PN 2.1	2	The system shall use a resolution system to locate and provide access to content with persistent names	.
PN 2.2	2	The system shall support resolution of a single persistent name to multiple distributed locations	
PN 2.3	2	The system shall support resolution of a single persistent name to multiple content versions	

3.2.11.3 Persistent Naming – Metadata (PN 3.0)

ID	Criticality	Capability	Spec. Required
PN 3.1	2	The system shall record persistent names associated with content	
PN 3.1.1	2	The system shall record existing persistent names associated with content	
PN 3.2	2	The system shall provide the capability to associate metadata with the persistent name	

3.2.12 Authentication

3.2.12.1 Authentication - Certification of Content (AUT 1.0)

ID	Criticality	Capability	Spec. Required
AUT 1.1	1	The system shall provide the capability to certify content as authentic and/or official	Yes

AUT 1.2	1	The system shall provide the capability to certify content at levels of granularity defined in GPO's business rules	Yes
AUT 1.3	1	The system shall convey certification by means of an integrity mark.	Yes

3.2.12.2 Authentication - Verification/Validation of Content (AUT 2.0)

ID	Criticality	Capability	Spec. Required
AUT 2.1	1	The system shall provide the capability to verify and validate the authenticity of deposited content	Yes
AUT 2.2	1	The system shall provide the capability to verify and validate the authenticity of harvested content	Yes
AUT 2.3	1	The system shall provide the capability to verify and validate the authenticity of converted content	Yes
AUT 2.4	1	The system shall accept and validate integrity marks in SIPs at the time of ingest	Yes
AUT 2.5	1	The system shall verify chain of responsibility in SIPs at the time of ingest	Yes
AUT 2.6	1	The system shall provide the capability to provide date verification for certified content	Yes
AUT 2.7	1	The system shall provide the capability to provide time verification for certified content	Yes

3.2.12.3 Authentication - Re-authentication of Content (AUT 3.0)

ID	Criticality	Capability	Spec. Required
AUT 3.1	1	The system shall support the capability to re-authenticate content that has already been authenticated	Yes

AUT 3.2	1	The system shall provide the capability to notify GPO service specialists when content needs to be re-authenticated	Yes
AUT 3.3	1	The system shall provide the capability to change or revoke the authentication status of content	Yes

3.2.12.4 Authentication – Credentials (AUT 4.0)

ID	Criticality	Capability	Spec. Required
AUT 4.1	1	The system shall verify the identity of the content creator	Yes
AUT 4.2	1	The system shall verify the authority of the content creator	Yes

3.2.12.5 Authentication - Content Changes (AUT 5.0)

ID	Criticality	Capability	Spec. Required
AUT 5.1	1	The system shall provide notification that a change has occurred to content within the system	Yes
AUT 5.1.1	1	The system shall provide the capability to notify when changes were made to content	Yes
AUT 5.1.2	1	The system shall provide the capability to notify where changes were made to content	Yes
AUT 5.1.3	1	The system shall provide the capability to notify by who changes were made to content	Yes
AUT 5.1.4	1	The system shall provide the capability to notify what changes were made to content	Yes
AUT 5.2	1	The system shall provide the capability to securely store authenticated content	Yes

AUT 5.3	1	The system shall provide the capability of demonstrating continued integrity of content packages when changes are made (such as to the metadata)	Yes

3.2.12.6 Authentication - Standards/Best Practices (AUT 6.0)

ID	Criticality	Capability	Spec. Required
AUT 6.1	1	The system shall support Internet Engineering Task Force Public Key Infrastructure (PKIX) X.509 v.3 standards for authentication	Yes
AUT 6.2	1	The system shall support up to 2048-bit RSA public/private key generation for authentication	Yes
AUT 6.3	1	The system shall support cryptographic standards in accordance with the FIPS 140 series	Yes

3.2.12.7 Authentication - Integrity Marks (AUT 7.0)

ID	Criticality	Capability	Spec. Required
AUT 7.1	1	The system shall support the use of integrity marks	Yes
AUT 7.2	1	The system shall provide the capability to add integrity marks to content that is delivered from the system.	Yes
AUT 7.3	1	The system shall support the use of visible integrity marks	Yes
AUT 7.4	1	The system shall support the use of invisible integrity marks	Yes
AUT 7.5	1	The system shall place integrity marks that do not interfere with presentation/delivery	Yes

AUT 7.6	1	The system shall support the capability to apply an integrity mark to content that already has an integrity mark	Yes
AUT 7.7	1	The system shall support the application of multiple integrity marks on the same information content	Yes
AUT 7.8	1	The system shall support the application of security policies, such that integrity marks can be applied to content in particular sequences depending on levels of authority	Yes

3.2.12.8 Authentication - Records Management (AUT 8.0)

ID	Criticality	Capability	Spec. Required
AUT 8.1	1	The system shall create administrative records of authentication processes	Yes
AUT 8.2	1	The system shall create transaction records of administrative processes	Yes
AUT 8.3	1	The system must support an audit capability for content certification	Yes
AUT 8.4	1	The system must support an audit capability for content validation	Yes

3.2.12.9 Authentication – Metadata (AUT 9.0)

ID	Criticality	Capability	Spec. Required
AUT 9.1	1	The system shall provide the capability to include authentication information in the content's metadata	Yes

3.2.13 Version Control

3.2.13.1 Version Control - Core Capabilities (VER 1.0)

ID	Criticality	Capability	Spec. Required
VER 1.1	1	The system shall determine if version identifiers are present in content packages.	Yes
VER 1.2	1	The system shall have the ability to assign version identifiers to content packages that do not already contain version identifiers.	Yes
VER 1.3	1	The system shall record existing version identifiers.	Yes
VER 1.4	1	The system must apply rules for version triggers.	Yes
VER 1.4.1	1	The system shall apply rules for version triggers to groups of related content as defined by GPO business units.	Yes
VER 1.5	1	The system must allow authorized users to input, view, and manage version information (metadata).	Yes
VER 1.6	1	The system shall perform version detection on SIPs (e.g. final published versions) and assign version identifiers at ingest.	Yes
VER 1.7	1	The system shall compare SIPs to existing content packages to determine if identical versions already exists in the system.	Yes
VER 1.8	1	The system shall evaluate SIPs against GPO version control policy.	Yes
VER 1.9	1	The system shall express version information (e.g., version identifiers, version crosswalks, version triggers) in metadata.	Yes

VER 1.10	1	The system shall detect version triggers as defined by GPO business units. Version triggers may include the following:	Yes
VER 1.10.1		Modifications to the content	
VER 1.10.2		Changes to the "last updated" date	
VER 1.10.3		Language translations	
VER 1.10.4		Changes to a publication's title	
VER 1.10.5		Changes to a publication's edition statement	
VER 1.10.6		Changes in the issuing agency of a publication	
VER 1.10.7		Changes in medium (e.g., print to CD ROM, microform to PDF)	
VER 1.10.8		Changes in file format (e.g., TIFF to JPEG)	
VER 1.10.9		Levels of authentication (e.g., authentic vs. official)	
VER 1.10.10		Changes to the publication's numbering (e.g. volume 100, issue 50, year 2005, etc.)	
VER 1.11	1	The system shall provide the capability to alert GPO users when version triggers have been activated	Yes
VER 1.12	1	The system shall provide notification when a version cannot be determined	Yes
VER 1.13	1	The system shall log all version history.	Yes

VER 1.14	3	The system shall detect changes that were previously detected and "excluded" as a version trigger.	Yes
VER 1.15	1	The system shall record chain of responsibility (e.g. who created the content, when it was created, who approved the content for release, etc.).	Yes
VER 1.16	1	The system shall provide the capability to reject duplicate content at ingest.	Yes
VER 1.17	1	The system shall determine and record relationships between versions (e.g. version links).	Yes
VER 1.18	1	The system shall provide the capability to apply version control to pre-publication content.	Yes

3.2.13.2 Version Control - WIP Content Versions (VER 3.0)

ID	Criticality	Capability	Spec. Required
VER 3.1	1	The system will manage multiple versions of work in progress.	Yes

3.2.14 Access

3.2.14.1 Access - Core Capabilities (ACC 1.0)

ID	Criticality	Capability	Spec. Required
ACC 1.1	1	The system shall provide open and interoperable access to content packages in content stores (ACS, CPS, WIP, AIS).	Yes
ACC 1.2	1	The system shall allow GPO users to designate levels of access based on user privileges and credentials.	Yes
ACC 1.3	1	The system shall accept access rules defined by GPO.	Yes

ACC 1.4	1	The system shall allow GPO to limit access to content packages based on rules and policy (e.g., publications with re-dissemination restrictions and limited distribution).	Yes
ACC 1.5	1	The system shall provide the capability to access in scope content not resident within the system.	Yes
ACC 1.6	1	The system shall provide the capability for users to access content in multiple languages and non-Roman character sets.	Yes
ACC 1.7	1	The system shall provide section 508 compliant access to content packages.	Yes
ACC 1.8	1	The system shall create section 508 compliant Access Content Packages.	Yes
ACC 1.9	1	The system shall provide the capability to perform records management functions for Access.	Yes

3.2.14.2 Search

3.2.14.2.1 Search - Core Capabilities (S 1.0)

ID	Criticality	Capability	Spec. Required
S 1.1	1	The system shall provide the capability to search and retrieve content packages from all content stores.	Yes
S 1.2	1	The system shall provide the ability to search content collections based on access rights and privileges.	Yes
S 1.3	1	The system shall allow users to search and retrieve content and metadata from select external storage devices as defined by GPO business rules.	Yes

S 1.3.1	1	The system shall allow users to search across multiple internal and external content collections simultaneously and seperately.	Yes
S 1.3.2	1	The system shall allow users to search metadata and content both simultaneously and separately.	Yes
S 1.4	2	The system shall allow users to search and retrieve selected BPI (e.g., information about current and historical Requests and C.O. Orders for products and services).	Yes
S 1.5	1	The system shall have the capability to search and retrieve unstructured content (e.g., text).	Yes
S 1.5.1	1	The system shall have the capability to match character strings (e.g., search exact phrases).	Yes
S 1.6	1	The system shall have the capability to search and retrieve semi-structured content and metadata (e.g., inline markup).	Yes
S 1.7	1	The system shall have the capability to search and retrieve structured content and metadata (e.g., fielded).	Yes
S 1.8	2	The system shall allow GPO users and content originators to search in ACS and work in progress both simultaneously and separately.	Yes
S 1.9	1	The system shall provide the capability to support multiple user classes as defined by GPO business rules.	Yes

3.2.14.2.2 Search – Query (S 2.0)

ID	Criticality	Capability	Spec. Required
S 2.1	1	The system shall allow users to select available search options.	Yes
S 2.2	1	The system shall allow users to select content collections to search.	Yes
S 2.3	2	The system shall allow users to select search complexity levels (e.g., simple search, advanced/fielded search).	Yes
S 2.4	1	The system shall allow users to limit searches by available qualifiers, options, or limits as defined by GPO business rules.	Yes
S 2.4.1	1	The system shall provide the ability to limit a search to full text.	
S 2.4.2	1	The system shall provide the ability to limit a search to bibliographic information.	
S 2.4.3	1	The system shall provide the ability to limit a search by format (e.g., PDF, image, audio).	
S 2.5	2	The system shall allow users to perform a search for conceptually related terms (e.g., search for "World Series" returns articles on the Red Sox).	Yes
S 2.6	1	The system shall support standard Boolean search language, including AND, OR, NOT, BEFORE, and NEAR, and Boolean operators must not be case-sensitive.	Yes
S 2.7	2	The system shall support fuzzy logic searching.	Yes
S 2.8	1	The system shall allow users to perform a natural language search that does not require connectors or a specific syntax.	Yes

S 2.9	1	The system shall support a customizable list of stop words.	Yes
S 2.10	2	The system shall allow for right and left truncation.	Yes
S 2.11	2	The system shall allow users to use wildcard characters to replace characters within words.	Yes
S 2.12	2	The system shall support proximity searching.	Yes
S 2.13	2	The system shall support synonyms searching.	Yes
S 2.14	2	The system shall allow users to apply multiple search logic in a single search query (e.g., Boolean, truncation, wildcards, nesting).	Yes
S 2.15	1	The system shall allow users to select specified search functionality.	Yes
S 2.16	1	The system shall support queries of variable lengths.	Yes
S 2.17	1	The systems shall have the ability to limit search query length.	Yes
S 2.18	1	The system shall allow users to weight search terms (e.g., term must appear, term must not appear, term is part of an exact phrase).	Yes

3.2.14.2.3 Search – Refine (S 3.0)

ID	Criticality	Capability	Spec. Required
S 3.1	1	The system shall provide the ability to modify previous search queries to enable execution of subsequent searches.	Yes
S 3.1.1	2	The system shall provide the ability to direct subsequent queries against different content collections.	Yes
S 3.1.2	2	The system shall provide the capability for users to retain selected targets while modifying queries.	Yes

S 3.2	2	The system shall provide the ability to collect selected results from multiple search queries.	Yes
S 3.3	2	The system shall provide the ability to display a list of terms that are conceptually related to the original search term.	Yes
S 3.3.1	2	The system shall provide users with the ability to directly execute a search from conceptually related terms.	Yes
S 3.4	2	The system shall recognize alternate spellings of terms and provide suggestions for alternative terms.	Yes
S 3.4.1	2	The system shall suggest corrected spellings of terms.	Yes

3.2.14.2.4 Search – Results (S 4.0)

ID	Criticality	Capability	Spec. Required
S 4.1	1	The system shall provide search results	
S 4.2	2	The system shall provide user customizable results lists.	Yes
S 4.2.1	2	The system shall provide results lists based on search skill level.	Yes
S 4.2.2	2	The system shall provide results lists based on user class.	Yes
S 4.2.3	2	The system shall provide results lists based on user preferences.	
S 4.3	1	The system shall allow users to sort results lists.	Yes
S 4.3.1	1	The system shall allow users to sort results by title.	
S 4.3.2	1	The system shall allow users to sort results by date.	
S 4.3.3	2	The system shall allow users to sort results by content collection.	

S 4.3.4	1	The system shall allow users to sort results by relevancy.	
S 4.3.5	2	The system shall allow users to sort results by format (e.g., text, audio, video).	
S 4.3.6	2	The system shall allow users to sort results by Content Originator.	
S 4.3.7	2	The system shall allow users to sort results by certification.	
S 4.3.8	2	The system shall allow users to sort results by GPO defined metadata fields.	
S 4.3.9	2	The system shall allow users to sort results by version.	
S 4.3.10	2	The system shall allow users to sort results by price.	
S 4.4	3	The system shall provide the capability to analyze results lists.	Yes
S 4.4.1	3	The system shall provide the capability to cluster results.	
S 4.4.2	3	The system shall provide the capability to display results graphically.	
S 4.5	2	The system shall provide the capability for users to limit the number of results displayed.	Yes
S 4.6	1	The system shall provide the capability to display the total number of results in the result set returned by the search.	Yes
S 4.7	2	The system shall display an explanation for returning a null set of results.	Yes
S 4.8	1	The system shall provide the capability to configure the elements in a result.	Yes
S 4.8.1	1	The system shall display, at a minimum, title, file size, version, content collection (source), and an identifier (link).	

S 4.8.2	2	The system shall display other elements in a result (e.g., relevance rank, description of content) when available.	
S 4.9	3	The system shall provide the capability to highlight query terms in the results list.	Yes
S 4.10	1	The system shall provide the ability to generate error messages for failed searches.	Yes
S 4.11	2	The system shall display search results in a format that makes subsequent options clear to users at various search skill levels. (e.g., providing expanded metadata, following links to content, modifying a search, saving a search, initiating a new search).	Yes
S 4.12	2	The system shall provide the capability to display inline image thumbnails of content in a results list.	Yes
S 4.13	3	The system shall provide information to enable users to determine why a result was returned.	Yes
S 4.14	2	The system shall allow users to save search results individually or as a batch (e.g., without selecting each result individually) for export.	Yes
S 4.15	1	The system shall provide the capability to deliver search results at the finest level of granularity supported by the target content package.	Yes
S 4.16	1	The system shall have the capability to combine the metadata for multiple versions of the same content into a single display.	Yes

3.2.14.2.5 Search - Saved Searches (S 5.0)

ID	Criticality	Capability	Spec. Required
S 5.1	2	The system shall allow users with an established user profile to enter or store queries, preferences, and results sets or portions of results sets.	Yes
S 5.2	2	The system shall provide the capability to automatically execute saved searches on a schedule defined by the user.	Yes
S 5.3	2	The system shall provide the capability to notify users when automatically executed searches return results.	Yes

3.2.14.2.6 Search – Performance (S 6.0)

ID	Criticality	Capability	Spec. Required
S 6.1	1	The system shall have a response rate for the search process based on GPO business rules.	Yes
S 6.2	1	The system shall allow simultaneous searches based on GPO business rules.	Yes

3.2.14.2.7 Search - Federated Search (S 7.0)

ID	Criticality	Capability	Spec. Required
S 7.1	1	The system shall conform to international standards for search interoperability.	Yes
S 7.1.1	1	The system shall conform to ISO 23950.	Yes

S 7.2	1	The system shall provide the capability to perform federated searches across multiple internal and external repositories, including legacy repositories (e.g., WAIS).	Yes
S 7.3	1	The system must have a documented search interface to allow search by non-GPO systems (e.g., Web search engines).	Yes

3.2.14.2.8 Search – Interface (S 8.0)

ID	Criticality	Capability	Spec. Required
S 8.1	1	The system shall provide a search interface that allows users to submit queries to the system and receive results.	Yes
S 8.2	1	The system shall provide multiple search interfaces based on search skill level and user class.	Yes
S 8.3	1	The system shall provide customizable search interfaces based on user preferences and requirements.	Yes
S 8.4	1	The system shall provide navigational elements to allow users to view results from internal and external repositories.	Yes
S 8.5	2	The system shall have the capability to store and access user search preferences (e.g., preferred layout, preferred search method, frequently used content collections).	Yes
S 8.6	2	The system shall provide a search progress indicator while the search is in progress	Yes
S 8.7	2	The system shall display the search parameters selected by the user while the search is in progress	Yes

S 8.8	3	The system shall provide an estimate to the user of how long the search will take to execute while the search is in progress	Yes
S 8.9	1	The system shall notify the user that the search is complete	Yes
S 8.10	1	The system shall provide the capability to integrate search, reference tools, request, and user support seamlessly into a single interface.	Yes
S 8.11	1	The system must meet accessibility requirements as defined in section 508 of the Rehabilitation Act.	Yes

3.2.14.2.9 Search – Administration (S 9.0)

ID	Criticality	Capability	Spec. Required
S 9.1	1	The system shall provide for the control of search run times, including the ability to preempt runtimes by an administrator-defined limit.	Yes
S 9.2	1	The system must support search capability on multiple redundant systems in multiple locations for uninterrupted service.	Yes
S 9.3	1	The system must provide the capability to support user search while other system functions are being performed (e.g., re-indexing databases, updating content).	Yes
S 9.4	1	The system shall log search transactions (e.g., user access, administrative changes).	Yes

3.2.14.3 Request

3.2.14.3.1 Request - Core Capabilities (R 1.0)

ID	Criticality	Capability	Spec. Required
R 1.1	1	The system shall provide the capability for users to request delivery of content and/or metadata contained in access storage (ACS)	Yes
R 1.1.1	1	The system shall provide the capability for users to request delivery of content and metadata located in the GPO system	Yes
R 1.1.2	1	The system shall provide the capability for users to request delivery of content and metadata located outside the GPO system	Yes
R 1.2	1	The system shall determine what options are available for delivery of particular content.	Yes
R 1.3	1	The system shall allow users to request delivery from available options as defined by GPO business units.	Yes
R 1.3.1	1	The system shall allow users to select format from available options (e.g., document, audio)	Yes
R 1.3.2	1	The system shall allow users to select file type from available options (e.g., DOC, MP3)	Yes
R 1.3.3	2	The system shall have the capability to support custom composition and content formatting from available options (e.g., 2 columns, cover stock, font)	Yes
R 1.3.4	1	The system shall provide the capability to preview requested content.	Yes

R 1.3.5	1	The system shall allow users to select output type from available options (e.g., hard copy, electronic presentation, digital media)	Yes
R 1.3.6	1	The system shall allow users to select data storage device from available options (e.g., CD, DVD)	Yes
R 1.3.7	1	The system shall allow users to select level of granularity from available options (e.g., title, part, section)	Yes
R 1.3.8	1	The system shall allow users to select tangible delivery method from available options (e.g., air transportation, ground transportation, pickup)	Yes
R 1.3.9	1	The system shall allow users to select electronic delivery method from available options (e.g., FTP, RSS, email, download, broadcast)	Yes
R 1.3.10	1	The system must offer customers separate “bill to” and “ship to” options.	Yes
R 1.3.11	1	The system shall allow users to submit multiple address options for delivery or shipment.	Yes
R 1.4	1	The system shall provide the ability for users to request fee and no-fee delivery options when available as defined by GPO business rules	Yes
R 1.4.1	1	The system shall have the capability to generate price information for the delivery of content	Yes
R 1.4.2	1	The system shall have the capability to adjust price information for the delivery of content	Yes
R 1.5	1	The system shall provide the capability to create and assign an alphanumeric user order number for each request.	Yes
R 1.5.1	1	The system shall not repeat a user order number	Yes

R 1.5.2	1	The system shall record user order numbers in metadata	Yes
R 1.5.3	1	The system shall have the capability to provide order numbers to users	Yes
R 1.6	1	The system shall allow Federal Depository Library users to select and request content for delivery to their library based on their preferences.	Yes
R 1.7	1	The system shall provide the capability for GPO users, agencies, and Congress to ride requests as defined by GPO business rules.	Yes
R 1.7.1	1	The system shall provide notification to GPO and Content Originators that riders have taken place.	Yes
R 1.7.2	1	The system shall have the capability to alert GPO users, agencies, and Congress that GPO is accepting riders for content as defined by GPO business rules.	Yes

3.2.14.3.2 Request - Content Delivery (Orders) (R 2.0)

ID	Criticality	Capability	Spec. Required
R 2.1	1	The system shall provide the capability to process no-fee based content delivery requests.	Yes
R 2.2	1	The system shall allow users to submit payment for delivery.	Yes
R 2.3	1	The system shall interface with GPO's financial and inventory infrastructures to process fee-based requests.	Yes
R 2.4	1	The system shall ensure that user transactions are conducted in a secure environment at the industry standard level of encryption.	Yes

R 2.5	1	The system must adhere to industry best practices for performance of an e-commerce system.	Yes
R 2.6	1	The system must offer a shopping cart feature that adheres to industry best practices.	Yes
R 2.6.1	1	The shopping cart shall include price, title of content, user order number and selected delivery options.	Yes
R 2.6.2	1	The shopping cart shall allow users to manage items (e.g., change quantity requested, add or remove items)	Yes
R 2.7	2	The system shall allow users to save the request information in a shopping cart after a session has ended (e.g., stored pending orders).	Yes
R 2.8	1	The system shall provide and support methods of payment as defined by GPO business rules (e.g. deposit accounts, credit cards, check/electronic transfer).	Yes
R 2.9	1	The system must automatically verify and validate payment information submitted by users before fulfillment (e.g. credit card, deposit account, and electronic transfer information).	Yes
R 2.10	2	The system shall enable customers to store and access user preferences and request histories in a secure environment (e.g. request status, delivery preferences, preferred payment methods, request tracking, prior request history)	Yes
R 2.11	1	The system shall allow the user to track the status of all requests using unique order numbers or other information as defined by GPO business rules.	Yes

R 2.12	1	The system shall provide all users with detailed transaction summary and receipt for all requests (including title(s) requested, quantities, price of each publication, order number, and any cost that will be billed to the user)	Yes
R 2.13	3	The system shall provide the capability to deliver personalized offers based on user request history (e.g. "you may also be interested in…")	Yes
R 2.14	1	The system shall provide the capability to allow users to cancel full or partial requests prior to fulfillment.	Yes
R 2.15	1	The system shall support delivery of content by subscriptions (i.e. An agreement by which a user obtains access to requested content by payment of a periodic fee or other agreed upon terms.)	Yes
R 2.15.1	1	The system shall allow users to request, renew, modify, and end subscriptions.	Yes
R 2.15.2	1	The system shall provide notification to users when their subscriptions are about to end (e.g., renewal notices)	Yes
R 2.16	1	The system shall provide the capability for content originators to view the request history of their content.	Yes
R 2.17	1	The system shall allow users to delegate requests to other users (e.g. users “hand-off” orders to other authorized officials to submit payment)	Yes
R 2.18	2	The system shall provide lists of new and popular titles, best sellers, and other lists as defined by GPO business rules.	Yes

3.2.14.4 Cataloging and Reference Tools

3.2.14.4.1 Cataloging and Reference Tools - Metadata Management (CR 1.0)

ID	Criticality	Capability	Spec. Required
CR 1.1	1	The system shall provide for the creation of metadata for content.	Yes
CR 1.2	1	The system shall support creation of metadata according to specified cataloging rules	Yes
CR 1.2.1	1	The system will apply authority control to provide cross-referencing of terms. (e.g., A user enters any form of a name, title, or subject in a search, all database items associated with that form must be retrieved)	
CR 1.3	1	The system shall support the creation of bibliographic information meeting book industry requirements	Yes
CR 1.4	1	The system shall support the creation of library standard bibliographic records	Yes
CR 1.5	1	The system shall support the creation of metadata by the system (e.g., automatically create)	
CR 1.6	1	The system shall provide for the creation of metadata by users (e.g., manually create)	
CR 1.7	1	The system shall provide tools for creation of new metadata for content at varying levels of aggregation.	
CR 1.8	1	The system shall provide for the creation of new metadata records based on existing metadata records	
CR 1.9	1	The system shall provide the capability to acquire metadata from external sources	Yes

CR 1.10	1	The system shall check the quality of metadata against GPO-defined standards	Yes
CR 1.11	1	The system shall relate descriptive metadata with the content described	
CR 1.12	1	The system shall provide capability for users to manage (add, modify, delete) metadata	
CR 1.13	1	The system shall have the ability to manage metadata	
CR 1.14	1	The system shall support versioning of metadata (i.e. maintain transaction history)	
CR 1.15	2	The system shall provide the capability to link related resources in descriptive metadata	
CR 1.16	1	The system shall have the ability to provide access to metadata prior to publication.	
CR 1.17	1	The system must provide the capability to add metatdata specifically for GPO sales purposes (e.g., book jacket art, reviews, summaries, etc.)	Yes

3.2.14.4.2 Cataloging and Reference Tools - Metadata Delivery (CR 2.0)

ID	Criticality	Capability	Spec. Required
CR 2.1	1	The system shall provide the capability to export metadata as individual records or in batch	
CR 2.2	1	The system will provide for display and output of brief citations, basic bibliographic citations, full records and MARC records. Output can be saved in a variety of forms (e.g., electronic mail, as ASCII text, comma delimited text and/or bibliographic formats)	Yes

CR 2.3	1	The system shall output metadata in formats specified by the user (e.g., MARC, ONIX)	Yes

3.2.14.4.3 Cataloging and Reference Tools - Reference Tools (CR 3.0)

ID	Criticality	Capability	Spec. Required
CR 3.1	1	The system shall have the ability to generate lists based on any indexed metadata field.	
CR 3.2	1	The system should have the capability to generate lists based on user defined criteria (e.g., that match a library's item selection profile)	
CR 3.3	1	The system should have the capability to generate lists that point to content (e.g., electronic journals, lists of products that are available for purchase from the GPO Sales Program)	
CR 3.4	1	The system should have the capability to generate lists that point to metadata (e.g., lists of publications available for selection by depository libraries)	
CR 3.5	1	The system should have the capability to generate lists that point to related resources or other reference tools (e.g., Browse Topics)	
CR 3.6	1	The system shall have the capability to link to external content and metadata.	
CR 3.7	2	The system shall be interoperable with third party reference tools (e.g., search catalogs of other libraries).	Yes
CR 3.8	2	They system shall have the capability to dynamically generate Reference Tools.	
CR 3.9	1	They system shall have the capability to deliver Reference Tools in electronic and tangible formats.	Yes

CR 3.10	1	The system will allow GPO to manage reference tools	
CR 3.11	2	The system must be able to generate lists based on user preferences.	
CR 3.12	2	The system shall support interactive processes so users can create reference tools.	

3.2.14.4.4 Cataloging and Reference Tools - Interoperability and Standards (CR 4.0)

ID	Criticality	Capability	Spec. Required
CR 4.1	1	The system shall interface with, and allow full functionality of, the GPO Integrated Library System	Yes
CR 4.2	1	The system must be able to interact with the GPO's implementation of the OCLC PURL software application	Yes
CR 4.3	1	The system must be compliant with the following NISO and ISO standards: Z39.2 - Information Interchange Format, Z39.9 - International Standard Serial Numbering-ISSN, Z39.50 - Information Retrieval: Application Service Definition & Protocol Specification, Z39.56 - Serial Item and Contribution Identifier (SICI), Z39.69 - Record Format for Patron Records, Z39.71 - Holding Statements for Bibliographic Items, Z39.85 - Dublin Core Metadata Element Set	Yes

CR 4.4	1	The system must support the use of the following and support all subsequent modifications, updates and revisions to the Anglo-American Cataloging Rules, 2nd Edition (AACR2), Library of Congress Classification, Library of Congress Cataloging Rules, AACR2 Rev., LC Rule Interpretations, Cooperative Online Serials (CONSER) Cataloging Guidelines, Superintendent of Documents Classification Manual, Library of Congress Subject Headings, NASA Subject Headings, MESH Subject Headings, all MARC Formats, and other GPO specified standards and best practices	Yes
CR 4.5	1	The system shall support the creation of ONIX records.	Yes
CR 4.6	1	The system must provide for the use of open APIs.	
CR 4.7	1	The system must be capable of accommodating and providing search/index functionality for GPO local data elements that identify unique attributes of the FDLP, such as GPO Superintendent of Documents (SuDocs) classification number, Item number, Depository Library number.	Yes

3.2.14.4.5 Cataloging and Reference Tools - Workflow (CR 5.0)

ID	Criticality	Capability	Spec. Required
CR 5.1	1	The system shall provide resources and references for internal cataloging staff	
CR 5.2	2	The system will support priority processing; e.g., alerts, assignments to staff, nonstandard workflow, tracking, etc.	

3.2.14.5 Interface

3.2.14.5.1 Interface - Core Capabilities (IF 1.0)

ID	Criticality	Capability	Spec. Required
IF 1.1	1	The system shall provide an interface for each functional element as outlined in the requirements.	Yes
IF 1.1.1	1	The system shall provide a GUI for each functional element as outlined in the requirements.	Yes
IF 1.2	1	The system shall provide an interface (ie GUI) for each user class.	Yes
IF 1.3	1	The system shall provide a default workbench (ie set of available tools) for each user class.	Yes
IF 1.3.1	1	The system shall display the appropriate default workbench based on a user's rights and privileges.	Yes
IF 1.3.2	2	The system shall provide the user the ability to customize the user interfaces by adding tools to the default workbench.	Yes
IF 1.3.3	2	The system shall provide the user the ability to customize the user interfaces by removing and hiding tools from the default workbench.	Yes
IF 1.3.4	2	The system shall provide the user the ability to customize the appearance of the workbench.	Yes
IF 1.3.5	2	The system shall allow users to select among available workbenches.	Yes
IF 1.3.6	2	The system shall allow users to work on multiple workbenches simultaneously.	Yes
IF 1.4	1	The system shall have the capability to provide system information to users at login.	Yes

IF 1.5	1	The system shall provide the capability for users to login and create an account.	Yes
IF 1.6	1	The system shall provide the capability to create a "group login." This will allow individual users to log into the system but provide access to an entire group of users.	Yes
IF 1.7	2	The system shall provide the capability for GPO to create default interfaces for subsets of user classes (e.g. kids, law community, individual agencies).	Yes
IF 1.8	2	The system shall maintain workbench configuration across user sessions.	Yes
IF 1.9	1	The system shall provide a default workbench for public end users that does not require them to log-in.	Yes
IF 1.10	1	The system shall provide the capability to maintain a consistent look and feel through out all workbenches and interfaces.	Yes
IF 1.11	1	The system shall support web based and non web based (e.g., desktop application) interfaces.	Yes
IF 1.12	2	The system shall provide the capability for users to create interfaces based on their rights and preferences.	Yes
IF 1.13	1	The system shall provide user interfaces capable of rendering supported types of electronic files (e.g., representing electronic presentation).	Yes
IF 1.14	1	The system shall provide for non-English language extensibility such that the user interface could contain non-English language text (e.g., ISO standard 10646 for Unicode).	Yes

IF 1.15	1	The system shall provide for the creation of system interfaces that promote interoperability among networked systems (e.g., APIs)	Yes
IF 1.16	1	The system shall support multiple application windows open simultaneously and integrate with standard desktop applications.	Yes

3.2.14.5.2 Interface – Standards (IF 2.0)

ID	Criticality	Capability	Spec. Required
IF 2.1	1	The system shall comply with best practices and guidelines regarding usability for interface (e.g., The Research-Based Web Design & Usability Guidelines function as best practices for Federal Agencies).	Yes
IF 2.2	1	The system shall ensure that interfaces comply with accessibility laws and regulations (e.g., Section 508 of the Rehabilitation Act Amendments of 1998) as appropriate.	Yes
IF 2.3	1	The system shall conform to current World Wide Web Consortium (W3C) guidelines for interoperable technologies.	Yes
IF 2.4	1	The system shall have the capability to comply with ICGI recommendations.	Yes
IF 2.5	2	The system shall conform to Policies for Federal Agency Web sites, an OMB memorandum issued on December 17, 2004.	Yes

3.2.14.5.3 Interface - User Interfaces by Functional Elements (IF 3.0)

ID	Criticality	Capability	Spec. Required
IF 3.1	1	The system shall provide an interface to support the following Functional Elements: Style Tools, Content Processing, Metadata, Preservation, Deposited, Harvested and Converted Content, Authentication, Persistent Name, Version Control, Search, Request, Cataloging and Reference Tools, Support, Content Delivery, Storage, Data Mining, Security, CO Ordering and Workflow.	Yes

3.2.14.6 User Support

3.2.14.6.1 User Support - General Features (US 1.0)

ID	Criticality	Capability	Spec. Required
US 1.1	1	The system shall provide context specific help on all user interfaces (e.g. help functions related to what is being viewed.)	Yes
US 1.2	1	The system shall provide users with the ability to opt-out of help features.	Yes
US 1.3	2	The system shall provide interactive user assistance.	Yes
US 1.4	1	The system shall provide multiple methods of contact for user assistance (e.g., web, phone, email, snail mail, chat).	Yes
US 1.5	3	The system shall provide online tutorials.	Yes
US 1.6	3	The system shall allow users to interact with subject matter experts.	Yes

3.2.14.6.2 User Support - User Preferences (US 2.0)

ID	Criticality	Capability	Spec. Required
US 2.1	1	The system shall provide the capability for authorized users to manage user preferences and queries.	Yes
US 2.2	2	The system shall provide recommendations for content and services based on preferences and queries of users and groups of similar users.	Yes
US 2.3	2	The system shall provide customized services for user classes and sub-groups within user classes as defined by GPO.	Yes

3.2.14.6.3 User Support - Help Desk and Knowledge Base (US 3.0)

ID	Criticality	Capability	Spec. Required
US 3.1	1	The system shall support a helpdesk.	Yes
US 3.2	2	The system shall allow authorized users to add information to a knowledge base.	Yes
US 3.3	2	The system shall have the ability to monitor the quality (e.g., did the contact result in successful resolution in a designated time frame?) of responses given by Helpdesk staff.	Yes
US 3.4	1	The system shall automatically confirm receipt of questions.	Yes
US 3.5	1	The system shall provide automated routing of inquiries to the departments/individuals according to workflow guidelines.	Yes

US 3.6	1	The system shall have the capacity to manage an unlimited number of user records.	Yes
US 3.7	1	The system shall allow authorized GPO users to search for and retrieve user contact information.	Yes
US 3.8	1	The system shall allow for search of user information.	Yes
US 3.9	1	The system shall allow for search of knowledge base.	Yes
US 3.10	3	The system shall provide users with access to history of their questions and answers.	Yes
US 3.11	3	The system shall provide users with access to questions and answers from other users related to their queries.	Yes
US 3.12	2	The system shall provide the capability to identify GPO users answering user questions. (e.g., name, department, function)	Yes
US 3.13	1	The system shall provide the capability to request user feedback.	Yes
US 3.14	1	The system shall provide the capability to alert designated users when user questions are submitted to the system.	Yes
US 3.15	1	The system shall provide the capability for alerts to be configurable by designated users.	Yes
US 3.16	2	The system shall provide the capability to perform records management functions on knowledge base data and user information.	Yes

3.2.14.6.4 User Support - Information Exchange (US 4.0)

ID	Criticality	Capability	Spec. Required
US 4.1	1	The system shall support the exchange of information between and among user classes.	Yes
US 4.1.1	2	The system shall support real-time, interactive information exchange (e.g., chat, discussion groups, web conferencing).	Yes
US 4.1.2	1	The system shall provide the capability to queue requests for information (e.g., "help me!" e-mail).	Yes
US 4.2	1	The system shall provide the capability to log information exchanges.	Yes
US 4.3	2	The system shall provide the capability to perform records management functions on information exchange logs.	Yes
US 4.4	1	The system shall have the capability to provide alert services which automatically deliver information about content based on user preferences.	Yes
US 4.4.1	1	The system shall allow users to subscribe and unsubscribe to alert services.	Yes
US 4.4.2	2	The system shall allow users to customize alert services.	Yes
US 4.4.3	2	The system shall provide alerts based on user profiles and history.	Yes

3.2.14.6.5 User Support - Training and Events (US 5.0)

ID	Criticality	Capability	Spec. Required
US 5.1	2	The system shall provide interactive training.	Yes
US 5.2	1	The system shall provide users access to training materials and training history.	Yes
US 5.3	1	The system shall allow users to enroll in training and events.	Yes
US 5.4	2	The system shall provide users verification of enrollment in training and events.	Yes
US 5.5	1	The system shall allow GPO users to manage training and events.	Yes
US 5.6	3	The system shall provide the capability for users to measure their progress and performance.	Yes
US 5.7	3	The system shall provide the capability for users to provide feedback.	Yes

3.2.14.6.6 User Support - Transactions and Reporting (Workflow) (US 6.0)

ID	Criticality	Capability	Spec. Required
US 6.1	1	The system shall provide the capability to automate logging and tracking of all types of incoming and outgoing communications (e.g., e-mail, faxes, telephone calls).	Yes
US 6.2	1	The system will support priority processing. (e.g., alerts, assignments to staff, nonstandard workflow, tracking, etc.)	Yes
US 6.3	1	The system shall provide the capability to create reports on user support activities.	Yes

3.2.14.7 Data Mining

3.2.14.7.1 Data Mining - Core Capabilities (DAM 1.0)

ID	Criticality	Capability	Spec. Required
DAM 1.1	1	The system shall be capable of extracting, analyzing and presenting data from Business Process Information (BPI).	Yes

3.2.14.7.2 Data Mining - Data Extraction (DAM 2.0)

ID	Criticality	Capability	Spec. Required
DAM 2.1	1	The system shall be able to extract from entire collection of BPI	Yes
DAM 2.2	1	The system shall be able to extract data in multiple formats (e.g. XML, PDF, XLS)	Yes
DAM 2.3	1	The system shall be able to extract data in a time-frame defined by GPO's business rules	Yes
DAM 2.4	1	The system shall be able to extract data using operator defined parameters	Yes
DAM 2.4.1	1	The system shall be able to extract random samples of data	

3.2.14.7.3 Data Mining - Data Presentation (DAM 3.0)

ID	Criticality	Capability	Spec. Required
DAM 3.1	1	The system shall be able to normalize data based on administrator defined parameters	Yes
DAM 3.1.1	1	The system shall be able to identify missing values or metadata	Yes

DAM 3.1.2	1	The system shall be able to identify and flag data anomalies	Yes
DAM 3.1.3	1	The system shall be able to identify data formats	Yes
DAM 3.1.4	1	The system shall be able to identify format discrepancies	Yes
DAM 3.1.5	1	The system shall be able to identify standard data elements	Yes
DAM 3.1.6	1	The system shall be able to identify data types	Yes
DAM 3.1.7	1	The system shall be able to identify content or field sizes	Yes
DAM 3.2	1	The system shall be able to merge and separate data sets based on administrator defined parameters (e.g. joining or separating fields, removing NULL values, string conversion of date data)	Yes

3.2.14.7.4 Data Mining - Analysis and Modeling (DAM 4.0)

ID	Criticality	Capability	Spec. Required
DAM 4.1	1	The system shall be able to perform analyses on BPI	Yes
DAM 4.1.1	1	The system shall be able to perform cross tabulations	Yes
DAM 4.1.2	1	The system shall be able to perform clusterization	Yes
DAM 4.1.3	1	The system shall be able to perform categorization	Yes
DAM 4.1.4	1	The system shall be able to perform association and link analyses	Yes
DAM 4.1.5	1	The system shall be able to perform regression analysis	Yes
DAM 4.1.6	3	The system shall be able to incorporate pre-defined taxonomies and ontologies	Yes

DAM 4.1.7	1	The system shall be able to expose hierarchical or parent/child relationships	Yes
DAM 4.1.8	1	The system shall be able to expose sequential relationships and patterns	Yes
DAM 4.1.9	1	The system shall be able to expose temporal relationships and patterns	Yes
DAM 4.1.10	1	The system shall be able to expose inferences and rules that led to a result set	Yes
DAM 4.1.11	1	The system shall be able to prevent processing of illogical operations, e.g. calculating averages out of categorical data	Yes
DAM 4.1.12	1	The system shall be able to filter data at different levels of granularity	Yes
DAM 4.2	1	The system shall allow user input while analysis is in progress	Yes
DAM 4.3	2	The system shall have ability to create customizable reports for analysis of search terms and search success/failure.	Yes

3.2.14.7.5 Data Mining - Presentation and Interface (DAM 5.0)

ID	Criticality	Capability	Spec. Required
DAM 5.1	1	The system shall allow differentiated views based on access levels	Yes
DAM 5.2	2	The system shall allow for different views of data based on user preferences	Yes
DAM 5.2.1	2	The system shall present graphic models of data	Yes
DAM 5.3	1	The system shall be able to produce reports (e.g., trend analysis, usage patterns)	Yes
DAM 5.4	2	The system shall be able to send alerts or notifications to GPO users based on defined criteria	Yes

DAM 5.5	1	The system shall be able to link analysis results to data	Yes
DAM 5.6	1	The system shall enable GPO users to define permissions to view/modify output based on access rights	Yes
DAM 5.7	1	The system shall be able to expose analysis criteria and algorithms	Yes
DAM 5.8	1	The system shall be able to export results	Yes

3.2.14.7.6 Data Mining - Security and Administration (DAM 6.0)

ID	Criticality	Capability	Spec. Required
DAM 6.1	1	The system shall allow access to BPI based on permissions and access rights	Yes
DAM 6.2	1	The system shall log transactions	
DAM 6.3	1	The system shall allow for data mining to create metadata.	

3.2.14.7.7 Data Mining – Storage (DAM 7.0)

ID	Criticality	Capability	Spec. Required
DAM 7.1	1	The system shall store extracted data	
DAM 7.2	1	The system shall store reports, report templates, analysis criteria and algorithms	Yes
DAM 7.2.1	1	The system shall have a records management process (e.g., delete files and reports at a defined time)	Yes

3.2.15 Preservation Services

3.2.15.1 Preservation - Core Functionality (PRE 1.0)

ID	Criticality	Capability	Spec. Required
PRE 1.1	1	The system shall have the ability to preserve AIPs	
PRE 1.2	1	The system shall manage preservation processes (e.g., set of activities to keep content alive)	Yes
PRE 1.3	1	The system shall maintain the integrity of content throughout preservation processes	Yes
PRE 1.4	1	The system shall preserve all essential behaviors of digital content	Yes
PRE 1.4.1	1	The system shall maintain content functionality	Yes
PRE 1.4.2	1	The system shall support content presentation	Yes
PRE 1.5	1	The system shall preserve all significant properties and attributes of digital content	Yes
PRE 1.5.1	1	The system shall maintain content context	Yes
PRE 1.5.2	1	The system shall maintain content structure	Yes

3.2.15.2 Preservation - Preservation Processes (PRE 2.0)

ID	Criticality	Capability	Spec. Required
PRE 2.1	1	The system shall have the ability to faithfully reproduce digital files in formats other than those in which the files were created or received	Yes
PRE 2.1.1	1	The system shall assure that the files resulting from such conversion will be in a format free of proprietary restrictions	Yes

PRE 2.1.2	1	The system shall have the ability to verify that a file converted from one fomat to another retains specified attributes and behaviors (ie. is authentic and faithful)	Yes
PRE 2.1.3	1	The system shall provide logs that record the results of conversions	Yes
PRE 2.1.4	1	The system shall have the ability to produce notification of incomplete or unsuccessful conversion	Yes
PRE 2.2	1	The system shall have the ability to preserve files in their native or received form by refreshment of files (e.g., media, veracity, etc.)	Yes
PRE 2.3	1	The system shall have the ability to support emulation to preserve access to content package	Yes
PRE 2.4	1	The system shall manage archival information packages defined in Preservation Standards	Yes

3.2.15.3 Preservation – Assessment (PRE 3.0)

ID	Criticality	Capability	Spec. Required
PRE 3.1	1	The system shall assess ingested content for preservation	Yes
PRE 3.2	1	The system shall have the ability to re-assess content stored in the system	
PRE 3.3	1	The system shall have the ability to determine preservation actions based on preservation assessments	

3.2.15.4 Preservation – Administration (PRE 4.0)

ID	Criticality	Capability	Spec. Required
PRE 4.1	1	The system shall support scheduling the automatic execution of preservation processes	
PRE 4.2	1	The system shall support batch preservation processing of content	
PRE 4.3	1	The system shall support preservation processing on an item-by-item basis	
PRE 4.4	1	The system shall maintain an audit trail of preservation processes associated with content	

3.2.15.5 Preservation – Storage (PRE 5.0)

ID	Criticality	Capability	Spec. Required
PRE 5.1	1	The system shall provide a digital archival repository environment which is based on open-standards architecture	
PRE 5.1.1	1	The repository environment shall keep archival information packages separate from working or production copies or versions which support end user access	

3.2.15.6 Preservation – Metadata (PRE 6.0)

ID	Criticality	Capability	Spec. Required
PRE 6.1	1	The system shall capture information documenting all preservation processes	
PRE 6.2	1	The system shall capture or generate metadata which specifies the relationship of files resulting from preservation processes to their predecessors	Yes
PRE 6.3	1	The system shall employ metadata for preservation which is compliant with the emerging standard developed by the PREMIS working group	Yes
PRE 6.3.1	1	The system shall employ schema for facilitating preservation metadata processes compliant with those developed by the PREMIS working group	Yes

3.2.15.7 Preservation – Security (PRE 7.0)

ID	Criticality	Capability	Spec. Required
PRE 7.1	1	The system shall enable varying levels of access to preserved objects; e.g. limiting access to authorized user classes, or denying or restoring access to security-restricted content.	Yes

3.2.16 Content Delivery - Core Capabilities (CD 1.0)

ID	Criticality	Capability	Spec. Required
CD 1.1	1	The system shall retrieve ACPs from access storage based on user request.	
CD 1.2	1	The system shall transform a copy of a user requested ACP into a DIP.	Yes
CD 1.2.1	1	The system shall transform ACPs in content processing.	Yes
CD 1.2.2	1	The system shall create DIPs containing the digital object and packaging metadata for dissemination.	
CD 1.2.3	1	The system shall transform ACPs into DIPs based on user preferences.	
CD 1.3	1	The system shall deliver DIPs based on user requests.	
CD 1.3.1	1	The system shall deliver DIPs in a timeframe based on user requirements and GPO business rules.	
CD 1.4	1	The system shall have the capability to deliver DIPs to all users.	
CD 1.5	1	The system shall have the capability to deliver integrity marks associated with content in a delivered DIP.	Yes
CD 1.5.1	1	The system shall have the capability to include integrity marks with content delivered for electronic presentation.	Yes
CD 1.5.2	1	The system shall have the capability to apply integrity marks to content delivered as hard copy (e.g., watermarks).	Yes
CD 1.6	1	The system shall have the capability to provide notification of delivery to the user.	

CD 1.6.1	1	The system shall have the capability to provide users with options in response to undelivered content (e.g., resubmit content, cancel delivery).	Yes
CD 1.7	1	The system shall have the capability to provide GPO with confirmation of delivery.	
CD 1.8	1	The system shall use metadata to determine if requested delivery is possible.	

3.2.16.1 Content Delivery - Service Provider Information (CD 2.0)

ID	Criticality	Capability	Spec. Required
CD 2.1	1	The system shall maintain information about service providers.	
CD 2.2	1	The system shall maintain Service Provider profile information (e.g., equipment, capabilities).	Yes
CD 2.2.1	1	The system shall maintain Service Provider performance information (e.g., quality data, performance data).	Yes
CD 2.3	1	The system shall provide the capability for users to specify service providers.	Yes
CD 2.4	1	The system shall provide the capability for users to select service providers.	Yes
CD 2.4.1	1	The system shall allow content originators and users to select a service provider based on user requirements.	
CD 2.5	1	The system shall provide the capability for Service Providers to manage their business profile (e.g., equipment, capabilities, staffing).	Yes

CD 2.6	1	The system shall allow authorized GPO users to manage Service Provider performance information (e.g., quality data, performance data).	Yes
CD 2.7	1	The system shall provide the capability to access Service Provider databases (e.g., current workload, inventory, profile information).	

3.2.16.2 Content Delivery – Workflow (CD 3.0)

ID	Criticality	Capability	Spec. Required
CD 3.1	1	The system shall provide the capability to query Service Providers for job status (e.g., tracking of orders).	Yes
CD 3.2	1	The system shall have the capability to log activities with Service Providers (e.g., job received by the Service Provider, job complete, job fulfillment).	

3.2.16.3 Content Delivery – Standards (CD 4.0)

ID	Criticality	Capability	Spec. Required
CD 4.1	1	The system shall comply with GPO Quality Assurance standards for content delivery (to be developed).	Yes
CD 4.2	1	The system shall comply with best practices and guidelines regarding usability for electronic content (e.g., The Research-Based Web Design & Usability Guidelines function as best practices for Federal Agencies).	Yes
CD 4.3	1	The system shall ensure that DIPs comply with accessibility laws and regulations (e.g., Section 508 of the Rehabilitation Act Amendments of 1998).	Yes

CD 4.4	1	The system shall comply with W3C guidelines.	
CD 4.5	1	The system shall have the capability to comply with ICGI recommendations.	

3.2.17 Hard Copy Output (HC 1.0)

ID	Criticality	Capability	Spec. Required
HC 1.1	1	The system shall have the capability to deliver DIPs to service providers from which hard copy output can be created.	Yes
HC 1.2	1	The system shall support hard copy production by internal and external service providers.	
HC 1.2.1	1	The system shall support the production of hard copy on any available hard copy output technology (e.g., offset press, digital printing).	Yes
HC 1.3	1	The system shall support the production of hard copy output that conforms to GPO-specificed standards (e.g., standard trim sizes, paper types, binding as depicted in JCP regulations).	Yes
HC 1.4	1	The system shall conform to GPO quality assurance standards for the creation of hard copy output.	Yes
HC 1.4.1	1	The system shall conform to GPO quality assurance standards for traditional printing.	Yes
HC 1.4.2	1	The system shall conform to GPO quality assurance standards for digital printing.	Yes
HC 1.5	1	The system shall have the capability to deliver hard copy output to users in timeframes according to user needs and GPO business rules.	Yes

HC 1.6	1	The system shall provide the capability to support multiple hard copy fulfillment options (e.g., customer pick-up, same day, next day, 2-day).	
HC 1.6.1	1	The system shall allow users to choose a fulfillment option for hard copy output.	
HC 1.7	1	The system shall provide the capability to provide confirmation of hard copy output fulfillment to the user and GPO.	
HC 1.8	1	The system shall provide the capability to determine the most cost-effective method for hard copy output (e.g., offset press, digital printing)	Yes

3.2.18 Electronic Presentation

3.2.18.1 Electronic Presentation - Core Capabilities (EP 1.0)

ID	Criticality	Capability	Spec. Required
EP 1.1	1	The system shall have the capability to render content for presentation on end user devices.	Yes
EP 1.1.1	1	The system shall have the capability to render content for presentation on multiple computer platforms (e.g., Windows, Mac, UNIX).	Yes
EP 1.1.2	1	The system shall have the capability to render content for presentation on non-desktop electronic devices (e.g., PDA, MP3 players, e-books).	Yes
EP 1.2	1	The system shall provide the capability to deliver DIPs that support static and dynamic text.	
EP 1.3	1	The system shall provide the capability to deliver DIPs that support static and dynamic images.	

EP 1.4	1	The system shall provide the capability to deliver DIPs that support audio information.	
EP 1.5	1	The system shall provide the capability to deliver DIPs that support visual information.	
EP 1.6	1	The system shall have the capability to present the integrity mark to the user.	
EP 1.7	1	The system shall provide the capability to encode content in open formats, wherever possible.	Yes
EP 1.7.1		The system shall deliver electronic content in XML.	
EP 1.7.2		The system shall deliver electronic content in JPG.	
EP 1.7.3		The system shall deliver electronic content in TIFF.	
EP 1.7.4		The system shall deliver electronic content in GIF.	
EP 1.7.5		The system shall deliver electronic content in EPS.	
EP 1.7.6		The system shall deliver electronic content in SVG.	
EP 1.7.7		The system shall deliver electronic content in MPEG.	
EP 1.7.8		The system shall deliver electronic content in ASCII text.	
EP 1.7.9		The system shall deliver electronic content in HTML/XHTML.	
EP 1.8	1	The system shall deliver electronic content that maintains desired user functionality (e.g., links, bookmarking).	Yes
EP 1.9	1	The system shall have the capability to deliver content in proprietary formats in accordance with GPO business rules responding to user need.	Yes

EP 1.9.1		The system may deliver electronic content in MS Office formats.	
EP 1.9.2		The system may deliver electronic content in PDF.	

3.2.19 Digital Media

3.2.19.1 Digital Media - Overall (DM 1.0)

ID	Criticality	Capability	Spec. Required
DM 1.1	1	The system shall have the capability to deliver DIPs to users via digital media (e.g., CDs, DVDs).	Yes
DM 1.2	1	The system shall have the capability to deliver DIPs to digital media (e.g., devices external to the system).	Yes
DM 1.2.1	1	The system shall have the capability to deliver DIPs to non-GPO storage devices (e.g., customer servers).	Yes
DM 1.2.2	1	The system shall have the capability to deliver DIPs to non-GPO multifunctional devices (e.g., PDAs, MP3 players, e-books).	Yes

3.2.19.2 Digital Media - Data Storage Devices (CDs, DVDs) (DM 2.0)

ID	Criticality	Capability	Spec. Required
DM 2.1	1	The system shall encode data based on industry standards (e.g., ISO and NISO Standards, Redbook).	Yes

3.2.19.3 Digital Media - Delivery Mechanisms (DM 3.0)

ID	Criticality	Capability	Spec. Required
DM 3.1	1	The system shall have the capability to deliver electronic content utilizing various methods.	
DM 3.2	1	The system shall have the capability to automatically push content to users (e.g., RSS feeds, e-mail, raw data feeds).	Yes
DM 3.3	1	The system shall provide the capability for users to pull content from the system (e.g., FTP).	Yes
DM 3.4	1	The system shall allow GPO and end users to schedule deliveries of content.	
DM 3.5	1	The system shall have the capability to provide users with estimated transfer time.	

3.2.20 Workflow

3.2.20.1 Workflow - Core Capabilities (WF 1.0)

ID	Criticality	Capability	Spec. Required
WF 1.1	1	The system shall provide the capability to define workflows	Yes
WF 1.2	1	The system shall provide the capability to create new versions of existing workflows.	Yes
WF 1.3	1	The system shall provide the capability to test new versions of existing workflows.	Yes
WF 1.4	1	The system shall provide the capability to place new versions of workflows into production.	Yes

WF 1.5	1	The system shall provide the capability to replace current versions of workflows with previous versions when required.	Yes
WF 1.6	1	The system shall provide the capability to modify workflows	Yes
WF 1.7	1	The system shall provide the capability to define business rules	Yes
WF 1.8	1	The system shall provide the capability to define manual activities	Yes
WF 1.9	1	The system shall provide the capability to define automated activities	Yes
WF 1.10	1	The system shall provide the capability to define work lists of activities	Yes
WF 1.11	1	The system shall provide the capability to express all logs in metadata	Yes

3.2.20.2 Workflow - Messaging and Notification (WF 2.0)

ID	Criticality	Capability	Spec. Required
WF 2.1	1	The system shall provide the capability to support messaging capabilities of the workflows	Yes
WF 2.2	1	The system shall provide the capability to associate notifications with workflows	Yes
WF 2.3	1	The system shall provide the capability to change notifications attached to workflows	Yes
WF 2.4	1	The system shall provide the capability to delete notifications attached to workflows	Yes
WF 2.5	1	The system shall send notification to GPO operations	Yes

5.4.1.3 Workflow - Resource Requirements (WF 3.0)

ID	Criticality	Capability	Spec. Required
WF 3.1	1	The system shall provide the capability to estimate resource requirements associated with internal workflow	Yes
WF 3.2	1	The system shall provide the capability to estimate resource requirements associated with external workflow	Yes
WF 3.3	1	The system shall provide the capability to make estimated resource requirements associated with a workflow available to other external systems	Yes
WF 3.4	1	The system shall provide the capability to make estimated resource requirements associated with a workflow available to internal systems	Yes
WF 3.5	2	The system shall provide the capability to support defining timeframes for completion of activities performed (this could prove useful for highly visibility documents)	Yes

3.2.20.4 Workflow - Definition Tool (WF 4.0)

ID	Criticality	Capability	Spec. Required
WF 4.1	1	The Workflow definition function shall provide the capability to support a standard language / tool	Yes
WF 4.2	1	The Workflow definition tool shall provide the capability to support a Graphical User Interface (GUI) to define new and modify current or previous Workflows	Yes

WF 4.3	1	The Workflow definition tool shall provide the capability to support interoperability between Workflows within the system	Yes
WF 4.4	1	The Workflow definition tool shall provide the capability to validate Workflow throughout the process	Yes
WF 4.5	1	The Workflow definition tool shall provide the capability to test new workflow versions in a test environment.	Yes

3.2.20.5 Workflow - Control of Execution (WF 5.0)

ID	Criticality	Capability	Spec. Required
WF 5.1	1	The system shall provide the capability to sequence jobs to optimize operations	Yes
WF 5.2	1	The system shall provide the capability to sequence activities to optimize operations	Yes
WF 5.3	1	The system shall provide the capability to dynamically manipulate workflows	Yes
WF 5.4	1	The system shall provide the capability to create work lists of jobs	Yes
WF 5.5	1	The system shall provide the capability to remove jobs from work lists	Yes
WF 5.6	1	The system shall provide the capability to schedule for manual activities	Yes
WF 5.7	1	The system shall provide the capability to assign human resources to manual activities	Yes
WF 5.8	1	The system shall provide the capability to suspend jobs	Yes
WF 5.9	1	The system shall provide the capability to suspend activities	Yes

WF 5.10	1	The system shall provide the capability to resume activities	Yes
WF 5.11	1	The system shall provide the capability to resume a suspended job	Yes
WF 5.12	1	The system shall provide the capability to cancel a job	Yes
WF 5.13	1	The system shall provide the capability to manually adjust the priority of a job	Yes
WF 5.14	1	The system shall provide the capability to dynamically adjust the priority of a job	Yes

3.2.20.6 Workflow – Interoperability (WF 6.0)

ID	Criticality	Capability	Spec. Required
WF 6.1	1	The system shall provide the capability to interact / interoperate with applications working in different platforms within the system.	Yes

3.2.20.7 Workflow – Monitoring (WF 7.0)

ID	Criticality	Capability	Spec. Required
WF 7.1	1	The system shall provide the capability to monitor system workflow	Yes
WF 7.2	1	The system shall provide the capability for users to monitor jobs.	Yes
WF 7.3	1	The system shall provide the capability for users to monitor process work lists.	Yes
WF 7.4	1	The system shall provide the capability for users to monitor activity work lists.	Yes

WF 7.5	1	The system shall provide the capability for users to monitor one or more activity work lists	Yes
WF 7.6	1	The system shall provide the capability for users to monitor one or more process work lists	Yes
WF 7.7	1	The system shall provide the capability to monitor planned, scheduled and actual times for selected activity work lists	Yes
WF 7.8	1	The system shall provide the capability to monitor planned, scheduled and actual times for selected process work lists	Yes

3.2.20.8 Workflow – History (WF 8.0)

ID	Criticality	Capability	Spec. Required
WF 8.1	1	The system shall provide the capability for users to monitor processing history	Yes
WF 8.2	2	The system shall provide the capability for users to monitor processing history over a specified time period	Yes

3.2.20.9 Workflow – Notification (WF 9.0)

ID	Criticality	Capability	Spec. Required
WF 9.1	1	The system shall provide the capability to notify users when workflow process conditions have been met.	Yes
WF 9.2	1	The system shall provide the capability to monitor notifications and messages for selected activity work lists	Yes

WF 9.3	1	The system shall provide the capability to monitor notifications and messages for selected process work lists	Yes

3.2.20.10 Workflow – Status (WF 10.0)

ID	Criticality	Capability	Spec. Required
WF 10.1	2	The system shall provide the capability to group process workflow work list with a defined status	Yes
WF 10.2	2	The system shall provide the capability to group activity work lists with a defined status	Yes

3.2.20.11 Workflow - Monitoring Tool (WF 11.0)

ID	Criticality	Capability	Spec. Required
WF 11.1	1	All Workflow monitoring capabilities must be available through a Monitoring Tool containing a Graphical User Interface (GUI)	Yes
WF 11.2	1	The Monitoring Tool shall provide the capability for the user to Customize views	Yes
WF 11.3	1	The Monitoring Tool shall provide the capability to save Customized views for future use	Yes

3.2.20.12 Workflow – Security (WF 12.0)

ID	Criticality	Capability	Spec. Required
WF 12.1	1	The system shall provide the capability to have security controls on workflow activities	Yes

3.2.21 Storage Management

3.2.21.1 Functional Data Storage (STO 1.0)

ID	Criticality	Capability	Spec. Required
STO 1.1	1	Pre-Ingest WIP Store	
STO 1.1.1	1	Pre-Ingest WIP Store shall contain high access, Networked High Performance Storage for CO and GPO users	
STO 1.1.2	1	Pre-Ingest WIP Store shall contain Mid-term Archival Storage	
STO 1.1.3	1	Pre-Ingest WIP Store shall contain Failover Storage	
STO 1.1.4	1	Pre-Ingest WIP Store shall contain Back-up Retrieval Media Storage	
STO 1.2	1	Archival Information Package (AIP) Storage	
STO 1.2.1	1	The AIP Storage shall exist in isolation from other system stores	
STO 1.2.2	1	AIP Storage shall contain high access, Networked Moderate Performance Storage for GPO users	
STO 1.2.3	1	AIP Storage shall contain Long-term Permanent Archival Storage	
STO 1.2.4	1	AIP Storage shall contain Failover Storage	
STO 1.2.5	1	AIP Storage shall contain Back-up Retrieval Media Storage	

STO 1.3	1	Access Content Storage (ACS)
STO 1.3.1	1	ACS Storage Store shall contain high access, Networked High Performance Storage GPO users and Access Users
STO 1.3.2	1	ACS Storage Store shall contain high access, Networked Moderate Performance Storage for GPO users and Access Users
STO 1.3.3	2	ACS Storage Store shall contain Low Criticality - Low Cost Storage for GPO users and Access Users
STO 1.3.4	1	ACS Storage Store shall contain Mid-term Archival Storage
STO 1.3.5	2	ACS Storage shall contain Long-term Permanent Archival Storage
STO 1.3.6	1	ACS Storage Store shall contain Failover Storage
STO 1.3.7	1	ACS Storage Store shall contain Back-up Retrieval Media Storage
STO 1.4	1	Content Process Storage (CPS)
STO 1.4.1	1	CPS Storage shall contain high access, Networked High Performance Storage GPO users
STO 1.4.2	1	CPS Storage shall contain Failover Storage
STO 1.4.3	1	CPS Storage shall contain Back-up Retrieval Media Storage
STO 1.5	1	Business Process Storage (BPS)
STO 1.5.1	1	BPS Storage Store shall contain high access, Networked High Performance Storage GPO users and Access Users
STO 1.5.2	1	BPS Storage Store shall contain high access, Networked Moderate Performance Storage for GPO users and Access Users
STO 1.5.3	2	BPS Storage Store shall contain Low Criticality - Low Cost Storage for GPO users and Access Users

STO 1.5.4	1	BPS Storage Store shall contain Mid-term Archival Storage	
STO 1.5.5	1	BPS Storage shall contain Long-term Permanent Archival Storage	
STO 1.5.6	1	BPS Storage Store shall contain Failover Storage	
STO 1.5.7	1	BPS Storage Store shall contain Back-up Retrieval Media Storage	

3.2.21.2 Storage System Standards (STO 2.0)

ID	Criticality	Capability	Spec. Required
STO 2.1	1	The system storage shall integrate with Unix and Windows based Directory Services (LDAP, AD), and role based access.	Yes
STO 2.2	1	The system storage shall support multiple file systems to include but not limited to: Windows XP Filesystem, Linux File System, SunOS File System, Solaris Filesystem, Apple, FAT, FAT32, VFAT, NTFS, HPFS, EXT2,	Yes
STO 2.3	1	The system storage shall utilize common Redundant Array of Independent Disks (RAID) Disk Data Format (DDF) architecture	Yes
STO 2.4	1	The system storage shall conform to common protocols: Apple File Protocol (AFP), Network File System (NFS), SMB and CIFS protocols, Simple Network Management Protocol (SNMP), Internet Small Computer Systems Interface (iSCSI), Internet Fibre Channel Protocol (iFCP), Fibre Channel over IP (FCIP),Serial across SCSI (SAS), and Serial ATA	Yes

STO 2.5	1	The system storage shall allow interaction with management information bases (MIB) via SNMP, must conform to or interoperate within Object-based Storage Device (OSD) specification	Yes
STO 2.6	1	The system storage shall support ANSI INCITS 388-2004 Storage Management Initiative Specification	Yes
STO 2.7	3	The system back-up tapes shall conform to Linear Tape-Open (LTO) standard	Yes

3.2.21.3 Operational Stores (STO 3.0)

ID	Criticality	Capability	Spec. Required
STO 3.1	1	Networked High Performance Storage	
STO 3.1.1	1	Networked High Performance Storage shall have the ability to store data dynamically in high performance-high availability stores and External Content Delivery Networks based on hit rate/criticality of content	Yes
STO 3.1.2	2	Content Delivery Network (CDN) shall have assured delivery through a global network	Yes
STO 3.1.3	1	CDN shall have security mechanisms to ensure no malicious code is imbedded in GPO content	Yes
STO 3.1.4	2	Networked High Performance Storage shall have the capability to support direct application access with latency in application performance less than 1 sec	Yes
STO 3.1.5	1	Networked High Performance Storage shall be able to support automated fail-over without buffer application data loss.	Yes

STO 3.1.6	1	Networked High Performance Storage shall operate reliably to allow less than 0.1% downtime	Yes
STO 3.1.7	1	Networked High Performance Storage shall have record management capabilities	Yes
STO 3.1.8	1	Networked High Performance Storage shall have redundant components that will take over in the event of a hardware failure in the primary part.	Yes
STO 3.1.9	2	Networked High Performance Storage System shall be able to support hot-spare standby drives (e.g. extra drives installed in the disk array that automatically come online in the event of a disk failure)	Yes
STO 3.1.10	2	Networked High Performance Storage shall have a full-system battery backup to allow the disk array to remain operational in the event of a power.	Yes
STO 3.2	1	Networked Moderate Performance Storage	
STO 3.2.1	2	Networked Moderate Performance Storage shall support static and dynamic storage assignment	Yes
STO 3.2.2	1	Networked Moderate Performance Storage shall have limited scalability (e.g., multi- tens of terabyte capacities)	Yes
STO 3.2.3	1	Networked Moderate Performance Storage shall have open support (control of its resources) for a consolidated storage management back plane	Yes
STO 3.2.4	2	Networked Moderate Performance Storage shall operate Reliably to allow less than .2% Downtime	Yes

STO 3.2.5	2	Networked Moderate Performance Storage shall have the capability to support direct application access with latency in application performance less than 3 sec	Yes
STO 3.3	2	Low Criticality - Low Cost Storage	
STO 3.3.1	2	Low Criticality - Low Cost Storage shall support low cost devices (e.g., Serial ATA storage drives)	Yes
STO 3.3.2	2	Low Criticality - Low Cost Storage shall allow central control and allocation of storage resources.	Yes
STO 3.3.3	2	Low Criticality - Low Cost Storage shall allow RAID 0 thru 5 configurations	Yes
STO 3.3.4	2	Low Criticality - Low Cost Storage shall allow scaling and partitioning	Yes
STO 3.3.5	2	Low Criticality - Low Cost Storage shall operate reliably with less than .3% downtime	Yes

3.2.21.4 Contingency Stores (STO 4.0)

ID	Criticality	Capability	Spec. Required
STO 4.1	1	Failover Storage	
STO 4.1.1	1	Failover Storage system shall have a fault tolerance-system able to survive local environmental casualties	Yes
STO 4.1.2	1	Failover Storage system shall be able to reconstitute and switch-over to alternate systems at a remote site in the event of local catastrophic damage	Yes
STO 4.1.3	1	Failover Storage system shall have a remote storage site over 50 miles from the main GPO facility	Yes
STO 4.1.4	2	Failover Storage system shall allow RAID 0 thru 5 configurations	Yes

STO 4.1.5	1	Failover Storage system shall support alternate pathing. (e.g., ability to automatically switch between input/output (I/O) paths in the event of a failure in one of the paths.)	Yes
STO 4.2	1	Back-up Retrieval Media Storage	
STO 4.2.1	2	The Back-up Retrieval Media Storage system shall be able to accomplish periodic backup on mass removable storage media	Yes
STO 4.2.2	1	The Back-up Retrieval Media Storage system shall be able to accomplish a full back-up of all critical data in less than six hours or in a step-wise scheduled fashion over 24 hours	Yes
STO 4.2.3	1	The Back-up Retrieval Media Storage system shall be over 50 miles from the main GPO facility	Yes
STO 4.2.4	1	The Back-up Retrieval Media Storage system shall allow reconstitution of GPO Applications and data within 48 hours at an alternate work site	Yes
STO 4.2.5	2	The Back-up Retrieval Media Storage system shall have battery backed-up cache (e.g., battery power that protects any data that happens to be in cache at the time of a power interruption).	Yes
STO 4.2.6	2	The Back-up Retrieval Media Storage system shall support mirrored cache (e.g., the process of mirroring the write data in cache as a further method of data protection).	Yes
STO 4.2.7	2	The Back-up Retrieval Media Storage system shall have cache or disk scrubbing (e.g., a method of proactively testing data for errors even when the cache or disk is inactive, so that problems can be detected before they can disrupt data flow).	Yes

STO 4.2.8	2	Storage System must be able to support remote mirroring, or the process of copying data to a second disk array, often housed in a separate location from the originating disk array.	Yes

3.2.21.5 Archival Stores (STO 5.0)

ID	Criticality	Capability	Spec. Required
STO 5.1	1	Mid-term Archival Storage	
STO 5.1.1	1	Mid-term Archival Storage shall have off-line storage and indexing capability for 100's of Terabytes of data	Yes
STO 5.1.2	1	Mid-term Archival Storage shall preserve data integrity and quality for no less than 10 Years in a data center environment	Yes
STO 5.1.3	2	Mid-term Archival Storage shall support error-free retrieval of data to network storage at rated network speeds (e.g., 2 Gbps).	Yes
STO 5.2	1	Long-term Permanent Archival Storage	
STO 5.2.1	1	Long-term Permanent Archival Storage shall have off-line storage and indexing capability for multiple Petabytes of data	Yes
STO 5.2.2	1	Long-term Permanent Storage shall support error-free retrieval of data to network storage at network speeds (e.g., 2 Gbps).	Yes
STO 5.2.3	1	Long-term Permanent Storage Archival storage site must be remote from the main GPO facility	Yes

STO 5.2.4	1	Storage must preserve data integrity and quality for no less than 100 Years under controlled storage conditions (e.g., 70° F, 60% Humidity) without preservation processes being performed	Yes

3.2.21.6 Storage Management (STO 6.0)

ID	Criticality	Capability	Spec. Required
STO 6.1	1	Monitoring	
STO 6.1.1	1	Storage shall have capability to be monitored for real-time health of the system components	Yes
STO 6.1.2	2	Monitoring shall have capability to have conditional thresholds customized to allow timely preventative maintenance	Yes
STO 6.1.3	1	The system shall have the ability to send alerts to GPO users via multiple channels should a performance problem, failure condition or impending failure be detected	Yes
STO 6.1.4	1	The system shall have the capability to monitor real-time performance of the system in terms of service levels.	Yes
STO 6.1.5	1	The system shall have the ability to monitor data access history and evaluate appropriate storage in terms of cost and performance	Yes
STO 6.1.6	1	The system shall have the ability to monitor health of externally hosted data stores	Yes
STO 6.1.7	2	The system shall support user configurable RAID levels. (e.g., the ability to configure storage RAID levels in the field without vendor intervention).	Yes
STO 6.2	1	Preventative Action	

STO 6.2.1	1	Storage shall have the ability to have automated preventative actions configured to allow critical failures from causing data loss.	Yes
STO 6.2.2	2	The Storage system shall have the ability to allow hot swapping of components should a failure condition be detected.	Yes
STO 6.2.3	1	The Storage system shall have the ability to dynamically move data to improve system performance	Yes
STO 6.2.4	2	The Storage system shall be able to execute non-disruptive microcode updates or replacements or the ability to update or replace the RAID controller microcode without having to shut down the disk array.	Yes
STO 6.3	1	Data Integrity	
STO 6.3.1	2	The Storage system shall allow for securing of partitions	Yes
STO 6.3.2	2	The Storage system shall allow encryption of logical content	Yes
STO 6.3.3	1	The Storage system shall have the capability to limit access to data via role-based security	Yes
STO 6.4	1	Allocation	
STO 6.4.1	2	The Storage system shall support the management of heterogenous storage architectures (e.g. direct attached storage (DAS), network attached storage (NAS), storage area network (SAN))	Yes
STO 6.4.2	1	The Storage system shall have capability to have conditional threshholds customized to allow automated reallocation of storage to meet application needs	Yes
STO 6.4.3	2	The Storage system shall be able to allocate any compliant serial drive, and near-line storage devices.	Yes

STO 6.4.4	2	The Storage system shall allow automated compression of data to vary infrequently accessed content the system requires	Yes
STO 6.4.5	1	The Storage system shall be able to immediately allocate newly added storage assets	Yes

3.2.22 Security

3.2.22.1 Security - System User Authentication (SEC 1.0)

ID	Criticality	Capability	Spec. Required
SEC 1.1	1	The system shall have the capability to support identification of users through the provision of a claimed identity (e.g., user idenitity) to the system.	Yes
SEC 1.1.1	1	The system shall have the capability to authenticate users based on a unique user identity.	Yes
SEC 1.1.2	1	The system shall authenticate system and security administrators.	Yes
SEC 1.2	1	The system shall permit users to create a unique user identity for access to the system	Yes

3.2.22.2 Security - User Access Control (SEC 2.0)

ID	Criticality	Capability	Spec. Required
SEC 2.1	1	The system shall have the capability to arbitrate access based on a role-based access model driven by policy.	Yes
SEC 2.2	1	The system shall have secure interfaces for transaction processing (e.g., to facilitate electronic ordering)	Yes

SEC 2.3	1	The system shall provide a means to ensure that users cannot view or modify information of other users unless authorized.	Yes
SEC 2.4	1	The system shall securely store personal information (e.g. user names and passwords)	Yes
SEC 2.5	1	The system shall provide the capability for authorized users to manage (add, modify, delete) information.	Yes

3.2.22.3 Security - Capture and Analysis of Audit Logs (SEC 3.0)

ID	Criticality	Capability	Spec. Required
SEC 3.1	1	The system shall keep an audit log of all transactions in the system	Yes
SEC 3.1.1	1	The system shall the capability to reconstruct complete transactions in event there is a need to investigate the validity and integrity of user transactions	Yes
SEC 3.1.2	1	The system shall keep an store audit logs (e.g., audit trails) and utilize records management processes on these stores	Yes
SEC 3.1.3	1	The system shall keep an audit log of system administration transactions	Yes
SEC 3.1.4	1	The system shall keep an audit log of security administrator transactions	Yes
SEC 3.1.5	1	The system shall keep an audit log of system access rights	Yes
SEC 3.1.6	1	The system shall keep an audit log of Deposited, Harvested and Converted Content activities	Yes
SEC 3.1.7	1	The system shall keep an audit log of CO Ordering activities	Yes
SEC 3.1.8	1	The system shall keep an audit log of Content Authentication activities	Yes

SEC 3.1.9	1	The system shall keep an audit log of Version Control activities	Yes
SEC 3.1.10	1	The system shall keep an audit log of Cataloging activities	Yes
SEC 3.1.11	1	The system shall keep an audit log of Support activities (e.g., support status)	Yes
SEC 3.2	1	The system shall have the capability to maintain integrity of audit logs	Yes
SEC 3.3	1	The system shall keep an audit log of attempts to access the system.	Yes
SEC 3.3.1	1	The system shall keep an audit log of any detected breaches of security policy	Yes

3.2.22.4 Security - User Privacy (SEC 4.0)

ID	Criticality	Capability	Spec. Required
SEC 4.1	1	The system shall provide the capability conform to GPO's privacy policy and Federal privacy laws and regulations	Yes
SEC 4.1.1	1	The system shall provide the capability of maintaining Access privacy (e.g., Search, Request)	Yes
SEC 4.1.2	1	The system shall provide the capability of maintaining Support privacy (e.g., user identity)	Yes
SEC 4.1.3	1	The system shall provide the capability of maintaining CO Ordering privacy	Yes

3.2.22.5 Security – Confidentiality (SEC 5.0)

ID	Criticality	Capability	Spec. Required
SEC 5.1	1	The system shall provide the capability of maintaining confidentiality of user data (e.g., passwords)	Yes
SEC 5.1.1	1	The system shall have the capability to provide confidentiality of user data, including user authentication data exchanged through external interfaces	Yes
SEC 5.1.2	1	The system shall have the capability to provide confidentiality of user data, including user authentication data stored within the system (e.g., passwords)	Yes
SEC 5.2	1	The system shall provide the capability of maintaining confidentiality of sensitive content (e.g., sensitive but unclassified content)	Yes

3.2.22.6 Security – Administration (SEC 6.0)

ID	Criticality	Capability	Spec. Required
SEC 6.1	1	The system shall provide an administrative graphical user interface to perform user administration and security administration.	Yes
SEC 6.2	1	The system shall have the capability for authorized security administrators to set and maintain system security policy.	Yes

SEC 6.3	1	The system shall provide the capability for authorized security administrators to monitor system security policy settings and policy enforcement.	Yes
SEC 6.4	1	The system shall provide the capability to define tasks that require more than one authorized administrator to perform (e.g., setting or changing security policies, two person integrity (TPI))	Yes
SEC 6.4.1	1	The system shall provide the capability to support separation of functions between system administrators, policy makers, security administrators and auditors	Yes
SEC 6.5	1	The system shall provide the capability to partition security administration into logical elements such that security administrators can be assigned accordingly	Yes
SEC 6.5.1	1	The system shall provide the capability to limit security administrator's authority to assigned logical elements	Yes

3.2.22.7 Availability

ID	Criticality	Capability	Spec. Required
SEC 7.1	1	The system shall provide appropriate security backup systems to assure availability to meet customer and GPO needs.	Yes

3.2.22.8 Security – Integrity (SEC 8.0)

ID	Criticality	Capability	Spec. Required
SEC 8.1	1	The system shall have the capability to assure integrity of content within the system (e.g., content will not be corrupted)	Yes
SEC 8.1.1	1	The system shall have the capability to assure integrity of content within the system at a definable frequency	Yes
SEC 8.1.2	1	The system shall have the capability to assure integrity of content in a timeframe based on GPO business rules	Yes
SEC 8.1.3	1	The system shall have the capability to verify that electronic content to be delivered is clean (e.g., virus-free, uncorrupted)	Yes
SEC 8.2	1	The system shall have the capability to assure integrity of content delivered (e.g., PKI, watermarking)	Yes
SEC 8.3	1	The system shall have the capability to maintain integrity of content ingested (e.g., digital signatures)	Yes
SEC 8.4	1	The system shall have the capability to assure integrity of BPI	Yes

3.2.22.9 Security – Standards (SEC 9.0)

ID	Criticality	Capability	Spec. Required
SEC 9.1	1	The system must have the capability to support industry integrity standards.	Yes
SEC 9.1.1	1	The system must have the capability to support RSA Digital Signature	Yes
SEC 9.1.2	1	The system must have the capability to support Public Key Infrastructure (PKI)	Yes

SEC 9.1.3	1	The system must have the capability to support International Telecommunication Union (ITU) X.509	Yes
SEC 9.1.4	1	The system must have the capability to support Public Key Infrastructure Exchange (PKIX)	Yes
SEC 9.1.5	1	The system must have the capability to support Message Authentication Control (MAC)	Yes
SEC 9.1.6	1	The system must have the capability to support Cyclical Redundancy Checking (CRC)	Yes
SEC 9.1.7	1	The system must have the capability to support Secure Hash Algorithm (SHA) Federal Information Processing Standard (FIPS) 180-2	Yes
SEC 9.1.8	1	The system must have the capability to support Digital Signature Standards (FIPS 186-2)	Yes
SEC 9.1.9	1	The system must have the capability to support Keyed Hash Message Authentication Code (HMAC) (FIPS 198)	Yes
SEC 9.2	1	The system must have the capability to support confidentiality standards	Yes
SEC 9.2.1	1	The system must have the capability to support Advanced Encryption Standard (AES) FIPS 197	Yes
SEC 9.2.2	1	The system must have the capability to support Triple Data Encryption Standard (TDES) ANSI X9-52	Yes
SEC 9.2.3	1	The system must have the capability to support Secure Sockets Layer (SSL) / Transport Layer Security (TLS)	Yes
SEC 9.3	1	The system must have the capability to support access control standards	Yes

SEC 9.3.1	1	The system must have the capability to support Lightweight Directory Access Protocol (LDAP) Internet Engineering Task Force (IETF) Request for Comments (RFC) 2251	Yes
SEC 9.3.2	1	The system must have the capability to support X500	Yes
SEC 9.3.3	1	The system must have the capability to support Security and Access Markup Language (SAML)	Yes

Appendix A – Glossary

Access: Tools and processes associated with finding, analyzing, ordering, and retrieving CPI or BPI.

Access aids: Tools and processes associated with finding, analyzing, retrieving, and ordering CPI or BPI.

Access Content Package (ACP): The result of ingest processing; i.e., validation, authentication, version control, transformation, verification of scope, validation or assignment persistent name, and metadata generation/capture.

Access (or service) copy: A digital publication whose characteristics (for example a screen-optimized PDF file) are designed for ease or speed of access rather than preservation.

Accessibility: Making tools and content available and usable for all users including those with disabilities; the degree to which the public is able to retrieve or obtain Government publications, either through the FDLP or directly through an digital information service established and maintained by a Government agency or its authorized agent or other delivery channels, in a useful format or medium and in a time frame whereby the information has utility.

Activity: A description of a piece of work that forms one logical step within a process. An activity may be a manual activity, which does not support computer automation, or a workflow (automated) activity. A workflow activity requires human and/or machine resources(s) to support process execution.

Application Security: The protection of application data and systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats at the application level. See also **Security.**

Archival information package (OAIS): Content information and its associated PDI needed to preserve the content over the long term, bound together by packaging information.

Archive: A collection with related systems and services, organized to emphasize the long-term preservation of information.

Archive management - See **Preservation**.

Authentic: Describes content that is verified by GPO to be complete and unaltered when compared to the version approved or published by the Content Originator.

Authentication: Validation of a user, a computer, or some digital object to ensure that it is what it claims to be. In the specific context of the Future Digital System, the assurance that an object is as the author or issuer intended it. See also **Certification**.

Authenticity: A digital publication's identity, source, ownership and/or other attributes are verified. Authentication also connotes that any change to the publication may be identified and tracked.

Availability - The degree to which information is obtainable through an intentional or unintentional provision of information and services.

Born digital: In the Future Digital System context, digital objects, created in a digital environment, with the intention of multiple eventual output products, potentially including hard copy, electronic presentation, and digital media. Born digital object will exist in an entirely digital lifecycle; relating to a document that was created and exists only in a digital format.

Browse: To explore a body of information on the basis of the organization of the collections or by scanning lists, rather than by direct searching.

Business process: A set of one or more linked activities which collectively realize a business objective or policy goal, normally within the context of an organizational structure defining functional roles and relationships.

Business process information: Administrative information, non-content specific information that is used within the business process and package description (PD) to support access aids and data mining.

Cataloging and indexing: Cataloging is comprised of the processes involved in constructing a catalog: describing information or documents to identify or characterize them, providing "entry points" (terms) peculiar to the information or document, e.g., author, title, subject, and format information, by which the information can be located and retrieved. The immediate product of cataloging is bibliographic records, which are then compiled into catalogs. Indexing is the process of compiling a set of identifiers that characterize a document or other piece of information by analyzing the content of the item and expressing it in the terms of a particular system of indexing. In GPO context, cataloging and indexing is the statutory term for the processes that produce the *Catalog of U.S. Government Publications* and its indexes. In the FDSys context, the process or results of applying bibliographic control to final published versions.

Certification: Proof of verification or authority. Process associated with ensuring that a digital object is authentically the content issued by the author or issuer. The "certificate" is a mark of veracity which is in some way joined to the object itself.

Certified: Providing proof of verification of authenticity or official status.

Collaboration: Allowing for multiple authors or content sources while maintaining digital asset and document control and provenance.

Collection of Last Resort – See **National Collection of U.S. Government Publications**

Collection plan, or **Collection management plan:** The policies, procedures, and systems developed to manage and ensure current and permanent public access to remotely accessible digital Government publications maintained in the National Collection.

Compose: The ability to style/format content

Composition: Creating content using FDsys applications.

Content: Information presented for human understanding.

Content Analysis: Interpretation of intended context.

Content Information (OAIS): The set of information that is the primary target for preservation, composed of the data object and its RI.

Content Package Information (CPI): Information that directly relates to the content and is ultimately used in the dissemination and preservation of the content to the end users.

Converted content: Digital content created from a tangible publication.

Cooperative Publication: Publications excluded from GPO's dissemination programs because they are produced with non-appropriated funds or must be sold in order to be self-sustaining. See 44 USC 1903.

Dark archive (digital): The site or electronic environment wherein a second "copy" or instance of all master and derivative digital files, data, and underlying enabling code resides and is maintained, under the control of the managing organization or its proxy. The dark archive must be inaccessible to the general public. Access to the dark repository contents and resources ("lighting" the archive) is triggered only by a specified event or condition.

Dark archive (tangible): A collection of tangible materials preserved under optimal conditions, designed to safeguard the integrity and important artifactual characteristics of the archived materials for specific potential future use or uses. Eventual use of the archived materials ("lighting" the archives) is to be triggered by a specified event or condition. Such events might include failure or inadequacy of the "service" copy of the materials; lapse or expiration of restrictions imposed on use of the archives content; effect of the requirements of a contractual obligation regarding maintenance or use; or other events as determined under the charter of the dark archives.

Data mining: Discovery method applied to large collections of data, which proceeds by classifying and clustering data (by automated means) often from a variety of different databases, then looking for associations. Specifically applied to the analysis of use and user data for GPO systems, data mining includes the tools and processes for finding, aggregating, and associating BPI to enhance internal and external business efficiencies.

Deposited content: Content received from content originators in digital form.

Derivative: A new presentation of existing content optimized for access. This does not include language translation.

Device: Content delivery mechanisms for digital media, such as data storage devices (e.g., CD, DVD, etc.), wireless handheld devices, future media, and storage at user sites.

Digital media: An intermediary mechanism consisting of data storage devices to deliver content to users' storage or display devices.

Digital object: An item stored in a digital library or other digital collection of information, consisting of data, metadata, and an identifier.

Digital signature: A cryptographic code consisting of a hash, to indicate that data has not changed, encrypted with the public key of the creator or the signature.

Dissemination: The transfer from the stored form of a digital object in a repository to the client or user.

Dissemination information package (DIP): An information package that contains parts of all or one or more archival information packages, to be distributed to the user or consumer as requested, or to service providers to produce various outputs.

Distribution: Applying GPO processes and services to a tangible publication and sending a tangible copy to depository libraries.

Document: A digital object that is the analog of a physical document, especially in terms of logical arrangement and use.

Draft: A preliminary version of content, not yet in its finalized form.

Dynamically Changed Workflow: Workflow process that is changed during executing.

Electronic presentation: The dynamic and temporary representation of content in digital format; strongly dependent upon file format and user's presentation device

Emulation: Replication of a computing system to process programs and data from an earlier system that is no longer is available.

Existing digital: In GPO's current situation, publications or digital objects which are produced solely for digital dissemination, such as documents on agency web sites for which there is no printed equivalent.

Faithful digital reproduction: Digital objects that are optimally formatted and described with a view to their *quality* (functionality and use value), *persistence* (long-term access), and *interoperability* (e.g. across platforms and software environments). Faithful reproductions meet these criteria, and are intended to accurately render the underlying source document, with respect to its completeness, appearance of original pages (including tonality and color), and correct (that is, original) sequence of pages. Faithful digital reproductions will support production of legible printed facsimiles when produced in the same size as the originals (that is, 1:1).

FDLP Electronic Collection, or **EC:** The digital Government publications that GPO holds in storage for permanent public access through the FDLP, or are held by libraries and/or other institutions operating in partnership with the FDLP. These digital publications may be remotely accessible online publications, or tangible publications such as CD-ROMs maintained in depository library collections.

FDLP partner: A depository library or other institution that stores and maintains for permanent access segments of the Collection.

Final Published Version: Content in a specific presentation and format approved by its Content Originator for release to an audience. (See also **Government Publication; Publication**).

Fixity: the quality of being unaltered (e.g. "fixity of the text" refers to the durability of the printed word).

Format: In a general sense, the manner in which data, documents, or literature are organized, structured, named, classified, and arranged. Specifically, the organization of information for storage, printing, or display. The format of floppy disks and hard disks is the magnetic pattern laid down by the formatting utility. In a document, the format includes margins, font, and alignment used for text, headers, etc. In a database, the format comprises the arrangement of data fields and field names.

Format management -See **Preservation**.

Fugitive document: A U.S. Government publication that falls within the scope of the Federal Depository Library Program (FDLP), but has not been included in the FDLP. These publications include tangible products such as ink-on-paper, microforms, CD-ROM, or DVDs. Fugitive documents most commonly occur when Federal agencies print or procure the printing of their publications on their own, without going through GPO.

Government publication: A work of the United States Government, regardless of form or format, which is created or compiled in whole or in part at Government expense, or as required by law, except that which is required for official use only, is for strictly operational or administrative purposes having no public interest or educational value, or is classified for reasons of national security.

Granularity: The degree or level of detail available within content in the system

Granularity policy: The system shall have the ability to certify related or continuous piece of content in context

Handle System: A comprehensive system for assigning, managing, and resolving persistent identifiers, known as "handles," for digital objects and other resources on the Internet. Handles can be used as Uniform Resource Names (URNs).

Hard copy: Tangible printed content.

Harvest: The gathering and capture of content resident on official Federal Government Web sites that falls within the scope of GPO dissemination programs.

Harvested content: Digital content within the scope of dissemination programs that is gathered from Federal agency Web sites.

History: A record of all system activities.

Information granularity: The degree or level of detail available in an information system. With reference to authentication, the level of detail or specificity (e.g., page, chapter, paragraph, line) to which veracity can be certified.

Ingest (OAIS): The OAIS entity that contains the services and functions that accept SIPs from Producers, prepare Archival Information packages for storage, and ensure that information packages and their supporting descriptive information packages are established within OAIS. In the FDSys, ingest processing includes validation, authentication, version control, transformation, verification of scope, validation or assignment persistent name, and metadata generation/capture.

Integrity Mark: Emblem that is used to convey authentication information to users. The mark may be visible or invisible, and all content delivery methods should have associated marks.

Interoperability: Compatibility of workflow across standards (e.g., WFMC to BPEL) and, compatibility of workflow within a standard and across programming languages (e.g., Java and C++ working in WFMC).

Item: A specific piece of material in a digital library or collection; a single instance, copy, or manifestation.

Job: An instance that will result in a product or service supplied by the system.

Light archive: A collection of tangible materials preserved under optimal conditions, designed to safeguard the integrity and important artifactual characteristics of the archived materials while supporting ongoing permitted use of those materials by the designated constituents of the archives. A light archive normally presupposes the existence of a dark archive, as a hedge against the risk of loss or damage to the light archives content through permitted uses. A light archive is also distinct from regular collections of like materials in that it systematically undertakes the active preservation of the materials as part of a cooperative or coordinated effort that may include other redundant or complementary light archives.

Localized Presentation: Temporary representation of layout or structure on a user's local presentation device.

Locate (discover): The organized process of finding Web-based documents or publications that are within scope for a particular collection.

Manage: In Information Technology contexts, to add, modify, or delete content.

Manifestation: Form given to an expression of a work, e.g., by representing it in digital form.

Message: Communication between a process and the Workflow Management System.

Metadata: Metadata is a structured representation of information that facilitates interpretation, management, and location by describing essential attributes and significant properties. Metadata describes the content, quality, condition, or other characteristics of other data. Metadata describes how, when, and by whom information was collected, where it resides, and how it is formatted. Metadata helps locate, interpret, or manage. In current usage several types of metadata are defined: **descriptive**, which aids in locating information; **structural/technical,** which records structures, formats, and relationships; **administrative,** which records responsibility, rights, and other information for managing the information; and **preservation,** which incorporates elements of the other types specific to preserving the information for the long term.

METS (Metadata Encoding and Transmission Standard): Essentially a standard DTD (document type definition) for interpreting XML as metadata.

Migration: Preservation of digital content where the underlying information is retained but older formats and internal structures are replaced by newer.

Modified Workflow: Workflow process that is changed during process development or, not at runtime.

National Collection of U.S. Government Publications, or **NC:** A comprehensive collection of all in-scope publications, content that should be (or should have been) in the FDLP, regardless of form or format. The NC will consist of multiple collections of tangible and digital publications, located at multiple sites, and operated by various partners within and beyond the U.S. Government.

No-fee access: There are no charges to individual or institutional users for searching, retrieving, viewing, downloading, printing, copying, or otherwise using digital publications in scope for the FDLP.

Notification: A message in Workflow between a process and the WMS that indicates when an identified event or condition, such as an exception, has been met.

OAIS: Open Archival Information System Reference Model (ISO 14721:2003) - A reference model 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 designate community. The model defines functions, activities, responsibilities, and relationships within this archive, sets forth common terms and concepts, and defined component functions which serve as the basis for planning implementation.

Official: A version that has been approved by someone with authority.

Official content: Content that falls within the scope of the FDLP EC and is approved by, contributed by, or harvested from an official source in accordance with accepted program specifications

Official source: The Federal publishing agency, its business partner, or other trusted source.

ONIX (Online Information eXchange): A standard format that publishers can use to distribute electronic information about their books to wholesale, e-tail and retail booksellers, other publishers, and anyone else involved in the sale of books.

Online: A digital publication that is published at a publicly accessible Internet site.

Online dissemination: Applying GPO processes and services to an online publication and making it available to depository libraries and the public.

Permanent Public Access, or **PPA:** Government publications within the scope of the FDLP remain available for continuous, no-fee public access through the program.

Persistent Name: Provides permanence of identification, resolution of location, and is expected to be globally (e.g., internationally) registered, validated, and unique

Preliminary Composition: Preparatory representation of content format or structure

Presentation Device: A device that can present content for comprehension

Preservation: The activities associated with maintaining publications for use, either in their original form or in some verifiable, usable form. Preservation may also include creation of a surrogate for the original by a conversion process, wherein the intellectual content and other essential attributes of the original are retained. For digital materials, preservation includes the management of formats of information (including possible migration to newer versions), the storage environment, and the archival arrangement of information to facilitate preservation.

Preservation description information (OAIS): Information necessary for adequate preservation of content information, including information on provenance, reference, fixity, and context.

Preservation master: A copy which maintains all of the characteristics of the original publication, from which true copies can be made.

Preservation master requirement: A set of attributes for a digital object of sufficient quality to be preserved and used as the basis for derivative products and subsequent editions, copies, or manifestations. Requirements for use, users, and state/condition/format of the source of the original object need to be noted.

Preservation processes: Activities necessary to keep content accessible and usable, including **Migration, Refreshment,** and **Emulation.**

Print on demand (POD): Hard copy produced in a short production cycle time and typically in small quantities.

Process: A formalized view of a "business process", represented as a coordinated (parallel and/or serial) set of process activities that are connected in order to achieve a common goal.

Provenance: The chain of ownership and custody which reflects the entities that accumulated, created, used, or published information. In a traditional archival sense, provenance is an essential factor in establishing authenticity and integrity.

Publication: (N) Content approved by its Content Originator for release to an audience. See also **Government publication**.

Reference tools: Finding aids, bibliographies, and other services to assist in the locating and use of information, often less formally organized than catalogs and indexes.

Refreshment: A preservation process for data extraction, cleaning and integration, and the triggering events of these activities.

Render: To transform digital information in the form received from a repository into a display on a computer screen or other presentation to a user.

Replication: Make copies of digital material for backup, performance, reliability, or preservation.

Repository: A computer system used to store digital collections and disseminate them to users.

Requirements: In system planning, a requirement describes what users want and expect according to their various needs. Requirements draw a comprehensible picture to facilitate communications between all stakeholders in the development of a system, and outline the opportunities for development of successful products to satisfy user needs.

Rich media: An electronic presentation incorporating audio, video, text, etc.

Rider: Request by GPO, agency, or Congress that adds copies to a Request or C.O. Order placed by a publishing agency or Congress.

Search: Process or activity of locating specific information in a database or on the World Wide Web. A search involves making a statement of search terms and refining the terms until satisfactory result is returned. Searching is distinct from browsing, which facilitates locating information by presenting references to information in topical collections or other logical groupings or lists.

Secondary dark archive (digital): Multiple "copies" or instances of the dark repository, maintained as assurance against the failure or loss of the original dark repository. The secondary dark repository must provide redundancy of content to the original dark repository, and the systems and resources necessary to support access to and management of that content must be fully independent of those supporting the original dark repository content.

Secondary service repository (digital): The secondary service archive is a "mirror" of the service archive, created to provide instantaneous and continuous access to all designated constituents when the access copy or service archive is temporarily disabled.

Security: The protection of systems against unauthorized access to or modification of information, whether in storage, processing or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats. The measures and controls, including physical controls in conjunction with management, technical and procedural controls, that ensure the confidentiality, integrity and availability of information processed and stored by a system. See also **Application Security.**

Service archive (digital): The site or electronic environment wherein the derivative, or "use," files and metadata created from source objects (here, tangible government documents), as well as the software, systems, and hardware necessary to transmit and make those files and metadata accessible, are maintained for public display and use. The service repository contains the current and most comprehensive electronic versions of those source materials.

Shared repository: A facility established, governed, and used by multiple institutions to provide storage space and, in some instances limited service for low-use library materials, primarily paper-based materials that do not have to be readily available for consultation in campus libraries.

Status: A representation of the internal conditions defining the state of a process or activity at a particular point in time.

Storage: The functions associated with saving digital publications on physical media, including magnetic, optical, or other alternative technologies.

Storage management - See **Preservation**.

Sub-versions of content: The state of content within the style tools and prior to ingest.

Submission information package (OAIS): The information package identified by the producer for ingest into an OAIS system.

Subscription: An agreement by which a user obtains access to requested content by payment of a periodic fee or other agreed upon terms.

System: An organized collection of components that have been optimized to work together in a functional whole.

Tangible publication: Products such as ink-on-paper, microforms, CD-ROM, or DVDs, characterized by content recorded or encoded on a physical substrate .

Transformation: The process, or the results of a process, of reformatting or otherwise changing the way content is digitally encoded.

Trusted content: Official content that is provided by or certified by a trusted source.

Trusted source: The publishing agency or a GPO partner that provides or certifies official FDLP content.

Unique Identifier: A character string that uniquely identifies digital objects, content packages and jobs within the system.

User: The person who uses a program, system, or collection of information to perform tasks and produce results.

Validation: A process that ensures data entered into the system conforms to standards for format, content and metadata.

Verification: The process of determining and assuring accuracy and completeness.

Version: Unique manifestation of a publication.

Version control: Relating to a specific manifestation, revision, issuance, or edition of a previously published or issued document or publication. Changes beyond an agreed upon threshold or tolerance constitute a new version. That threshold is a version trigger, and the activity of scanning for changes and activating the trigger is "version control."

Version detection: Activity of inspecting a content package for changes and responding to version triggers. Also, activity of polling the system to identify if an identical version already exists in the system.

Version identifier: Information stored in metadata that identifies version.

Version trigger: Changes beyond an agreed upon threshold or tolerance which constitute a new version.

Work Item: The representation of the work to be processed (by a workflow participant) in the context of an activity within a process.

Workflow: The automation of a business process, in whole or part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules.

Workflow Management System (WMS): A system that defines, creates and manages the execution of workflows through the use of software, running on one or more workflow engines, which is able to interpret the process definition, interact with workflow participants and, where required, invoke the use of IT tools and applications.

Workflow Participant: A resource, human or computer tool/application, which performs the work represented in an activity.

Worklist: A list of "work items" associated with a given workflow participant (or in some cases with a group of workflow participants who may share a common worklist). The worklist forms part of the interface between a workflow engine and the worklist handler.