REQUIREMENTS DOCUMENT
(RD V3.1)

FOR GPO'S
DIGITAL CONTENT SYSTEM (FDsys)

FINAL

June 7, 2007

Table of Contents

1 Introduction 6
2 Requirements for System, General 7
3 Requirements for Content Metadata 8
3.1 Content Metadata Core Capabilities 8
3.2 Content Metadata Types 8
3.3 Content Metadata Schema 9
3.4 Content Metadata Import and Export 10
3.5 Content Metadata Management 11
4 Requirements for SIP 11
4.1 SIP – Deposited Content 11
4.2 SIP – Harvested Content 11
4.3 SIP – Converted Content 11
4.4 Core SIP Requirements 12
4.5 Requirements for sip.xml File 12
4.6 Structural Layout for SIPs 13
4.7 Packaging of SIPs 13
4.8 SIP Descriptive Metadata Requirements 13
4.9 SIP Administrative Metadata Requirements 14
5 Requirements for AIP 14
5.1 AIP Core Capabilities 14
5.2 Requirements for aip.xml File 15
5.3 Structural Layout for AIPs 16
5.4 AIP Metadata 16
5.5 AIP Unique ID 17
6 Requirements for ACP 17
6.1 ACP Core Capabilities 17
6.2 ACP Binding Metadata File 18
6.3 ACP Metadata 18
7 Requirements for DIP 19
7.1 DIP Core Capabilities 19
7.2 DIP Binding Metadata File 19
7.3 DIP Metadata 20
8 Requirements for Pre-ingest Processes 20
8.1 Pre-ingest Processing 20
9 Requirements for Ingest Processing 21
9.1 Ingest Processing Core Capabilities 21
9.2 Ingest Processing 22
10 Requirements for Preservation Processing 22
10.1 Preservation Processing Core Capabilities 22
10.2 Preservation Processing 23
10.3 Preservation Processing – Assessment 26
10.4 Preservation Processing – Administration 26
10.5 Preservation Processing – Storage 27
10.6 Preservation Processing – Metadata 27
10.7 Preservation Processing – Security 27
11 Requirements for Unique Identifier 27
11.1 Unique ID Core Capabilities 27
11.2 Job ID 28
11.3 Content Package ID 29
11.4 Interface for Unique ID 29
12 Requirements for Persistent Name 29
12.1 Persistent Name Core Capabilities 29
12.2 Persistent Name Resolution 30
12.3 Persistent Name Metadata 30
13 Requirements for Authentication 30
13.1 Authentication Core Capabilities 30
13.2 Authentication – Content Pre-ingest and Ingest 31
13.3 Authentication – User Credentials 33
13.4 Authentication – Content Integrity 33
13.5 Authentication – Time Stamps 34
13.6 Authentication – Integrity Marks 34
13.7 Authentication – Content Delivery 35
13.8 Re-authentication of Content 36
13.9 Authentication Standards/Best Practices 36
13.10 Authentication Records Management 36

13.11 Authentication Metadata 37
14 Requirements for Version Control 37
14.1 Version Control Core Capabilities 37
14.2 Version Triggers 38
14.3 Version Detection 38
14.4 Version Metadata 38
14.5 Version Relationships 38
14.6 Version Notification 38
15 Requirements for Workflow 39
15.1 Workflow Core Capabilities 39
15.2 Workflow – Control of Execution 40
15.3 Workflow – Monitoring 41
15.4 Workflow – Resource Requirements 42
15.5 Workflow – Notification 42
15.6 Workflow – Security 42
15.7 Workflow – Interface 42
16 Requirements for Storage Management 42
16.1 Storage Core Capabilities 42
16.2 Content Delivery Network Storage 43
16.3 Networked Moderate Performance Storage 43
16.4 Low Criticality- Low Cost Storage 43
16.5 Failover Storage 43
16.6 Backup Retrieval Media Storage 44
16.7 Mid-term Archival Storage 44
16.8 Long-term Permanent Archival Storage 44
16.9 Functional Data Storage 44
16.10 Storage System Standards 45
16.11 Storage – Monitoring 46
16.12 Storage – Preventive Action 46
16.13 Storage – Data Integrity 46
16.14 Storage – Allocation 47
17 Requirements for Security 47
17.1 Security – System User Authentication 47
17.2 Security – User Access Control 48
17.3 Security – Capture and Analysis of Audit Logs 48
17.4 Security – User Privacy 50
17.5 Security – Confidentiality 50
17.6 Security Administration 50
17.7 Security – Availability 51
17.8 Security – Integrity 52
17.9 Security Standards 52
18 Requirements for Enterprise Service Bus 53
18.1 ESB Core Capabilities 53
18.2 ESB Configuration 54
18.3 ESB Administration 55
18.4 ESB Interface 55
19 Requirements for Data Mining 55
19.1 Data Mining – Data Extraction 55
19.2 Data Mining – Data Normalization 56
19.3 Data Mining – Data Analysis and Modeling 56
19.4 Data Mining – Report Creation and Data Presentation 57
19.5 Data Mining – Security and Administration 58
19.6 Data Mining – Storage 59
20 Requirements for Content Submission 59
20.1 Content Submission Core Capabilities 59
20.2 Content Submission – System Administration 59
20.3 Content Submission Metadata 60
21 Requirements for Deposited Content 62
21.1 Deposited Content Core Capabilities 62
21.2 Deposited Content Metadata 62
21.3 Deposited Content Interfaces 62
22 Requirements for Converted Content 63
22.1 Converted Content Core Capabilities 63
22.2 Converted Content Interfaces 63
23 Requirements for Harvested Content 63
23.1 Harvested Content Core Capabilities 63

23.2 Harvested Content Metadata 63
23.3 Harvester Requirements 63
23.4 Metadata Requirements for Harvester 64
23.5 Harvester Rules and Instructions 65
23.6 Harvester Interface 65
23.7 System Administration for Harvester 65
24 Requirements for Style Tools 66
24.1 Style Tools Core Capabilities 66
24.2 Style Tools – Automated Composition 66
24.3 Style Tools – System Administration 67
25 Requirements for Content Originator Ordering 67
25.1 Content Originator Ordering Core Capabilities 67
25.2 Content Originator Ordering – Job Management 68
25.3 Content Originator Ordering – Job Tracking 72
25.4 Requirements for Access Content Processing 73
25.4.1 Access Core Capabilities 73
25.4.2 Access to Content Packages 75
25.4.3 Access to the System 77
25.4.4 Access – User Registration 77
25.4.5 Access – User Preferences 78
25.4.6 Access Processing 78
26 Requirements for Accessibility 79
26.1 Accessibility Core Capabilities 79
26.2 Accessibility – Section 508 Technical Standards 79
27 Requirements for Search 84
27.1 Search Core Capabilities 84
27.2 Search – Query 85
27.3 Search – Refine 87
27.4 Search – Results 87
27.5 Saved Searches 88
27.6 Search Interface 89
27.7 Search Administration 89
28 Requirements for Request 89
28.1 Request Core Capabilities 89
28.2 No Fee Requests 89
28.3 Fee-based Requests 90
28.4 Request – Delivery Options 92
28.5 Request – User Accounts 92
28.6 Order Numbers and Request Status 93
29 Requirements for Cataloging and Reference Tools 93
29.1 Cataloging and Reference Tools – Metadata Management 93
29.2 Cataloging and Reference Tools – Metadata Delivery 93
29.3 Reference Tools 94
29.4 Cataloging and Reference Tools – Interoperability and Standards 94
30 Requirements for User Interface 96
30.1 User Interface Core Capabilities 96
30.2 User Interface Standards and Best Practices 97
30.3 User Interface Customization and Personalization 97
30.4 User Interface Default Workbenches 98
31 Requirements for User Support 98
31.1 User Support Core Capabilities 98
31.2 User Support – Context Specific Help 99
31.3 User Support – Helpdesk 100
31.4 User Support – Knowledge Base 102
31.5 User Support – Alerts 103
31.6 User Support – Training and Events 103
31.7 Contact Management 104
32 Requirements for Content Delivery and Processing 105
32.1 Content Delivery Core Capabilities 105
32.2 Content Delivery Processing 106
32.3 Content Delivery Mechanisms 106
33 Requirements for Hard Copy Output 107
33.1 Hard Copy Output Core Capabilities 108
34 Requirements for Electronic Presentation 109
34.1 Electronic Presentation Core Capabilities 109
35 Requirements for Digital Media 111

35.1 Digital Media Core Capabilities 111
Appendix A – References 113
Appendix B – Acronyms and Glossary 123
Acronyms 123
Glossary 127

1 Introduction

This document defines the requirements for the U.S. Government Printing Office's Digital Content System (FDsys) and is intended to communicate those requirements to the technical development community which will build the system.

System Purpose:
FDsys will be a comprehensive, systematic, and dynamic means to create, ingest, authenticate, preserve, manage, and provide access to Government information from all three branches of the Federal Government. The system will automate and integrate lifecycle processes of Government information and deliver that information in formats suited to customer needs and desires.

System Scope:
FDsys will be built to include all known Federal Government publications falling within the scope of GPO's Federal Depository Library Program (FDLP), including text, graphics, video, audio, numeric, and other emerging forms of content. The full body of these publications will be available for searching, viewing, download, and printing, and will also be available for the production of document masters for conventional and on-demand printing.

System Releases:
FDsys is being implemented in a series of incremental releases, each of which builds on those preceding it, and add improvements to system capability and underlying infrastructure.

Requirements:
The requirements documented here are the product of a development process that has as its basis the Future Digital System Concept of Operations (ConOps) (rev. 2006) and previous versions of this document. Thirty-Four major system capabilities are described, each with multiple subsections arranged hierarchically. Each requirement is assigned a release in which we expect its implementation, as well as a ranking of criticality to that release:

- Must indicates a requirement essential to the successful function of the system;
- Should denotes functionality users will expect, and which should be implemented in as many cases as possible;
- Could indicates functionality that, although desirable, is not viewed as critical to system function or user experience.

ID	Object Number	2007-05-08 Requirements Baseline	RC
RD-1	2	**2 Requirements for System, General**	
RD-2	2.0-1	The system shall provide for the use of internal and external open interfaces.	R1B; Must
RD-3	2.0-1.0-1	The system may provide for the use of proprietary interfaces only when open interfaces are not available or do not meet system requirements.	R1B; Must
RD-4	2.0-2	The system shall provide an architecture that allows preservation of content independent of any specific hardware and software that was used to produce them.	R1B; Must
RD-5	2.0-3	The system shall use plug-in components that can be replaced with minimal impact to remaining components as workload and technology change.	R2; Must
RD-6	2.0-4	The system shall accommodate changes in technologies and policies without requiring major re-engineering or design changes.	R1C; Must
RD-7	2.0-4.0-1	The system shall support multiple user roles.	R1C; Must
RD-8	2.0-4.0-2	The system shall support the assignment of one or more roles to a user.	R1C; Must
RD-9	2.0-4.0-3	The system shall support the management of the functions permitted by a user role.	R1C; Must
RD-10	2.0-4.0-4	The system shall prevent a user from performing a function unless the user possesses a user role permitting that function.	R1C; Must
RD-11	2.0-4.0-5	The system shall support the capability to change key parameters affecting the operation of the system without redesigning the system.	R1C; Must
RD-12	2.0-4.0-6	The system shall support the capability to accommodate changes in hardware technologies without requiring major reengineering or design changes.	R1C; Must
RD-13	2.0-4.0-7	The system shall support the capability to accommodate changes in software technologies without requiring major reengineering or design changes.	R1C; Must
RD-14	2.0-4.0-8	The system shall support the capability to accommodate changes in processes without requiring major reengineering or design changes.	R1C; Must
RD-15	2.0-4.0-9	The system shall support the capability to accommodate changes in policies without requiring major reengineering or design changes.	R1C; Must
RD-16	2.0-4.0-10	The system shall support the capability to accommodate changes in personnel without requiring major reengineering or design changes.	R1C; Must
RD-17	2.0-4.0-11	The system shall support the capability to accommodate changes in system locations without requiring major reengineering or design changes.	R1C; Must
RD-18	2.0-5	The system shall provide the capability to scale to 50 petabytes of storage without requiring redesign of the system.	R1C; Must
RD-19	2.0-6	The system shall have the ability to handle additional kinds of content over time, not limited to specific types that exist today.	R1B; Must
RD-20	2.0-6.0-1	The system shall provide the ability to ingest content independently of its digital format.	R1B; Must
RD-21	2.0-6.0-2	The system shall provide the ability to store content independently of its digital format.	R1B; Must
RD-22	2.0-6.0-3	The system shall provide the ability to deliver content independently of its digital format.	R1B; Must
RD-23	2.0-7	The system shall provide support for content management lifecycle processes for harvested, converted and deposited content.	R2; Must
RD-24	2.0-8	The system shall 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.	R2; Must
RD-25	2.0-8.0-1	The system shall enable GPO to tailor content-based services to suit its customers needs.	R3; Must
RD-26	2.0-8.0-2	The system shall enable GPO to tailor content-based services to implement progressive improvements in business process.	R3; Must
RD-27	2.0-9	The system shall assemble content and metadata files into content packages that are compliant with open standards.	R1B; Must
RD-28	2.0-9.0-1	The system shall provide the capability for a content package to contain one binding file.	R1B; Must
RD-29	2.0-9.0-2	The binding file of the content package shall be expressed in XML.	R1B; Must
RD-30	2.0-9.0-3	The binding file of the content package shall contain an inventory of all the content files in the package.	R1B; Must
RD-31	2.0-9.0-4	The binding file of the content package shall contain an inventory of all the metadata files in the package.	R1B; Must
RD-32	2.0-9.0-5	The binding file of the content package shall contain the relationships between	R1B; Must

		the content files and metadata files in the package.	
RD-33	2.0-9.0-6	The system shall provide the capability for one or more metadata files to be related to each content file in a content package.	R1B; Must
RD-34	2.0-9.0-7	The system shall provide the capability for each metadata file to be related to one or more content files in a content package.	R1B; Must
RD-35	2.0-9.0-8	The system shall support the capability to transform the binding file of the content package into other formats.	R3; Must
RD-36	2.0-10	The system shall be available for use at all GPO locations.	R1C; Must
RD-37	2.0-11	The system is considered available when all critical system functions are operational. The critical functions of the system are those needed to support the submission, processing, access, and delivery of Priority 1 documents. The rationale for this definition is to insure that the system is considered operational when these top priority operations can be performed and not considered operational when they can not be performed. The functions are priority 1 document submission, pre-ingest, ingest, storage in AIP and ACP storage, index for search, search results, and electronic presentation delivery. This implies that the FDsys web site, workflow engine, content management system, search engine, and storage systems are also operational.	R1C; Must
RD-38	2.0-12	The system shall provide the capability to maintain required response times when there are 20,000 concurrent users performing a mix of operations that represents peak time operational use.	R1C; Must
RD-39	2.0-13	The system shall support an average peak time availability of 99.7%.	R1C; Must
RD-42	2.0-14	The system shall provide a response to the user within 2 seconds of a user on the GPO intranet initiating an operation.	R1C; Must

RD-43	3	**3 Requirements for Content Metadata**	
RD-44	3.1	***3.1 Content Metadata Core Capabilities***	
RD-45	3.1.0-1	The system shall have a central functionality which collects, edits, and shares content metadata among the broad functions of the system.	R1B; Must
RD-46	3.1.0-1.0-1	The system shall allow authorized users to edit content metadata residing within a SIP.	R1B; Must
RD-47	3.1.0-1.0-2	The system shall allow authorized users to edit content metadata residing within an AIP.	R1B; Must
RD-48	3.1.0-1.0-3	The system shall allow authorized users to edit content metadata residing within an ACP.	R1B; Must
RD-49	3.1.0-1.0-4	The system shall allow authorized users to edit content metadata residing within WIP.	R1B; Must
RD-50	3.1.0-2	The system shall have the capability to employ multiple content metadata schema, and to process and preserve multiple sets of content metadata for a digital object.	R1B; Must
RD-51	3.1.0-3	The system shall provide mechanisms to share content metadata and provide linkages and interoperability between extension schema and input standards.	R1B; Must
RD-52	3.1.0-4	The Application Programmer Interfaces of the system shall be based on open standards	R1B; Must
RD-53	3.1.0-5	The system shall provide the capability to link content metadata with system metadata.	R1B; Must
RD-54	3.1.0-6	The system shall provide the capability to link content metadata with business process information.	R1B; Must

RD-55	3.2	***3.2 Content Metadata Types***	
RD-56	3.2.0-1	The system shall employ metadata which relates descriptive information related to a target digital object(s) and its associated content package.	R1B; Must
RD-57	3.2.0-1.0-1	All metadata files shall be encoded in XML and conform to schema that are adopted by FDsys.	R1B; Must
RD-58	3.2.0-2	The system shall employ metadata which relates representation information	R1B; Must

		related to a target digital object(s) and its associated content package.	
RD-59	3.2.0-3	The system shall employ metadata which relates administrative information related to a target digital object(s) and its associated content package.	R1B; Must
RD-60	3.2.0-3.0-1	The system shall employ metadata which relates technical information related to a target digital object(s) and its associated content package.	R1B; Must
RD-61	3.2.0-3.0-2	The system shall employ metadata which relates the structure of a target digital object(s) and its associated content package.	R1B; Must
RD-62	3.2.0-3.0-2.0-1	The system shall employ publication-specific metadata as required to support existing and future publications.	R1C; Must
RD-63	3.2.0-3.0-2.0-2	The system shall employ document-specific metadata as required to support existing and future publications	R1C; Must
RD-64	3.2.0-3.0-3	The system shall employ metadata which relates the rights information of a target digital object(s) and its associated content package.	R1C; Must
RD-65	3.2.0-3.0-4	The system shall employ metadata which relates the source information of a target digital object(s) and its associated content package.	R1B; Must
RD-66	3.2.0-3.0-5	The system shall employ metadata which relates the provenance information of a target digital object(s) and its associated content package.	R1B; Must
RD-67	3.2.0-4	The system shall employ metadata which relates the Preservation Description Information (PDI) of a target digital object(s) and its associated content package.	R1B; Must
RD-68	3.2.0-5	The system shall employ metadata which relates the context of a digital object and relationship to other objects.	R1B; Must
RD-69	3.2.0-6	The system shall employ metadata which relates the fixity and authority (e.g., official, certified, etc) of the digital object and its associated content package.	R1B; Must
RD-70	3.2.0-7	The system shall employ metadata which describes and provides reference information about the digital object and its associated content package.	R1B; Must
RD-71	3.2.0-8	The system shall employ metadata which relates packaging information related to a target digital object(s) and its associated content package.	R1B; Must

RD-72	3.3	## *3.3 Content Metadata Schema*	
RD-73	3.3.0-1	GPO shall adopt the most current version of the Metadata Encoding and Transmission Standard (METS) as the encoding standard for content packages in the system.	R1B; Must
RD-74	3.3.0-2	In general, GPO shall refer to metadata schema rather than embed data elements in the METS wrapper.	R1B; Must
RD-75	3.3.0-3	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible.	R2; Must
RD-76	3.3.0-3.0-1	The system shall support the capability to employ additional established extension schema for expressing metadata in the future.	R2; Must
RD-77	3.3.0-3.0-2	The system shall support the capability to translate metadata conforming to registered input standards to an XML representation for storage in the system.	R2; Must
RD-78	3.3.0-3.0-3	The system shall have the capability to employ Dublin Core version 1.1 as an extension schema.	R1B; Must
RD-79	3.3.0-3.0-4	The system shall have the capability to employ PREMIS version 1.0 as an extension schema.	R1B; Must
RD-80	3.3.0-3.0-5	The system shall have the capability to employ Machine Readable Cataloging (MARC) as an input standard.	R1B; Must
RD-81	3.3.0-3.0-6	The system shall have the capability to employ Metadata Object Description Schema (MODS) version 3.2 as an extension schema.	R1B; Must
RD-82	3.3.0-3.0-7	The system shall support the capability to employ additional input standards for expressing metadata in the future.	R2; Must
RD-83	3.3.0-3.0-8	The system shall have the capability to employ Encoded Archival Description (EAD) version 2002 as an extension DTD.	R2; Could
RD-84	3.3.0-3.0-9	The system shall have the capability to employ Text Encoding Initiative (TEI) TEI P4 DTD as an extension DTD.	R2; Could
RD-85	3.3.0-3.0-10	The system shall have the capability to employ Data Document Initiative (DDI) version 2.1 as an extension DTD.	R2; Could
RD-86	3.3.0-3.0-11	The system shall have the capability to employ Federal Geographic Data Committee (FGDC) CSDGM Document Type Declaration as an extension DTD.	R2; Could
RD-87	3.3.0-3.0-12	The system shall have the capability to employ multiple established extension schema and input standards for expressing metadata when possible,	R1C; Must

		including Premis.	
RD-88	3.3.0-3.0-13	The system shall have the capability to employ MPEG 21 as an input standard.	R2; Should
RD-89	3.3.0-3.0-14	The system shall have the capability to employ JPEG 2000 as an input standard.	R2; Should
RD-90	3.3.0-3.0-15	The system shall have the capability to employ ONIX as an extension schema.	R2; Must
RD-91	3.3.0-3.0-16	The system shall have the capability to employ MIX (NISO Metadata for Images) as an extension schema.	R1C; Must
RD-92	3.3.0-4	The system shall employ a registry of extension schema and input standards in use.	R1C; Must
RD-93	3.3.0-5	Authorized users shall have the capability to manage the registry of schema employed by the system.	R1C; Must
RD-94	3.3.0-5.0-1	The system shall provide the capability for users to add new XML schemas to the Schema Registry,	R1C; Must
RD-95	3.3.0-5.0-2	The system shall provide the capability for users to remove XML schemas from the Schema Registry,	R1C; Must
RD-96	3.3.0-5.0-3	The system shall provide the capability for users to update XML schemas in the Schema Registry,	R1C; Must
RD-97	3.3.0-5.0-4	The system shall allow users to add new XML DTDs to the Schema Registry,	R1C; Must
RD-98	3.3.0-5.0-5	The system shall provide the capability for users to remove XML DTDs from the Schema Registry,	R1C; Must
RD-99	3.3.0-5.0-6	The system shall provide the capability for users to update XML DTDs in the Schema Registry,	R1C; Must
RD-100	3.3.0-5.0-7	The system shall provide a GUI interface for users to edit the Schema Registry	R2; Must
RD-103	3.3.0-8	Any schema registered in FDsys shall act as an extension schema to METS	R1C; Must
RD-104	3.3.0-9	The schema shall map to specific function(s), content type, or content formats within the system.	R1C; Must
RD-105	3.3.0-9.0-1	The schema shall map to specific function(s).	R1C; Must
RD-106	3.3.0-9.0-2	The schema shall map to content type(s).	R1C; Must
RD-107	3.3.0-9.0-3	The schema shall map to content format(s).	R1C; Must
RD-110	3.3.0-12	The system shall provide the capability to add extension schema developed by GPO to the Schema Registry.	R1C; Must
RD-111	3.3.0-13	Specific schema for each digital object shall be based on the specific needs of the target digital object or content package.	R1C; Must

RD-112	3.4	## *3.4 Content Metadata Import and Export*	
RD-113	3.4.0-1	The system shall have the capability to receive and record existing metadata from sources external to the system.	R3; Must
RD-114	3.4.0-1.0-1	The system shall have the capability to receive existing MARC metadata from sources external to the system."	R2; Must
RD-115	3.4.0-1.0-2	The system shall have the capability to record existing MARC metadata from sources external to the system."	R2; Must
RD-116	3.4.0-1.0-3	The system shall have the capability to receive existing COSATI metadata from sources external to the system."	R3; Must
RD-117	3.4.0-1.0-4	The system shall have the capability to record existing COSATI metadata from sources external to the system."	R3; Must
RD-118	3.4.0-2	The system shall provide the capability to deliver DIPs that contain only metadata.	R1C; Must
RD-119	3.4.0-2.0-1	The system shall provide the capability to export metadata from a single publication.	R1C; Must
RD-120	3.4.0-2.0-1.0-1	The system shall provide the capability to export content along with metadata from a single publication.	R1C; Must
RD-121	3.4.0-2.0-1.0-2	The system shall provide the capability to export metadata from one or more renditions of a single publication.	R1C; Must
RD-122	3.4.0-2.0-1.0-3	The system shall provide the capability to export one or more metadata files from a single publication."	R1C; Must
RD-123	3.4.0-2.0-2	The system shall provide the capability to export metadata in the form of a series of DIPs for the publications matching a user specified search.	R1C; Must
RD-124	3.4.0-2.0-2.0-1	The system shall provide the capability to export content along with metadata from multiple publications.	R1C; Must

RD-125	3.4.0-2.0-2.0-2	The system shall provide the capability to export metadata from one or more renditions of multiple publications."	R1C; Must
RD-126	3.4.0-2.0-2.0-3	The system shall provide the capability to export one or more metadata files from multiple publications."	R1C; Must
RD-127	3.4.0-3	The system shall provide the capability to transform metadata from one standard to another prior to exporting it.	R2; Must

RD-128	3.5	***3.5 Content Metadata Management***	
RD-129	3.5.0-1	The system shall have the ability to manage metadata regardless of its source.	R1B; Must
RD-130	3.5.0-2	The system shall have the ability to create metadata meeting the requirements of one or more schema.	R2; Must
RD-131	3.5.0-2.0-1	The system shall provide the capability for an authorized user to enter metadata.	R1B; Must
RD-132	3.5.0-2.0-2	The system shall provide the capability to transform metadata from one standard to another.	R2; Must
RD-133	3.5.0-2.0-3	The system shall provide the capability to extract metadata from content.	R2; Must
RD-134	3.5.0-3	The system shall provide the capability for GPO to designate metadata elements as mandatory.	R1B; Must
RD-135	3.5.0-4	The system shall have the capability to automatically record in system metadata information about the actions performed by the system on content.	R1B; Must
RD-136	3.5.0-5	The system shall have the capability to automatically record in BPI information about the actions performed by business processes on content.	R1B; Must
RD-137	3.5.0-6	The system shall log all additions, deletions, and changes to content metadata within the system.	R1B; Must

RD-138	4	**4 Requirements for SIP**	
RD-139	4.1	***4.1 SIP – Deposited Content***	
RD-140	4.1.0-1	The SIP for Deposited Content shall contain one or more renditions of the publication being submitted in the SIP.	R1B; Must
RD-141	4.1.0-2	The metadata for deposited content in the SIP shall consist of fundamental representation information, any necessary DTDs (or schema), style sheets, and submission level metadata for each rendition.	R1B; Must

RD-142	4.2	***4.2 SIP – Harvested Content***	
RD-143	4.2.0-1	The SIP for Harvested Content shall contain zero or more rendition consisting of the original harvested digital objects.	R1B; Must
RD-144	4.2.0-2	The metadata for harvested content in the SIP shall consist of representation information, documentation of harvest & transformation(s), submission level metadata for each rendition.	R2; Must
RD-145	4.2.0-2.0-1	The metadata for harvested content in the SIP shall include information about the harvest process.	R2; Must

RD-146	4.3	***4.3 SIP – Converted Content***	
RD-147	4.3.0-1	The SIP for Converted Content shall contain, at a minimum, a rendition consisting of the digital object(s) as produced by the conversion process.	R1B; Must
RD-148	4.3.0-2	The SIP for converted Content shall support the inclusion of representation information and metadata describing the conversion process for each rendition.	R1B; Must
RD-149	4.3.0-2.0-1	The metadata for converted content in the SIP shall include full technical information on the conversion, as specified by NISO Z 39.87-2002.	R1B; Must

RD-150	4.4	***4.4 Core SIP Requirements***	
RD-151	4.4.0-1	A SIP shall contain one or more renditions of one publication.	R1B; Must
RD-152	4.4.0-1.0-1	A SIP that describes a publication which only exists in tangible form shall contain a surrogate digital object that describes its tangible expression.	R1B; Must
RD-153	4.4.0-1.0-2	A SIP shall have the capability to contain metadata indicating if the publication it contains is in scope for GPO's dissemination programs.	R1B; Must
RD-154	4.4.0-1.0-3	Each rendition of a publication in a SIP shall be contained in its own subdirectory of the content directory.	R1B; Must
RD-155	4.4.0-1.0-4	A rendition of a publication in a SIP shall contain one or more digital objects.	R1B; Must
RD-156	4.4.0-1.0-5	A rendition of a publication in a SIP shall contain one or more subdirectories.	R1B; Must
RD-157	4.4.0-1.0-6	Each rendition of a publication in the SIP shall contain metadata that indicates if that rendition is a copy of the original file in which the publication was created.	R1B; Must
RD-158	4.4.0-1.0-7	Each rendition of a publication in the SIP shall contain metadata that indicates if that rendition is the highest fidelity rendition of the publication being submitted in the SIP.	R1B; Must
RD-159	4.4.0-1.0-8	Each rendition of a publication in the SIP shall contain metadata that indicates if that rendition is in a screen optimized format.	R1B; Must
RD-160	4.4.0-1.0-9	Each rendition of a publication in the SIP shall contain metadata that indicates if that rendition is in a print optimized format.	R1B; Must
RD-161	4.4.0-1.0-10	Each rendition of a publication in the SIP shall contain metadata that indicates if that rendition is in a press optimized format.	R1B; Must
RD-162	4.4.0-1.0-11	Each rendition of a publication in the SIP shall contain metadata that indicates if that rendition is a complete representation of the publication.	R1B; Must
RD-163	4.4.0-1.0-12	Each rendition of a publication in the SIP shall contain metadata that indicates if that rendition can be successfully edited using the software that created the rendition.	R1B; Must
RD-164	4.4.0-2	A SIP shall contain a METS file named sip.xml.	R1B; Must
RD-165	4.4.0-2.0-1	The sip.xml file shall contain an inventory of all the content files in a SIP.	R1B; Must
RD-166	4.4.0-2.0-2	The sip.xml file shall contain an inventory of all the metadata files in a SIP.	R1B; Must
RD-167	4.4.0-2.0-3	The sip.xml file shall contain the relationships between the content files and metadata files in a SIP.	R1B; Must
RD-168	4.4.0-2.0-4	The system shall provide the capability for one or more metadata files to be related to each content file in a SIP.	R1B; Must
RD-169	4.4.0-2.0-5	The system shall provide the capability for each metadata file to be related to one or more content files in a SIP.	R1B; Must
RD-170	4.4.0-3	A SIP shall contain one or more metadata files associated with the content.	R1B; Must
RD-171	4.4.0-3.0-1	The system shall provide the capability to store an XML schema that describes the format of a content file in a SIP.	R1B; Must
RD-172	4.4.0-3.0-2	The system shall provide the capability to store an XML DTD that describes the format of a content file in a SIP.	R1B; Must
RD-173	4.4.0-4	Metadata files in a SIP shall be encoded in XML.	R1B; Must
RD-174	4.4.0-4.0-1	Metadata files in a SIP shall conform to an XML Schema or XML DTD that is registered in the FDsys Metadata Schema Registry.	R1C; Must
RD-175	4.4.0-5	The SIP specified in this document shall apply to all content types specified and accepted by FDsys: converted, deposited and harvested.	R2; Must
RD-176	4.4.0-5.0-1	The SIP requirements shall apply to deposited content.	R1B; Must
RD-177	4.4.0-5.0-2	The SIP requirements shall apply to converted content.	R1C; Must
RD-178	4.4.0-5.0-3	The SIP requirements shall apply to harvested content.	R1C; Must

RD-179	4.5	***4.5 Requirements for sip.xml File***	
RD-180	4.5.0-1	The sip.xml file shall conform to the METS version 1.5.	R1B; Must
RD-181	4.5.0-2	The sip.xml file shall conform to the GPO METS Profile version 1.0.	R1B; Must
RD-182	4.5.0-3	Digital objects in the SIP shall be stored outside the sip.xml file.	R1B; Must
RD-183	4.5.0-3.0-1	Digital objects in the SIP shall be referred to in the sip.xml file using their filename and full path relative to the root of the SIP.	R1B; Must
RD-184	4.5.0-4	Metadata files in the SIP shall be stored outside the sip.xml file.	R1B; Must
RD-185	4.5.0-4.0-1	Metadata files in the SIP shall be referred to in the sip.xml file using their filename and full path relative to the root of the SIP.	R1B; Must

RD-187	4.6	***4.6 Structural Layout for SIPs***	
RD-188	4.6.0-1	The SIP shall contain the sip.xml at the top level of the SIP directory structure.	R1B; Must
RD-189	4.6.0-1.0-1	The SIP shall contain a directory named content at the top level of the SIP directory structure.	R1B; Must
RD-190	4.6.0-1.0-2	The SIP shall contain a directory named metadata at the top level of the SIP directory structure.	R1B; Must
RD-191	4.6.0-2	The content files for each rendition of a publication in a SIP shall be placed in its own subdirectory under the content directory.	R1B; Must
RD-192	4.6.0-2.0-1	The folder structure of the digital objects in a rendition folder shall be recorded in the sip.xml file.	R1B; Must
RD-194	4.6.0-3	All metadata files shall be placed in the metadata directory.	R1B; Must
RD-195	4.6.0-3.0-1	The metadata files for each rendition of a publication in a SIP shall be placed in its own subdirectory under the metadata directory.	R1B; Must
RD-196	4.6.0-3.0-1.0-1	The metadata subdirectory for a rendition shall have the same name as the content subdirectory for that rendition.	R1B; Must
RD-197	4.6.0-4	A SIP shall contain a least one metadata file containing descriptive metadata for the publication that shall be considered mandatory.	R1B; Must
RD-198	4.6.0-4.0-1	The mandatory descriptive metadata file for a publication shall be stored in MODS format.	R1B; Must
RD-199	4.6.0-4.0-2	The mandatory descriptive metadata file for a publication shall be located in the top level directory.	R1B; Must
RD-200	4.6.0-5	Each rendition of a publication shall have one or more metadata files that include administrative metadata about the rendition.	R1B; Must
RD-201	4.6.0-5.0-1	Each content file in a rendition shall have, at a minimum, a metadata file specifying the file format of the content file.	R1B; Must

RD-202	4.7	***4.7 Packaging of SIPs***	
RD-203	4.7.0-1	The system shall provide the capability to aggregate all the files and directories in a SIP into a single package.	R1B; Must
RD-204	4.7.0-1.0-1	The system shall provide the capability to aggregate the SIP into a ZIP file.	R1C; Must
RD-205	4.7.0-1.0-2	The system shall provide the capability to ingest into FDsys a SIP that is aggregated in a ZIP file.	R1C; Must
RD-206	4.7.0-1.0-3	The system shall support the capability to aggregate the SIP into additional file formats in the future.	R3; Must
RD-207	4.7.0-1.0-4	The system shall support the capability to ingest into Fdsys a SIP that is aggregated in additional file formats in the future.	R3; Must
RD-208	4.7.0-1.0-5	The system shall provide the capability to support batch input of multiple digital objects and metadata for multiple publications.	R1C, Must

RD-209	4.8	***4.8 SIP Descriptive Metadata Requirements***	
RD-210	4.8.0-1	The system shall have the capability to store descriptive metadata in multiple extension schema and records in the SIP.	R1B; Must
RD-211	4.8.0-1.0-1	The system shall have the capability to store descriptive metadata in ONIX format in the SIP.	R2; Must
RD-212	4.8.0-1.0-2	The system shall have the capability to store descriptive metadata in Dublin Core format in the SIP.	R1B; Must
RD-213	4.8.0-1.0-3	The system shall have the capability to store descriptive metadata in PREMIS format in the SIP.	R1B; Must
RD-214	4.8.0-1.0-4	The system shall have the capability to store descriptive metadata in COSATI format in the SIP.	R3; Must
RD-215	4.8.0-1.0-5	The system shall have the capability to store descriptive metadata in additional descriptive metadata formats in the future in the SIP.	R3; Must
RD-216	4.8.0-2	The system shall employ descriptive metadata elements in the SIP in MODS version 3.1 format.	R1B; Must
RD-217	4.8.0-3	The system shall allow all MODS elements to be stored in the MODS file in the SIP.	R1B; Must

RD-218	4.8.0-3.0-1	The system shall allow all MODS sub-elements to be stored in the MODS file in the SIP.	R1B; Must
RD-219	4.8.0-4	The system shall verify that all mandatory MODS descriptive metadata elements are present and valid in order for a SIP to be eligible for ingest into FDsys.	R1B; Must
RD-220	4.8.0-4.0-1	The OriginInfo:publisher MODS descriptive metadata element shall be considered mandatory.	R1B; Must
RD-221	4.8.0-4.0-2	The OriginInfo:dateIssued, Captured, Created, Modified, Valid, or Other MODS descriptive metadata elements shall be considered mandatory.	R1B; Must
RD-222	4.8.0-4.0-3	The Language MODS descriptive metadata elements shall be considered mandatory.	R1B; Must
RD-223	4.8.0-4.0-4	The Identifier MODS descriptive metadata elements shall be considered mandatory.	R1B; Must
RD-224	4.8.0-4.0-5	The Location MODS descriptive metadata elements shall be considered mandatory.	R1B; Must
RD-225	4.8.0-4.0-6	The PhysicalDescription:internetMediaType MODS descriptive metadata elements shall be considered mandatory.	R1B; Must
RD-226	4.8.0-4.0-7	The PhysicalDescription:digitalOrigin MODS descriptive metadata elements shall be considered mandatory.	R1B; Must
RD-227	4.8.0-4.0-8	The PhysicalDescription:extent MODS descriptive metadata elements shall be considered mandatory.	R1B; Must
RD-228	4.8.0-4.0-9	The TypeOfResource MODS descriptive metadata elements shall be considered mandatory.	R1B; Must
RD-229	4.8.0-4.0-10	The RecordInfo MODS descriptive metadata elements shall be considered mandatory.	R1B; Must
RD-230	4.8.0-4.0-11	The TitleInfo:title MODS descriptive metadata elements shall be considered mandatory	R1C, Must

RD-231	4.9	***4.9 SIP Administrative Metadata Requirements***	
RD-232	4.9.0-1	The system shall support the capability for the SIP to contain administrative metadata that conform to a METS extension schema.	R1B; Must
RD-233	4.9.0-1.0-1	The SIP shall identify the extension schema to which each administrative metadata file conforms.	R1B; Must
RD-234	4.9.0-1.0-2	The METS extension schema identified for an administrative metadata file in the SIP shall be registered in the Metadata Registry.	R1B; Must
RD-235	4.9.0-1.0-3	The system shall verify that each administrative metadata file in the SIP conforms to its identified METS extension schema.	R1B; Must
RD-236	4.9.0-1.0-4	The system shall have the capability to include technical metadata about each rendition in the SIP.	R1B; Must
RD-237	4.9.0-1.0-5	The system shall have the capability to include source metadata about each rendition in the SIP.	R1B; Must
RD-238	4.9.0-1.0-6	The system shall have the capability to include rights metadata about each rendition in the SIP.	R1B; Must
RD-239	4.9.0-1.0-7	The system shall have the capability to include provenance metadata about each rendition in the SIP.	R1B; Must
RD-240	4.9.0-1.0-8	The system shall have the capability to include system metadata about each rendition in the SIP.	R1B; Must
RD-241	5	**5 Requirements for AIP**	
RD-242	5.1	***5.1 AIP Core Capabilities***	
RD-243	5.1.0-1	An AIP shall contain one or more renditions of one publication.	R1B; Must
RD-244	5.1.0-1.0-1	An AIP shall only be created for SIPs that contain a publication that is in scope for GPO's dissemination programs.	R2; Must
RD-245	5.1.0-1.0-2	The AIP shall provide the capability to contain a rendition of the publication in the format in which it was created.	R1B; Must
RD-246	5.1.0-1.0-3	The system shall provide the capability for authorized users to add renditions of a publication to an AIP.	R1B; Must

RD-247	5.1.0-1.0-4	The system shall provide the capability for authorized users to delete renditions of a publication from an AIP.	R1C; Must
RD-248	5.1.0-2	The AIP shall provide the capability to include more than one rendition of a publication.	R1B; Must
RD-249	5.1.0-2.0-1	Each rendition of a publication in an AIP shall be contained in its own subdirectory of the content directory.	R1B; Must
RD-250	5.1.0-2.0-2	A rendition of a publication in an AIP shall contain one or more files.	R1B; Must
RD-251	5.1.0-2.0-3	A rendition of a publication in an AIP shall contain one or more subdirectories.	R1B; Must
RD-252	5.1.0-2.0-4	Each rendition of a publication in an AIP shall contain metadata that indicates if that rendition is a copy of the original file in which the publication was created.	R1B; Must
RD-253	5.1.0-2.0-5	Each rendition of a publication in an AIP shall contain metadata that indicates if that rendition is the highest fidelity rendition of the publication in the AIP.	R1B; Must
RD-254	5.1.0-2.0-6	Each rendition of a publication in an AIP shall contain metadata that indicates if that rendition is in a screen optimized format.	R1B; Must
RD-255	5.1.0-2.0-7	Each rendition of a publication in an AIP shall contain metadata that indicates if that rendition is in a print optimized format.	R1B; Must
RD-256	5.1.0-2.0-8	Each rendition of a publication in an AIP shall contain metadata that indicates if that rendition is in a press optimized format.	R1B; Must
RD-257	5.1.0-2.0-9	Each rendition of a publication in an AIP shall contain metadata that indicates if that rendition is a complete representation of the publication.	R1B; Must
RD-258	5.1.0-2.0-10	Each rendition of a publication in an AIP shall contain metadata that indicates if that rendition can be successfully edited using the software that created the rendition.	R1B; Must
RD-259	5.1.0-3	The AIP shall contain Representation Information metadata for every rendition of the publication in the AIP.	R1B; Must
RD-260	5.1.0-4	The system shall support the creation of AIPs which are independent of any particular hardware and software component.	R1B; Must
RD-261	5.1.0-4.0-1	The system shall provide the capability to add content to an AIP independent of the content's digital format.	R1B; Must
RD-262	5.1.0-4.0-2	The system shall provide the capability to store content in an AIP independent of the content's digital format.	R1B; Must
RD-263	5.1.0-4.0-3	The system shall provide the capability to deliver content stored in an AIP regardless of the content's digital format.	R1B; Must
RD-264	5.1.0-5	The system shall provide the capability for authorized users to access AIPs for the purpose of executing preservation processes or dissemination of DIPs from AIPs.	R1B; Must
RD-265	5.1.0-5.0-1	The system shall provide the capability for authorized users to access AIPs for the purpose of executing preservation processes on AIPs.	R1B; Must
RD-266	5.1.0-5.0-2	The system shall provide the capability for authorized users to access AIPs for the purpose of disseminating DIPs from AIPs.	R1B; Must
RD-268	5.1.0-7	An AIP shall contain a METS file named aip.xml.	R1B; Must
RD-269	5.1.0-7.0-1	The aip.xml file shall contain an inventory of all the content files in an AIP.	R1B; Must
RD-270	5.1.0-7.0-2	The aip.xml file shall contain an inventory of all the metadata files in an AIP.	R1B; Must
RD-271	5.1.0-7.0-3	The aip.xml file shall contain the relationships between the content files and metadata files in an AIP.	R1B; Must
RD-272	5.1.0-7.0-4	The system shall provide the capability for one or more metadata files to be related to each content file in an AIP.	R1B; Must
RD-273	5.1.0-7.0-5	The system shall provide the capability for each metadata file to be related to one or more content files in an AIP.	R1B; Must
RD-274	5.1.0-8	The AIP shall contain one or more metadata files associated with the content.	R1B; Must
RD-275	5.1.0-8.0-1	The system shall provide the capability to store an XML schema that describes the format of a content file in an AIP.	R1B; Must
RD-276	5.1.0-8.0-2	The system shall provide the capability to store an XML DTD that describes the format of a content file in an AIP.	R1B; Must
RD-277	5.1.0-9	The system shall provide the capability for authorized users to delete AIPs.	R1C; Must
RD-278	5.1.0-9.0-1	In order to delete an AIP, two authorized users shall be required to approve the deletion.	R1C; Must
RD-279	5.1.0-9.0-2	The system shall provide a user the capability to restrict an AIP, disabling the capability to create an ACP from it.	R1C; Must

RD-280	5.2	***5.2 Requirements for aip.xml File***	

RD-281	5.2.0-1	The aip.xml file shall conform to the METS version 1.5.	R1B; Must
RD-282	5.2.0-2	The aip.xml file shall conform to the GPO METS Profile version 1.0.	R1B; Must
RD-283	5.2.0-3	Digital objects in the AIP shall be stored outside the aip.xml file.	R1B; Must
RD-284	5.2.0-3.0-1	Digital objects in the AIP shall be referred to in the aip.xml file using their filename and full path relative to the root of the AIP.	R1B; Must
RD-285	5.2.0-4	Metadata files in the AIP shall be stored outside the aip.xml file.	R1B; Must
RD-286	5.2.0-4.0-1	Metadata files in the AIP shall be referred to in the aip.xml file using their filename and full path relative to the root of the AIP.	R1B; Must
RD-287	5.2.0-5	A metadata file shall be associated with one or more digital objects inside the aip.xml file.	R1B; Must

RD-288	5.3	## *5.3 Structural Layout for AIPs*	
RD-289	5.3.0-1	The AIP shall contain the aip.xml at the top level of the AIP directory structure.	R1B; Must
RD-290	5.3.0-1.0-1	The SIP shall contain a directory named content at the top level of the AIP directory structure.	R1B; Must
RD-291	5.3.0-1.0-2	The AIP shall contain a directory named metadata at the top level of the AIP directory structure.	R1B; Must
RD-292	5.3.0-2	The content files for each rendition of a publication in an AIP shall be placed in its own subdirectory under the content directory.	R1B; Must
RD-293	5.3.0-2.0-1	The hierarchical structure of the digital objects in a rendition folder shall be recorded in the aip.xml file.	R1B; Must
RD-295	5.3.0-3	All metadata files shall be placed in the metadata directory.	R1B; Must
RD-296	5.3.0-3.0-1	The metadata files for each rendition of a publication in an AIP shall be placed in its own subdirectory under the metadata directory.	R1B; Must
RD-297	5.3.0-3.0-1.0-1	The metadata subdirectory for a rendition shall have the same name as the content subdirectory for that rendition.	R1B; Must
RD-298	5.3.0-4	Each content file in a rendition shall have, at a minimum, a metadata file specifying technical parameters of the content file.	R1B; Must

RD-299	5.4	## *5.4 AIP Metadata*	
RD-300	5.4.0-1	Metadata files in a SIP shall be encoded in XML.	R1B; Must
RD-301	5.4.0-1.0-1	Metadata files in an AIP shall conform to an XML Schema or XML DTD that is registered in the Fdsys Metadata Schema Registry.	R1C; Must
RD-302	5.4.0-2	The AIP shall include preservation metadata to record preservation processes, from ingest into the repository through disposal.	R1C; Must
RD-303	5.4.0-3	The system shall store descriptive metadata elements in the AIP in MODS version 3.1 format.	R1B; Must
RD-304	5.4.0-3.0-1	The system shall have the capability to store descriptive metadata in ONIX format in the AIP.	R2; Must
RD-305	5.4.0-3.0-2	The system shall have the capability to store descriptive metadata in Dublin Core format in the AIP.	R1B; Must
RD-306	5.4.0-3.0-3	The system shall have the capability to store descriptive metadata in PREMIS format in the AIP.	R1B; Must
RD-307	5.4.0-3.0-4	The system shall have the capability to store descriptive metadata in COSATI format in the AIP.	R3; Must
RD-308	5.4.0-3.0-5	The system shall have the capability to store descriptive metadata in MODS format in the AIP.	R1B; Must
RD-309	5.4.0-3.0-6	The system shall have the capability to store descriptive metadata in additional descriptive metadata formats in the future in the AIP.	R3; Must
RD-310	5.4.0-3.0-7	The AIP shall incorporate all descriptive metadata elements from the SIP.	R1B; Must
RD-311	5.4.0-4	The AIP shall include metadata that expresses Preservation Description Information (PDI) according to the PREMIS Data Dictionary and extension schema which implement it.	R1C; Must
RD-312	5.4.0-5	The system shall support the capability for the AIP to contain administrative metadata that conform to a METS extension schema.	R1B; Must
RD-313	5.4.0-5.0-1	The AIP shall identify the METS extension schema to which each administrative metadata file conforms.	R1B; Must
RD-314	5.4.0-5.0-2	The METS extension schema identified for an administrative metadata file in the AIP shall be registered in the Metadata Registry.	R1B; Must
RD-315	5.4.0-5.0-3	The system shall verify that each administrative metadata file in the AIP	R1B; Must

		conforms to its identified METS extension schema.	
RD-316	5.4.0-5.0-4	The AIP shall have the capability to include Preservation Description Information (PDI) about each rendition included in the AIP.	R1B; Must
RD-317	5.4.0-5.0-5	The system shall have the capability to include technical metadata about each rendition in the AIP.	R1B; Must
RD-318	5.4.0-5.0-6	The system shall have the capability to include source metadata about each rendition in the AIP.	R1C; Must
RD-319	5.4.0-5.0-7	The system shall have the capability to include rights metadata about each rendition in the AIP.	R1B; Must
RD-320	5.4.0-5.0-8	The system shall have the capability to include provenance metadata about each rendition in the AIP.	R1B; Must

RD-321	5.5	***5.5 AIP Unique ID***	
RD-322	5.5.0-1	The AIP shall include the unique identification number assigned to the content in the SIP.	R1B; Must

RD-323	6	**6 Requirements for ACP**	
RD-324	6.1	***6.1 ACP Core Capabilities***	
RD-325	6.1.0-1	An ACP shall contain copies of one or more renditions of one publication.	R1C; Must
RD-326	6.1.0-1.0-1	The system shall provide the capability for authorized users to add renditions of a publication to an ACP.	R1C; Must
RD-327	6.1.0-1.0-2	The ACP shall have the capability to be retained in the system for period of time as is indicated in metadata.	R1C; Must
RD-328	6.1.0-1.0-3	The system shall provide the user the capability to alter the length of time to retain an ACP in the system.	R2; Must
RD-329	6.1.0-1.0-4	The system shall provide the capability for an authorized user to transform renditions of ACPs.	R2; Must
RD-330	6.1.0-1.0-5	The system shall create an ACP from its corresponding AIP when the AIP is accessed at a rate more than a user configurable frequency.	R2; Must
RD-331	6.1.0-1.0-6	The system shall provide the capability for authorized users to delete renditions of a publication from an ACP.	R1C; Must
RD-332	6.1.0-2	The ACP shall have the capability to include the following:	R1C; Must
RD-333	6.1.0-2.0-1	The ACP shall have the capability to include renditions of publications that are not in scope of GPO's dissemination programs.	R1C; Must
RD-334	6.1.0-2.0-2	The ACP shall have the capability to include renditions derived from AIP renditions.	R1C; Must
RD-335	6.1.0-2.0-3	The system shall create one or more access derivative renditions for an ACP if its corresponding AIP has no access derivative renditions.	R2; Must
RD-337	6.1.0-3	The ACP shall have the capability to contain one content unit (e.g., publication, report, issue, bill, document, volume) that may consist of one or more digital objects.	R1C; Must
RD-338	6.1.0-4	The ACP shall have the capability to include all digital objects included in its corresponding AIP.	R1C; Must
RD-339	6.1.0-5	The ACP shall contain a copy of the metadata files for each rendition which was copied from its corresponding AIP.	R1C; Must
RD-340	6.1.0-6	The access time for an ACP shall be as less than or equal to the access time for its corresponding AIP.	R1C; Must
RD-341	6.1.0-7	The ACP shall have the capability to replicate the structural layout of an AIP.	R1C; Could
RD-344	6.1.0-10	The ACP shall have the capability to be linked to one AIP, known as its corresponding AIP.	R1C; Must
RD-345	6.1.0-11	The ACP shall have the capability to include copies of one or more renditions from its corresponding AIP.	R1C; Must
RD-346	6.1.0-11.0-1	The ACP shall include copies of renditions from its corresponding AIP based on business rules.	R1C; Must
RD-347	6.1.0-11.0-2	The ACP shall have the capability to include copies of all renditions from its corresponding AIP whose metadata indicates they are screen optimized renditions.	R1C; Must

RD-348	6.1.0-11.0-3	The ACP shall have the capability to include copies of all renditions from its corresponding AIP whose metadata indicates they are press optimized renditions.	R1C; Must
RD-349	6.1.0-11.0-4	The ACP shall have the capability to include copies of all renditions from its corresponding AIP whose metadata indicates they are print optimized renditions.	R1C; Must
RD-350	6.1.0-12	The system provide the capability for authorized users to delete entire ACPs.	R1C; Must

RD-351	6.2	***6.2 ACP Binding Metadata File***	
RD-352	6.2.0-1	An ACP shall have the capability to contain a METS file named acp.xml.	R1C; Must
RD-353	6.2.0-1.0-1	The acp.xml file shall conform to the METS version 1.5.	R1C; Must
RD-354	6.2.0-1.0-1.0-1	The acp.xml file shall conform to the GPO METS Profile version 1.0.	R1C; Must
RD-355	6.2.0-1.0-2	Digital objects in the ACP shall be stored outside the acp.xml file.	R1C; Must
RD-356	6.2.0-1.0-3	The system shall provide the capability to include metadata files as required to support access and delivery	R1C; Must
RD-357	6.2.0-1.0-4	The system shall provide the capability to associate metadata files with one or more digital objects in the ACP.	R1C; Must

RD-358	6.3	***6.3 ACP Metadata***	
RD-359	6.3.0-1	Metadata files in an ACP shall be encoded in XML.	R1C; Must
RD-361	6.3.0-3	The system shall provide the capability to add structural and descriptive metadata for digital objects at a level of granularity that facilitates access.	R1C; Must
RD-363	6.3.0-5	The system shall have the capability to use descriptive metadata extension schema to support access to publications.	R1C; Must
RD-364	6.3.0-5.0-1	The system shall provide the capability to use descriptive metadata in MODS format to support access to publications.	R1B; Must
RD-365	6.3.0-5.0-2	The system shall provide the capability to use descriptive metadata in ONIX format to support access to publications.	R2; Must
RD-366	6.3.0-5.0-3	The system shall provide the capability to use descriptive metadata in Dublin Core format to support access to publications.	R1B; Must
RD-367	6.3.0-5.0-4	The system shall provide the capability to use descriptive metadata in PREMIS format to support access to publications.	R1B; Must
RD-368	6.3.0-5.0-5	The system shall provide the capability to use descriptive metadata in COSATI format to support access to publications.	R3; Must
RD-369	6.3.0-5.0-6	The system shall support the capability to use additional descriptive metadata formats in the future to support access to publications.	R3; Must
RD-370	6.3.0-6	The ACP shall have the capability to include mandatory descriptive metadata elements from the AIP and SIP.	R1C; Must
RD-371	6.3.0-7	The ACP shall have the capability to refer to extension schema for additional structural metadata as appropriate to the class of object and as necessary for access and delivery.	R1C; Must
RD-372	6.3.0-8	The ACP shall contain administrative metadata that conform to a METS extension schema	R1C; Must
RD-373	6.3.0-8.0-1	The ACP shall identify the METS extension schema to which each administrative metadata file conforms.	R1C; Must
RD-374	6.3.0-8.0-2	The METS extension schema identified for an administrative metadata file in the ACP shall be registered in the Metadata Registry.	R1C; Must
RD-375	6.3.0-8.0-3	The system shall verify that each administrative metadata file in the ACP conforms to its identified METS extension schema.	R1C; Must
RD-376	6.3.0-8.0-4	The system shall have the capability to include technical metadata about each rendition in the ACP.	R1C; Must
RD-377	6.3.0-8.0-5	The system shall have the capability to include source metadata about each rendition in the ACP.	R1C; Must
RD-378	6.3.0-8.0-6	The system shall have the capability to include rights metadata about each rendition in the ACP.	R1C; Must
RD-379	6.3.0-8.0-7	The system shall have the capability to include provenance metadata about each rendition in the ACP.	R1C; Must
RD-380	6.3.0-9	The system shall provide the capability to generate metadata that enables access to special publications at a level of granularity less than a single publication.	R1C; Must

RD-381	6.3.0-9.0-1	The ACP shall have the capability to include the unique ID assigned to the SIP and AIP in metadata.	R1C; Must

RD-382	7	**7 Requirements for DIP**	
RD-383	7.1	***7.1 DIP Core Capabilities***	
RD-384	7.1.0-1	The system shall create a DIP in response to a user request for a publication.	R1B; Must
RD-385	7.1.0-1.0-1	A DIP shall provide the capability to contain copies of one or more renditions of one publication.	R1B; Must
RD-386	7.1.0-1.0-2	A DIP shall provide the capability to contain copies of the metadata about each rendition it contains.	R1B; Must
RD-387	7.1.0-1.0-3	The system shall copy content and metadata to a DIP from the publication's ACP.	R1B; Must
RD-388	7.1.0-1.0-4	The system shall copy content and metadata to a DIP from the publication's AIP when the information needed is not present in the ACP.	R1B; Must
RD-389	7.1.0-1.0-5	The system shall provide the capability to generate screen optimized versions of renditions for inclusion in the DIP.	R1C; Must
RD-390	7.1.0-1.0-6	A DIP created for a service provider shall have the capability to contain the order information for the publication.	R1C; Must
RD-391	7.1.0-2	The DIP shall have the capability to include transient copies of digital objects that are optimized for delivery from the system.	R1B; Must
RD-392	7.1.0-3	The DIP shall have the capability to contain one content unit (e.g., publication, report, issue, bill, document, volume) that may consist of one or more digital objects.	R1B; Must
RD-393	7.1.0-4	The DIP shall have the capability to refer to or embed one or more metadata files associated with the content.	R1B; Must
RD-394	7.1.0-5	The DIP shall have the capability to refer to or embed one or more digital objects associated with metadata.	R1B; Must
RD-395	7.1.0-6	The system shall provide the capability to deliver DIPs that only include content metadata.	R1B; Must
RD-396	7.1.0-7	The DIP shall have the capability to be an exact replica of the AIP.	R1B; Must
RD-397	7.1.0-8	The DIP Metadata shall have the capability to include descriptive, structural, technical, administrative, and packaging metadata necessary for delivery from the system.	R1B; Must
RD-398	7.1.0-8.0-1	The DIP Metadata shall have the capability to include descriptive metadata necessary for delivery from the system.	R1B; Must
RD-399	7.1.0-8.0-2	The DIP Metadata shall have the capability to include structural metadata necessary for delivery from the system.	R1B; Must
RD-400	7.1.0-8.0-3	The DIP Metadata shall have the capability to include technical metadata necessary for delivery from the system.	R1B; Must
RD-401	7.1.0-8.0-4	The DIP Metadata shall have the capability to include administrative metadata necessary for delivery from the system.	R1B; Must
RD-402	7.1.0-8.0-5	The DIP Metadata shall have the capability to include packaging metadata necessary for delivery from the system.	R1B; Must
RD-403	7.1.0-8.0-6	The DIP Metadata shall have the capability to include system metadata necessary for delivery from the system.	R1B; Must
RD-405	7.1.0-10	The system shall have the capability to assemble optimally packaged DIPs based on the content type desired by the user.	R1C; Must
RD-406	7.1.0-11	The system shall provide the capability to deliver DIPs that only include one or more digital objects.	R1C; Must

RD-408	7.2	***7.2 DIP Binding Metadata File***	
RD-409	7.2.0-1	A DIP shall provide the capability to contain a METS file named dip.xml.	R1B; Must
RD-410	7.2.0-1.0-1	The dip.xml file shall conform to the METS version 1.5.	R1B; Must
RD-411	7.2.0-1.0-1.0-1	The dip.xml file shall conform to the GPO METS Profile version 1.0.	R1B; Must
RD-412	7.2.0-1.0-2	The system shall provide the capability to refer to digital objects (e.g., XML, OCR-ed text) as required to support delivery.	R1B; Must
RD-413	7.2.0-1.0-2.0-1	The system shall provide the capability to embed digital objects (e.g., XML,	R2; Must

		OCR-ed text) as required to support delivery	
RD-414	7.2.0-1.0-3	The system shall provide the capability to refer to metadata files (e.g., MARC, ONIX, Dublin Core, MODS) as required to support delivery.	R1B; Must
RD-415	7.2.0-1.0-3.0-1	The system shall provide the capability to embed metadata files (e.g., MARC, ONIX, Dublin Core, MODS) as required to support delivery.	R2; Must
RD-416	7.2.0-1.0-4	The system shall provide the capability to associate content metadata files with one or more digital objects in the DIP.	R1B; Must

RD-417	7.3	***7.3 DIP Metadata***	
RD-418	7.3.0-1	The system shall have the capability to encode metadata files in XML and conform to schema that are adopted by Fdsys, according to Fdsys Content Metadata requirements.	R1B; Must
RD-420	7.3.0-3	The DIP shall have the capability to include mandatory descriptive metadata elements from the SIP, ACP, and AIP.	R1B; Must
RD-421	7.3.0-4	The system shall provide the capability to copy descriptive metadata to a DIP.	R1B; Must
RD-422	7.3.0-4.0-1	The system shall provide the capability to copy descriptive metadata in MODS format to a DIP.	R1B; Must
RD-423	7.3.0-4.0-2	The system shall provide the capability to copy descriptive metadata in ONIX format to a DIP.	R2; Must
RD-424	7.3.0-4.0-3	The system shall provide the capability to copy descriptive metadata in Dublin Core format to a DIP.	R2; Must
RD-425	7.3.0-4.0-4	The system shall provide the capability to copy descriptive metadata in PREMIS format to a DIP.	R2; Must
RD-426	7.3.0-4.0-5	The system shall provide the capability to copy descriptive metadata in COSATI format to a DIP.	R3; Must
RD-427	7.3.0-4.0-6	The system shall support the capability to copy additional descriptive metadata formats to the DIP in the future.	R3; Must
RD-430	7.3.0-7	The DIP shall have the capability to include Business Process Information, including information collected about orders from the CO Ordering function and requests made by end users.	R1B; Must
RD-431	7.3.0-8	The system shall provide the capability to include information generated as a result of Content Originator ordering.	R1B; Must
RD-432	7.3.0-9	The system shall provide the capability to include information generated as a result of a user request.	R1B; Must
RD-433	7.3.0-10	The DIP shall have the capability to include the unique ID for any content or metadata being delivered in the DIP.	R1C; Must
RD-434	7.3.0-11	The system shall provide the capability to support the Open Archives Initiative Metadata Harvesting Protocol version (TBD-434A).	R3; Must

RD-435	8	**8 Requirements for Pre-ingest Processes**	
RD-436	8.1	***8.1 Pre-ingest Processing***	
RD-437	8.1.0-1	The system shall have the capability to read registered metadata schema to extract metadata for use by the system.	R1B; Must
RD-438	8.1.0-2	The system shall accept content from Content Originators.	R1B; Must
RD-439	8.1.0-3	The system shall accept jobs from Content Originator ordering.	R1B; Must
RD-440	8.1.0-4	The system shall accept deposited content created without using style tools.	R1B; Must
RD-441	8.1.0-5	The system shall accept deposited content created using style tools.	R2; Could / R3; Must
RD-442	8.1.0-6	The system shall accept converted content.	R1B; Must
RD-443	8.1.0-7	The system shall accept harvested content.	R1B; Must
RD-444	8.1.0-8	The system shall have the capability to apply version control.	R1B; Must
RD-445	8.1.0-9	The system shall detect duplicate content in the system and notify authorized users.	R1B; Must
RD-446	8.1.0-9.0-1	The system shall determine if the version of content is already in the system, using, at a minimum: Version Information, bibliographic information,	R1B; Must

		authentication information, content (e.g., hashes)	
RD-447	8.1.0-9.0-1.0-1	The system shall determine if the version of content is already in the system using version information.	R1B; Must
RD-448	8.1.0-9.0-1.0-2	The system shall determine if the version of content is already in the system using bibliographic information.	R1B; Must
RD-449	8.1.0-9.0-1.0-3	The system shall determine if the version of content is already in the system based on its content.	R1B; Must
RD-450	8.1.0-9.0-1.0-4	The system shall have the capability to detect near duplicate documents.	R3; Must
RD-451	8.1.0-9.0-2	The system shall have the capability to reject duplicate content.	R1B; Must
RD-452	8.1.0-9.0-2.0-1	The system shall notify users when duplicate content is detected.	R1B; Must
RD-453	8.1.0-9.0-2.0-2	The system shall notify users when near duplicate content is detected.	R3; Must
RD-454	8.1.0-10	The system shall have the capability to store content in WIP before job order information is received.	R1B; Must
RD-455	8.1.0-11	The system shall have the capability to assign a unique ID to content.	R1B; Must
RD-456	8.1.0-11.0-1	The system shall have the capability to assign a unique ID to content packages.	R1B; Must
RD-457	8.1.0-11.0-2	The system shall have the capability to assign a unique ID to digital objects.	R1B; Must
RD-458	8.1.0-12	The system shall have the capability to assign a unique ID to jobs.	R1B; Must
RD-459	8.1.0-13	The system shall populate the Identifier field in the corresponding MODS record with the content unique ID.	R1B; Must
RD-460	8.1.0-14	The system shall link related jobs, business process information (BPI), and content.	R1B; Must
RD-461	8.1.0-15	The system shall allow Content Evaluators to make scope determinations.	R1B; Must
RD-462	8.1.0-15.0-1	The system shall have the capability to make automatic scope determinations based on metadata.	R1C; Must
RD-463	8.1.0-15.0-2	The system shall have the capability to make automatic scope determinations based on BPI	R1C; Must
RD-464	8.1.0-15.0-3	The system shall have the capability to make automatic scope determinations based on content.	R3; Must
RD-465	8.1.0-15.0-4	The system shall allow users to modify the criteria by which the system makes automatic scope determinations.	R1C; Must
RD-466	8.1.0-15.0-5	The system shall provide a GUI interface for users to modify the criteria for automatic scope determinations	R2; Must
RD-467	8.1.0-16	The system shall have the capability to perform integrity checking.	R1B; Must
RD-468	8.1.0-17	The system shall have the capability to apply a digital time stamp to content.	R1B; Must
RD-469	8.1.0-18	The system shall have the capability to perform accessibility assessments.	R2; Must
RD-470	8.1.0-18.0-1	The system shall have the capability to allow users to manually perform 508 accessibility assessments on content.	R1B; Must
RD-471	8.1.0-18.0-2	The system shall have the capability to automatically perform 508 accessibility assessments on content.	R2; Must
RD-472	8.1.0-19	The system shall have the capability to support the creation of a pre-ingest bundle (PIB).	R1C; Must
RD-473	8.1.0-20	The system shall have the capability to accept modified packages from the Service Provider after publisher approval.	R1C; Must
RD-474	8.1.0-21	The system shall have the capability to accept modified digital objects from the Service Provider after publisher approval.	R1C; Must
RD-475	8.1.0-22	The system shall accept publisher approval information for SIP creation.	R1B; Must
RD-476	8.1.0-23	The system shall have the capability to assemble content and metadata to create SIPs.	R1B; Must
RD-477	8.1.0-24	The system shall have the capability to create a log of all transactions and activities.	R1B; Must
RD-407	8.1.0-25	The system shall have the capability to make automatic scope determinations.	R1C; Must
RD-478	9	**9 Requirements for Ingest Processing**	
RD-479	9.1	***9.1 Ingest Processing Core Capabilities***	
RD-480	9.1.0-1	Ingest processing performs the following functions:	
RD-481	9.1.0-1.0-1	Accept and validate SIPs	R1B; Must

RD-482	9.1.0-1.0-1.0-1	Ingest processing shall accept SIPs.	R1B; Must
RD-483	9.1.0-1.0-1.0-2	Ingest Processing shall validate SIPs.	R1B; Must
RD-484	9.1.0-1.0-2	Ingest processing shall have the capability to create AIPs from SIPs.	R1B; Must
RD-485	9.1.0-1.0-3	Ingest Processing shall have the capability to create ACPs from SIPs.	R1B; Must
RD-486	9.1.0-1.0-4	Ingest Processing shall apply a digital time stamp to content. Clarification: This item is meant to refer to recording a timestamp in metadata whenever content is received.	R1B; Must

RD-487	9.2	***9.2 Ingest Processing***	
RD-488	9.2.0-1	The system shall have the capability to transform textual content metadata into XML.	R2; Must
RD-489	9.2.0-2	The system shall support the capability to conform to future requirements for SIP validation.	R3; Must
RD-490	9.2.0-3	The system shall allow authorized users to submit content to ingest once content has been approved for release by the publisher.	R1B; Must
RD-491	9.2.0-3.0-1	The system shall provide a prompt to confirm that the user intends to submit the SIP to ingest.	R1B; Should
RD-492	9.2.0-4	The system shall validate that SIPs conform to requirements for a system compliant SIP.	R1B; Must
RD-493	9.2.0-4.0-1	The system shall verify that the SIP includes all mandatory metadata elements.	R1B; Must
RD-494	9.2.0-4.0-2	The system shall verify that the METS file is valid.	R1B; Must
RD-495	9.2.0-4.0-3	The system shall verify that at least one digital object is present.	R1B; Must
RD-497	9.2.0-5	The system shall provide the capability to reject non-conforming SIPs.	R1B; Must
RD-498	9.2.0-5.0-1	The system shall direct exceptions to authorized users.	R1B; Must
RD-499	9.2.0-5.0-1.0-1	The system shall provide the capability for authorized users to process SIPs to conform to SIP validation.	R1B; Must
RD-500	9.2.0-6	The system shall provide the capability to notify users that a SIP is nonconforming.	R1B; Must
RD-501	9.2.0-7	The system shall provide the capability to notify users of the reasons a SIP is nonconforming.	R1B; Must
RD-502	9.2.0-8	The system shall verify the file format of a digital object by a means other than mime type or file extension.	R1C; Must
RD-503	9.2.0-9	The system shall have the capability to verify content integrity (e.g., checksum).	R1B; Must
RD-506	9.2.0-12	The system shall have the capability to create a log of all transactions and activities.	R1B; Must

RD-507	10	**10 Requirements for Preservation Processing**	
RD-508	10.1	***10.1 Preservation Processing Core Capabilities***	
RD-509	10.1.0-1	The system shall have the ability to store AIPs in a preservation repository environment.	R1B; Must
RD-510	10.1.0-1.0-1	AIPs shall remain free from corruption and remain accessible as GPO undergoes changes in information technology and infrastructure.	R1B; Must
RD-511	10.1.0-1.0-1.0-1	AIPs shall remain free from corruption as GPO undergoes changes in information technology and infrastructure.	R1B; Must
RD-512	10.1.0-1.0-1.0-2	AIPs shall remain accessible as GPO undergoes changes in information technology and infrastructure.	R1B; Must
RD-513	10.1.0-2	The system shall manage preservation processes, including scheduled assessments and resulting actions, based on the attributes of the digital objects and apply the specified processes.	R2; Must
RD-515	10.1.0-3	The system shall maintain the integrity of content throughout preservation processes.	R2; Must

RD-516	10.1.0-3.0-1	The system shall ensure content is fully intelligible and unchanged in meaning and representation, compared to the original AIP, when a digital object goes through preservation processes	R2; Must
RD-517	10.1.0-4	The system shall preserve essential behaviors of digital content when a digital object goes through a preservation process.	R2; Must
RD-518	10.1.0-4.0-1	The system shall maintain content functionality associated with content presentation when a digital object goes through a preservation process.	R2; Must
RD-519	10.1.0-5	The system shall preserve significant properties and attributes of digital content as a digital object goes through a preservation process.	R2; Must
RD-520	10.1.0-5.0-1	The system shall maintain content structure when a digital object goes through a preservation process	R2; Must
RD-521	10.1.0-5.0-2	The system shall maintain content structure when a digital object goes through a preservation process.	R2; Must
RD-522	10.1.0-5.0-3	The system shall maintain hyperlinks to content within the target document when a digital object goes through a preservation process.	R2; Must
RD-523	10.1.0-5.0-3.0-1	The system shall have the capability to notify users that they are leaving GPO's website when a user selects a hyperlink that takes them to an external site.	R2; Must
RD-525	10.1.0-6.0-1	The system shall have the capability to produce DIPs which are interoperable with other OAIS-based repositories.	R1C; Could / R2; Must
RD-526	10.1.0-7	The system shall be capable of scheduling or executing preservation processes on individual AIPs or on selected groups of archival content.	R2; Must
RD-527	10.1.0-7.0-1	The system shall be capable of scheduling preservation processes on individual AIPs.	R2; Must
RD-528	10.1.0-7.0-2	The system shall be capable of scheduling preservation processes on selected groups of archival content.	R2; Must
RD-529	10.1.0-7.0-3	The system shall be capable of executing preservation processes on individual AIPs.	R2; Must
RD-530	10.1.0-7.0-4	The system shall be capable of executing preservation processes on selected groups of archival content.	R2; Must

RD-531	10.2	***10.2 Preservation Processing***	
RD-532	10.2.0-1	The system shall have the capability to transform digital object(s) into a digital object of another format.	R3; Must
RD-533	10.2.0-2	The system shall have the ability to migrate data to formats other than those in which the files were created or received.	R2; Must
RD-534	10.2.0-3	The system shall support the transformation of Quark digital objects as defined below:	R2; Must
RD-535	10.2.0-3.0-1	The system shall ensure that the files resulting from migrations will be in a format free of proprietary restrictions to the possible extent.	R1C; Should / R2; Must
RD-536	10.2.0-3.0-2	The system shall have the ability to verify that a file migrated from one format to another retains specified attributes and behaviors, i.e. is authentic and faithful.	R2; Must
RD-537	10.2.0-3.0-3	The system shall support the transformation of Quark digital objects in previous versions of Quark into Quark digital objects of the current shipping version of Quark as of 10-13-06.	R2; Must
RD-538	10.2.0-3.0-4	The system shall support the transformation of Quark digital objects into HTML digital objects.	R2; Must
RD-539	10.2.0-3.0-5	The system shall support the transformation of Quark digital objects into ASCII digital objects.	R2; Must
RD-540	10.2.0-3.0-6	The system shall support the transformation of Quark digital objects into XML digital objects.	R2; Must
RD-541	10.2.0-3.0-7	The system shall support the transformation of Quark digital objects into PDF digital objects.	R2; Must
RD-542	10.2.0-3.0-8	The system shall support the ability to set parameters of the output file of the transformation (resolution, color depth, etc).	R2; Must
RD-543	10.2.0-4	The system shall support the transformation of InDesign digital objects as defined below:	R2; Must
RD-544	10.2.0-4.0-1	The system shall support the transformation of InDesign digital objects in previous versions of InDesign into InDesign digital objects of the current shipping version of InDesign as of 10-13-06.	R2; Must

RD-545	10.2.0-4.0-2	The system shall support the transformation of InDesign digital objects into HTML digital objects.	R2; Must
RD-546	10.2.0-4.0-3	The system shall support the transformation of InDesign digital objects into ASCII digital objects.	R2; Must
RD-547	10.2.0-4.0-4	The system shall support the transformation of InDesign digital objects into XML digital objects.	R2; Must
RD-548	10.2.0-4.0-5	The system shall support the transformation of InDesign digital objects into PDF digital objects.	R2; Must
RD-549	10.2.0-5	The system shall support the transformation of Microsoft Word digital objects as defined below:	R2; Must
RD-550	10.2.0-5.0-1	The system shall support the transformation of Microsoft Word digital objects in previous versions of Microsoft Word into Microsoft Word digital objects of the current shipping version of Microsoft Word as of 10-13-06.	R2; Must
RD-551	10.2.0-5.0-2	The system shall support the transformation of Microsoft Word digital objects into HTML digital objects.	R2; Must
RD-552	10.2.0-5.0-3	The system shall support the transformation of Microsoft Word digital objects into ASCII digital objects.	R2; Must
RD-553	10.2.0-5.0-4	The system shall support the transformation of Microsoft Word digital objects into XML digital objects.	R2; Must
RD-554	10.2.0-5.0-5	The system shall support the transformation of Microsoft Word digital objects into PDF digital objects.	R2; Must
RD-555	10.2.0-5.0-6	The system shall support the transformation of Microsoft Word digital objects into Open Document digital objects.	R2; Must
RD-557	10.2.0-5.0-7	The system shall have the ability to produce notification of incomplete or unsuccessful migrations.	R2; Must
RD-558	10.2.0-5.0-7.0-1	The system shall have the ability to identify incomplete or unsuccessful migrations.	R2; Must
RD-559	10.2.0-5.0-7.0-2	The system shall have the ability to produce notification of incomplete or unsuccessful migrations.	R2; Must
RD-556	10.2.0-6	The system shall support the transformation of Microsoft Excel digital objects as defined below:	R2; Must
RD-560	10.2.0-6.0-1	The system shall support the transformation of Microsoft Excel digital objects in previous versions of Microsoft Excel into Microsoft Excel digital objects of the current shipping version of Microsoft Excel as of 10-13-06.	R2; Must
RD-561	10.2.0-6.0-2	The system shall support the transformation of Microsoft Excel digital objects into HTML digital objects.	R2; Must
RD-562	10.2.0-6.0-3	The system shall support the transformation of Microsoft Excel digital objects into ASCII digital objects.	R2; Must
RD-563	10.2.0-6.0-4	The system shall support the transformation of Microsoft Excel digital objects into XML digital objects.	R2; Must
RD-564	10.2.0-6.0-5	The system shall support the transformation of Microsoft Excel digital objects into PDF digital objects.	R2; Must
RD-565	10.2.0-6.0-6	The system shall support the transformation of Microsoft Excel digital objects into Open Document digital objects.	R2; Must
RD-566	10.2.0-7	The system shall support the transformation of Microsoft PowerPoint digital objects as defined below:	R2; Must
RD-567	10.2.0-7.0-1	The system shall support the transformation of Microsoft PowerPoint digital objects in previous versions of Microsoft PowerPoint into Microsoft PowerPoint digital objects of the current shipping version of Microsoft PowerPoint as of 10-13-06.	R2; Must
RD-568	10.2.0-7.0-2	The system shall support the transformation of Microsoft PowerPoint digital objects into HTML digital objects.	R2; Must
RD-569	10.2.0-7.0-3	The system shall support the transformation of Microsoft PowerPoint digital objects into ASCII digital objects.	R2; Must
RD-570	10.2.0-7.0-4	The system shall support the transformation of Microsoft PowerPoint digital objects into XML digital objects.	R2; Must
RD-571	10.2.0-7.0-5	The system shall support the transformation of Microsoft PowerPoint digital objects into PDF digital objects.	R2; Must
RD-572	10.2.0-7.0-6	The system shall support the transformation of Microsoft PowerPoint digital objects into Open Document digital objects.	R2; Must
RD-573	10.2.0-8	The system shall support the transformation of PDF digital objects as defined below:	R2; Must
RD-574	10.2.0-8.0-1	The system shall support the transformation of PDF digital objects in previous versions of PDF into PDF digital objects of the current shipping version of PDF as of 10-13-06.	R2; Must

RD-575	10.2.0-8.0-2	The system shall support the transformation of PDF digital objects into HTML digital objects.	R2; Must
RD-576	10.2.0-8.0-3	The system shall support the transformation of PDF digital objects into ASCII digital objects.	R2; Must
RD-577	10.2.0-8.0-4	The system shall support the transformation of PDF digital objects into XML digital objects.	R2; Must
RD-578	10.2.0-8.0-5	The system shall support the transformation of HTML digital objects into PDF digital objects.	R2; Must
RD-579	10.2.0-8.0-6	The system shall support the transformation of HTML digital objects into XHTML digital objects.	R2; Must
RD-580	10.2.0-9	The system shall support the transformation of HTML digital objects as defined below:	R2; Must
RD-581	10.2.0-9.0-1	The system shall support the transformation of HTML digital objects in previous versions of HTML into HTML digital objects of the current version of HTML as of 10-13-06.	R2; Must
RD-582	10.2.0-9.0-2	The system shall support the transformation of HTML digital objects into ASCII digital objects.	R2; Must
RD-583	10.2.0-9.0-3	The system shall support the transformation of HTML digital objects into XML digital objects.	R2; Must
RD-584	10.2.0-10	The system shall support the transformation of TIFF digital objects as defined below:	R2; Must
RD-585	10.2.0-10.0-1	The system shall support the transformation of TIFF digital objects in previous versions of TIFF into TIFF digital objects of the current version of TIFF as of 10-13-06.	R2; Must
RD-586	10.2.0-10.0-2	The system shall support the transformation of the full text index of any TIFF digital object into an ASCII digital object.	R2; Must
RD-587	10.2.0-10.0-3	The system shall support the transformation of the full text index of any TIFF digital object into an XML digital object.	R2; Must
RD-588	10.2.0-10.0-4	The system shall support the transformation of the full text index of any TIFF digital object into an HTML digital object.	R2; Must
RD-589	10.2.0-10.0-5	The system shall support the transformation a TIFF digital object into a JPG digital object.	R2; Must
RD-590	10.2.0-10.0-6	The system shall support the transformation of the full text index of any TIFF digital object into an PDF digital object.	R2; Must
RD-591	10.2.0-11	The system shall provide an interface to integrate transforming technologies as required.	R1B; Must
RD-592	10.2.0-12	Where formats containing images are transformed to formats that do not support images (e.g. ASCII, XML) the descriptive text of said images, if any, will be stored in the new format.	R2; Must
RD-593	10.2.0-13	Where formats containing images are transformed to XML the placement of said images, if any, will be stored in the new format	R2; Must
RD-594	10.2.0-14	The system shall support the transformation of WordPerfect digital objects as defined below:	R2; Must
RD-595	10.2.0-14.0-1	The system shall support the transformation of WordPerfect digital objects in previous versions of WordPerfect into WordPerfect digital objects of the current shipping version of WordPerfect as of as of 10-13-06.	R2; Must
RD-596	10.2.0-14.0-2	The system shall support the transformation of WordPerfect digital objects into Microsoft Word digital objects.	R2; Must
RD-597	10.2.0-14.0-3	The system shall support the transformation of WordPerfect digital objects into HTML digital objects.	R2; Must
RD-598	10.2.0-14.0-4	The system shall support the transformation of WordPerfect digital objects into ASCII digital objects.	R2; Must
RD-599	10.2.0-14.0-5	The system shall support the transformation of WordPerfect digital objects into XML digital objects.	R2; Must
RD-600	10.2.0-14.0-6	The system shall support the transformation of WordPerfect digital objects into PDF digital objects.	R2; Must
RD-601	10.2.0-15	The system shall support the transformation of EPS digital objects as defined below:	R2; Must
RD-602	10.2.0-15.0-1	The system shall support the transformation of EPS digital objects in previous versions of EPS into EPS digital objects of the current version of EPS as of as of 10-13-06.	R2; Must
RD-603	10.2.0-15.0-2	The system shall support the transformation of the full text index of any EPS digital object into an ASCII digital object	R2; Must
RD-604	10.2.0-15.0-3	The system shall support the transformation of the full text index of any EPS digital object into an XML digital object	R2; Must

RD-605	10.2.0-15.0-4	The system shall support the transformation of the full text index of any EPS digital object into an HTML digital object	R2; Must
RD-606	10.2.0-15.0-5	The system shall support the transformation of the full text index of any EPS digital object into an PDF digital object	R2; Must
RD-607	10.2.0-16	The system shall support the transformation of JPG digital objects in previous versions of JPG into JPG digital objects of the current version of JPG as of 10-13-06.	R2; Must
RD-608	10.2.0-17	The system shall support the transformation of XML as defined below:	R2; Must
RD-609	10.2.0-17.0-1	The system shall support the transformation of XML digital objects into other registered XML digital objects.	R2; Must
RD-610	10.2.0-17.0-2	The system shall support the transformation of XML metadata into other registered XML metadata.	R2; Must
RD-611	10.2.0-17.0-3	The system shall support the transformation of system metadata into other registered XML metadata.	R2; Must
RD-612	10.2.0-18	The system shall have the capability to perform transformations without deleting the content that has been acted upon.	R2; Must
RD-613	10.2.0-19	The system shall provide the capability to apply quality metrics to format transformations.	R2; Must
RD-614	10.2.0-20	The system shall ensure content submitted is not changed by refreshment.	R1C; Must
RD-615	10.2.0-20.0-1	The system shall have the ability to verify that the refreshed file is authentic and faithful.	R1C; Must
RD-616	10.2.0-20.0-2	The system shall provide logs that record the results of refreshment processes.	R1C; Must
RD-617	10.2.0-20.0-3	The system shall have the ability to notify users of incomplete or unsuccessful refreshment processes.	R1C; Must
RD-618	10.2.0-20.0-3.0-1	The system shall have the ability to identify incomplete or unsuccessful refreshments processes.	R1C; Must
RD-619	10.2.0-20.0-3.0-2	The system shall have the ability to produce notification of incomplete or unsuccessful refreshments processes.	R1C; Must
RD-620	10.2.0-21	The system shall have the ability to support emulation to preserve access to content.	R2; Must
RD-621	10.2.0-21.0-1	The system shall have the ability to verify that the emulated file retains specified attributes and behaviors, i.e. is authentic and faithful.	R2; Must
RD-622	10.2.0-22	The system shall support the transformation of AIPs into ACPs.	R2; Must
RD-623	10.2.0-23	When a preservation process results in the creation of an additional rendition in an AIP, the system shall be capable of retaining the as-ingested rendition of the content in the AIP.	R2; Must

RD-624	10.3	***10.3 Preservation Processing – Assessment***	
RD-625	10.3.0-1	The system shall have the ability to assess ingested content and determine preservation processes based on the assessments.	R2; Must
RD-626	10.3.0-1.0-1	The system shall allow scheduling of preservation assessments. Content attributes include, at a minimum, completeness, determination of structure, file format, file size, and fitness for use.	R2; Must
RD-627	10.3.0-1.0-2	There shall be no limit set on the number or frequency of assessments.	R2; Must
RD-628	10.3.0-1.0-3	The system shall have the ability to re-assess content stored in the system.	R2; Must
RD-629	10.3.0-2	The system shall present a range of options to the Service Specialist for decision if the system is unable to make a determination.	R3; Could

RD-630	10.4	***10.4 Preservation Processing – Administration***	
RD-631	10.4.0-1	The system shall support scheduling the automatic execution of preservation processes.	R2; Must
RD-632	10.4.0-2	The system shall support batch Content Preservation of content.	R2; Must
RD-633	10.4.0-3	The system shall support Content Preservation on an item-by-item basis.	R2; Must
RD-634	10.4.0-4	The system shall maintain an audit trail of preservation processes.	R2; Must
RD-635	10.4.0-5	The system shall support the ability for authorized users to request	R2; Must

		preservation processes.	

RD-636	10.5	***10.5 Preservation Processing – Storage***	
RD-637	10.5.0-1	The system shall provide a digital archival repository environment which is based on open-standards architecture.	R1C; Must
RD-638	10.5.0-1.0-1	The repository environment shall keep AIPs separate from working or production copies.	R1C; Must
RD-639	10.5.0-1.0-2	The system shall ensure that when content in AIP is changed, the content in the ACP is changed.	R1C; Must
RD-640	10.5.0-1.0-3	The system shall maintain one on more backups of the repository environment consistent with the overall Fdsys storage requirements.	R1C; Must

RD-641	10.6	***10.6 Preservation Processing – Metadata***	
RD-642	10.6.0-1	The system shall capture or generate metadata which specifies the relationship of files resulting from preservation processes to their predecessors.	R2; Must
RD-643	10.6.0-2	The system shall use the PREMIS Preservation Metadata Schema version 1.0	R1C; Must
RD-644	10.6.0-3	The system shall employ PREMIS Preservation Metadata Schema version 1.0 for facilitating preservation processes.	R1C; Must

RD-645	10.7	***10.7 Preservation Processing – Security***	
RD-646	10.7.0-1	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).	R2; Must

RD-647	11	**11 Requirements for Unique Identifier**	
RD-648	11.0-1	The system shall allow an authorized user to apply a new level of granularity to content without affecting previously applied levels.	R1C; Must
RD-649	11.0-2	The system shall assign unique IDs.	R1B; Must
RD-650	11.0-3	Unique ID shall be human-readable.	R1B; Must
RD-651	11.0-4	Unique ID shall be expressible in XML ID.	R1B; Must
RD-652	11.0-5	Unique ID shall be an alphanumeric identifier (ANI).	R1B; Must
RD-653	11.0-6	The system shall allow for the pre-assignment of unique IDs to external entities.	R1B; Must
RD-654	11.0-7	The system shall only accept unique IDs created by the system.	R1B; Must
RD-655	11.0-8	The system shall provide the capability to apply unique IDs to digital objects.	R1B; Must
RD-656	11.0-9	Unique ID characters shall include numbers 0-9 and letters A (minus I and O).	R1B; Must
RD-657	11.0-10	Unique ID shall be stored in Metadata.	R1B; Must
RD-658	11.0-11	Unique ID shall be unique.	R1B; Must

RD-659	11.1	***11.1 Unique ID Core Capabilities***	
RD-660	11.1.0-1	The system shall support granularity of any content based on the natural granularity boundaries of that content.	R2; Must
RD-661	11.1.0-1.0-1	The system shall support granularity of GPO Access content referenced in RD-2596 based on the natural granularity boundaries of that content.	R1C; Must
RD-662	11.1.0-2	The system shall allow GPO to define the level of granularity that content can be retrieved at.	R1B; Must
RD-663	11.1.0-2.0-1	The system shall have the capability for a user to decide the level of granularity that should be applied to a publication.	R1C; Must

RD-664	11.1.0-2.0-1.0-1	The system shall have the capability for a user to apply multiple levels of granularity to a publication (e.g. the whole publication can be found, every paragraph in the publication can be found but images can not be separately found).	R1C; Must
RD-665	11.1.0-2.0-1.0-2	The system shall allow elements to be retrieved by at all levels of granularity	R1C; Must
RD-666	11.1.0-2.0-2	The system shall support granularity to the level of a publication.	R1B; Must
RD-667	11.1.0-2.0-3	The system shall support granularity down to the level of any paragraph in a publication.	R1C; Should / R2; Must
RD-668	11.1.0-2.0-4	The system shall support granularity down to the level of any individual graphic	R1C; Must
RD-669	11.1.0-2.0-5	The system shall support granularity down to the level of any embedded graphical element in a publication	R1C; Should / R2; Must
RD-671	11.1.0-2.0-7	The system shall support granularity down to the level of any frame of a video.	R3; Must
RD-673	11.1.0-2.0-9	The system shall support granularity of audio down to smallest segment of time the audios encoding allows.	R3; Should
RD-679	11.1.0-3.0-5	The system shall provide the capability to support 1 trillion Digital Objects without software redesign.	R1C; Must
RD-685	11.1.0-7	The system shall support granularity down to the level of any section in a publication, as appropriate based on natural content boundaries.	R1C; Must
RD-686	11.1.0-8	The system shall support granularity down to the level of any article in a publication, as appropriate based on natural content boundaries.	R1C; Must
RD-687	11.1.0-9	The system shall provide the capability to display granular content in search results	R1C; Must
RD-688	11.1.0-10	The system shall provide the capability to associate granular content in search results with the entire publication.	R1C; Must
RD-689	11.1.0-11	The system shall provide the capability to associate granular content in the content detail with the entire publication.	R1C; Must
RD-690	11.1.0-12	The system shall provide the capability to deliver granular content separate from the entire publication.	R1C; Must
RD-691	11.1.0-13	The system shall provide the capability to deliver granular content in conjunction with the entire publication.	R1C; Must
RD-692	11.1.0-14	The system shall provide the capability to deliver text-based granular content in a PDF format that has been optimized for rapid access and delivery.	R1C; Must
RD-693	11.1.0-15	The system shall provide the capability to deliver text-based granular content in a HTML format that has been optimized for rapid access and delivery.	R1C; Must
RD-694	11.1.0-16	The system shall provide the capability to deliver text-based granular content in a text format that has been optimized for rapid access and delivery.	R1C; Must
RD-695	11.1.0-17	The system shall provide the capability to deliver text-based granular content in a XML format that has been optimized for rapid access and delivery.	R1C; Must
RD-696	11.1.0-18	The system shall provide the capability to transform text-based granular content into formats that have been optimized for access and delivery if these formats are not already present in the ACP.	R1C; Must
RD-697	11.1.0-19	The system shall provide the capability to deliver PDF granules at a page level of granularity.	R1C; Must
RD-698	11.1.0-20	The system shall provide the capability to deliver PDF granules at a page range level of granularity if the granules span multiple pages.	R1C; Must
RD-699	11.1.0-21	The system shall provide the capability to deliver PDF access renditions that are identical in formatting to the print rendition, if a print rendition is available.	R1C; Must

RD-700	11.2	***11.2 Job ID***	R1C; Must
RD-701	11.2.0-1	The system shall create and assign a unique ID for each job.	R1B; Must
RD-702	11.2.0-2	The system shall provide the capability to assign a unique IDs to each job.	R1B; Must
RD-703	11.2.0-2.0-1	The system shall provide the capability to assign unique IDs to Content Originator orders of content jobs.	R1B; Must
RD-704	11.2.0-2.0-2	The system shall provide the capability to assign unique IDs to Content Originator orders of service jobs.	R1B; Must
RD-705	11.2.0-2.0-3	The system shall provide the capability to assign unique IDs to non-Content Originator order related jobs.	R1B; Must
RD-706	11.2.0-3	The system shall not re-use Job unique IDs.	R1B; Must

RD-707	11.3	***11.3 Content Package ID***	
RD-708	11.3.0-1	The system shall create and assign a unique ID for each Content Package.	R1B; Must
RD-709	11.3.0-1.0-1	The system shall create and assign a unique ID to each SIP.	R1B; Must
RD-710	11.3.0-1.0-2	The system shall create and assign a unique ID to each AIP.	R1B; Must
RD-711	11.3.0-1.0-2.0-1	The AIP shall inherit the unique ID from the SIP if an ACP is not created.	R1B; Must
RD-712	11.3.0-1.0-2.0-2	The ACP shall inherit the unique ID from the SIP if an AIP is not created.	R1B; Must
RD-713	11.3.0-1.0-3	The system shall create and assign a unique ID to each ACP.	R1B; Must
RD-715	11.3.0-2	Content Package unique IDs shall be unique.	R1B; Must
RD-716	11.3.0-3	The system shall record package unique ID's in metadata.	R1B; Must

RD-717	11.4	***11.4 Interface for Unique ID***	
RD-718	11.4.0-1	The system shall allow the capability for a user to input a unique ID and retrieve content and information about the content associated with that ID.	R1B; Must
RD-719	11.4.0-1.0-1	The system shall allow the capability for an authorized user to input a unique ID.	R1B; Must
RD-720	11.4.0-1.0-2	The system shall allow the capability for an authorized user to retrieve content and information about the content associated with a unique ID.	R1B; Must
RD-721	11.4.0-1.0-3	The system shall allow the capability for an authorized user to input an agency supplied ID.	R1B; Must
RD-722	11.4.0-1.0-4	The system shall allow the capability for an authorized user to retrieve content and information about the content associated with an agency supplied ID.	R1B; Must
RD-723	11.4.0-1.0-5	The system shall restrict access to information about content associated with unique IDs according to user profiles and the FDsys security requirements (e.g., End User inputting an internal Job ID).	R1B; Must

RD-724	12	**12 Requirements for Persistent Name**	
RD-725	12.1	***12.1 Persistent Name Core Capabilities***	
RD-726	12.1.0-1	The system shall assign persistent names to all in-scope published versions during access processing.	R1C; Must
RD-727	12.1.0-1.0-1	Persistent name shall not conflict with other identifiers within FDsys.	R1C; Must
RD-728	12.1.0-2	The system shall comply with the following standards and best practices pertaining to persistent naming.	R1C; Must
RD-729	12.1.0-2.0-1	Persistent Identification: A Key Component Of An E-Government Infrastructure. CENDI Persistent Identification Task Group (March 10, 2004)	R1C; Must
RD-730	12.1.0-2.0-2	Interagency Committee on Government Information Recommendations to the Office of Management and Budget (December 17, 2004)	R1C; Must
RD-731	12.1.0-2.0-3	RFC 1737 Functional Requirements for Uniform Resource Names (December 1994)	R1C; Must
RD-732	12.1.0-2.0-4	RFC 2141 URN Syntax (May 1997)	R1C; Must
RD-733	12.1.0-2.0-5	RFC 2396 Uniform Resource Identifiers (URI): Generic Syntax (August 1998)	R1C; Must
RD-734	12.1.0-3	The system shall support interoperability across different naming systems to allow one system to access a resource within another.	R3; Should
RD-735	12.1.0-4	The system shall accommodate OpenURL syntax to enable federated searching.	R3; Must
RD-736	12.1.0-5	The system shall support the persistent name supplied by GPO as the definitive persistent name.	R1C; Must
RD-737	12.1.0-5.0-1	The system shall allow GPO to elect other systems or agencies to become recognized GPO naming authorities.	R1C; Must
RD-738	12.1.0-6	The system shall assign persistent names that are location independent.	R1C; Must
RD-739	12.1.0-7	The system shall assign persistent names that are protocol independent.	R3; Must
RD-740	12.1.0-8	Persistent names shall be unique.	R1C; Must
RD-741	12.1.0-9	The system shall have the capability to assign intelligent persistent names.	R1C; Must

RD-742	12.1.0-9.0-1	The system shall have the capability to assign predictable persistent names.	R1C; Must
RD-743	12.1.0-10	The system shall have the capability to assign non-intelligent persistent names.	R1C; Could
RD-745	12.1.0-12	The system shall have the capability to record the date and time of persistent name creation.	R1C; Must
RD-746	12.1.0-12.0-1	Date and time of the persistent name creation shall be recorded in metadata.	R1C; Must
RD-747	12.1.0-13	The system shall have the capability to create reports about persistent name management.	R2; Could
RD-748	12.1.0-14	The system shall resolve legacy existing GPO naming schemes.	R1C; Must
RD-749	12.1.0-14.0-1	The system shall resolve existing PURLs.	R1C; Must
RD-750	12.1.0-14.0-2	The system shall resolve existing URLS that were constructed using GetDoc.	R1C; Must
RD-751	12.1.0-14.0-3	The system shall resolve existing URLS that were constructed using GetPage.	R1C; Must
RD-752	12.1.0-14.0-4	The system shall resolve existing URLS that were constructed using GetCFR.	R1C; Must
RD-753	12.1.0-15	The system shall support one persistent name per AIP.	R1C; Must

RD-754	12.2	***12.2 Persistent Name Resolution***	
RD-755	12.2.0-1	The system shall use a resolution system to locate and provide access to content with persistent names.	R1C; Must
RD-756	12.2.0-1.0-1	The resolution process shall resolve an assigned name into a resource or the resource metadata.	R1C; Must
RD-757	12.2.0-1.0-2	The resolution process shall allow for persistent name recognition within standard browsers.	R1C; Must
RD-758	12.2.0-2	The system shall have the capability to support distributed persistent naming and resolution at the local and global level.	R1C; Must
RD-759	12.2.0-3	The system shall support resolution of a single persistent name to multiple distributed locations.	R1C; Should
RD-760	12.2.0-3.0-1	The system shall be able to identify and resolve to multiple identical copies of a resource at multiple locations through a single persistent name.	R1C; Should
RD-761	12.2.0-4	The system shall support resolution of a single persistent name to multiple content versions.	R1C; Should
RD-762	12.2.0-4.0-1	The system shall determine the most appropriate rendition based on attributes of the request.	R1C; Should

RD-763	12.3	***12.3 Persistent Name Metadata***	
RD-764	12.3.0-1	The system shall record persistent names associated with content.	R1C; Must
RD-765	12.3.0-2	The system shall record existing persistent names associated with content.	R1C; Must
RD-766	12.3.0-3	The system shall provide the capability to associate metadata with the persistent name	R1C; Must

RD-767	13	**13 Requirements for Authentication**	
RD-768	13.1	***13.1 Authentication Core Capabilities***	
RD-769	13.1.0-1	The system shall provide the capability to certify content as authentic.	R1C; Must
RD-776	13.1.0-4	The system shall provide the capability to certify content as official.	R1C; Must
RD-777	13.1.0-4.0-1	In some situations, Content Originators direct that specific content delivery methods, file formats, or content presentations must be used for the purpose of legal citation. As directed by a Content Originator, GPO shall record information about this designation (intended use) in metadata.	R1C; Must
RD-778	13.1.0-5	The system shall provide the capability to certify content at levels of granularity defined by GPO.	R2; Must
RD-779	13.1.0-6	The system shall provide the capability to convey certification by means of an integrity mark.	R1C; Must
RD-780	13.1.0-7	The system shall provide the capability to use GPO's Public Key Infrastructure (PKI).	R1C; Must
RD-783	13.1.0-10	The system shall provide the capability to use public key cryptography, digital certificates, encryption or other widely accepted information security	R1C; Must

		mechanisms for providing authentication services within Fdsys.	

RD-784	13.2	***13.2 Authentication – Content Pre-ingest and Ingest***	
RD-785	13.2.0-1	The system shall provide the capability to verify and validate the authenticity, integrity, and official status of deposited content.	R1C; Must
RD-786	13.2.0-1.0-1	The system shall provide the capability to validate the authenticity of deposited content.	R1C; Must
RD-787	13.2.0-1.0-2	The system shall provide the capability to validate the integrity of deposited content.	R1C; Must
RD-788	13.2.0-1.0-3	The system shall provide the capability to validate the official status of deposited content.	R1C; Must
RD-789	13.2.0-1.0-4	The system shall verify the identity and authority of authorized users.	R1C; Must
RD-790	13.2.0-1.0-5	Valid proof of the user's identity shall be logged by the system.	R1C; Must
RD-791	13.2.0-1.0-6	The source (e.g., OriginInfo:publisher) of the deposited content shall be recorded in metadata.	R1B; Must
RD-792	13.2.0-1.0-7	The system shall ensure that deposited content has not been altered or destroyed in an unauthorized manner during transmission from the authorized user to the system, and information about content integrity should be recorded in metadata.	R1C; Must
RD-793	13.2.0-1.0-7.0-1	The system shall validate that deposited content has not been altered in an unauthorized manner during transmission from the authorized user to the system.	R1C; Must
RD-794	13.2.0-1.0-7.0-2	The system shall validate that deposited content has not been destroyed in an unauthorized manner during transmission from the authorized user to the system.	R1C; Must
RD-795	13.2.0-1.0-7.0-3	The system shall record information about deposited content integrity in metadata.	R1C; Must
RD-796	13.2.0-1.0-8	The system shall verify that the sender and the recipient were, in fact, the parties who claimed to send or receive content, respectively, and this information should be recorded in metadata.	R1C; Must
RD-797	13.2.0-1.0-8.0-1	The system shall verify that the content sender is, in fact, the party who claimed to have sent the content.	R1C; Must
RD-798	13.2.0-1.0-8.0-2	The system shall verify that the content recipient is, in fact, the party who claimed to have received the content.	R1C; Must
RD-799	13.2.0-1.0-8.0-3	The system shall record content sender and recipient information in metadata.	R1C; Must
RD-800	13.2.0-1.0-9	The system shall have the capability to record intended use in metadata.	R1C; Must
RD-801	13.2.0-1.0-10	The system shall have the capability to use PKI for the establishment of a trust model for deposited content.	R1C; Must
RD-802	13.2.0-2	The system shall provide the capability to verify and validate the authenticity, integrity, and official status of harvested content.	R2; Must
RD-803	13.2.0-2.0-1	The system shall provide the capability to validate the authenticity of harvested content.	R2; Must
RD-804	13.2.0-2.0-2	The system shall provide the capability to validate the integrity of harvested content.	R2; Must
RD-805	13.2.0-2.0-3	The system shall provide the capability to validate the official status of harvested content.	R2; Must
RD-806	13.2.0-2.0-4	The system shall examine harvested content for the purpose of verifying the source of the harvested content.	R2; Must
RD-807	13.2.0-2.0-5	The source (e.g., OriginInfo:publisher) of harvested content shall be recorded in metadata.	R2; Must
RD-808	13.2.0-2.0-6	The system shall ensure that harvested content has not been altered or destroyed in an unauthorized manner as compared to the source from which the content was harvested, and information about content integrity should be recorded in metadata.	R2; Must
RD-809	13.2.0-2.0-6.0-1	The system shall validate that harvested content has not been altered in an unauthorized manner as compared to the source from which the content was harvested.	R2; Must
RD-810	13.2.0-2.0-6.0-2	The system shall validate that harvested content has not been destroyed in an unauthorized manner as compared to the source from which the content was harvested.	R2; Must
RD-811	13.2.0-2.0-6.0-3	The system shall record information about the harvested content integrity in	R2; Must

		metadata.	
RD-812	13.2.0-3	The system shall provide the capability to verify and validate the authenticity, integrity, and official status of converted content.	R1C; Must
RD-813	13.2.0-3.0-1	The system shall provide the capability to validate the authenticity of converted content.	R1C; Must
RD-814	13.2.0-3.0-2	The system shall provide the capability to validate the integrity of converted content.	R1C; Must
RD-815	13.2.0-3.0-3	The system shall provide the capability to validate the official status of converted content.	R1C; Must
RD-816	13.2.0-3.0-4	The source (e.g., OriginInfo:publisher) of converted content shall be recorded in metadata.	R1B; Must
RD-817	13.2.0-3.0-5	The source (e.g., OriginInfo:publisher) of tangible content that was used to create the converted content shall be recorded in metadata.	R1B; Must
RD-818	13.2.0-3.0-6	The system shall ensure that converted content has not been altered or destroyed in an unauthorized manner during transmission from authorized users to the system, and information about content integrity should be recorded in metadata.	R1C; Must
RD-819	13.2.0-3.0-6.0-1	The system shall validate that converted content has not been altered in an unauthorized manner during transmission to the system.	R1C; Must
RD-820	13.2.0-3.0-6.0-2	The system shall validate that converted content has not been destroyed in an unauthorized manner during transmission to the system.	R1C; Must
RD-821	13.2.0-3.0-6.0-3	The system shall record information about converted content integrity in metadata.	R1C; Must
RD-822	13.2.0-3.0-7	The system shall verify that the sender and the recipient were, in fact, the parties who claimed to send or receive content, respectively, and this information should be recorded in metadata.	R1C; Must
RD-823	13.2.0-3.0-7.0-1	The system shall verify that the sender is, in fact, the party who claimed to have sent the converted content.	R1C; Must
RD-824	13.2.0-3.0-7.0-2	The system shall verify that the recipient is, in fact, the party who claimed to have received the converted content.	R1C; Must
RD-825	13.2.0-3.0-7.0-3	The system shall record the sender and the recipient information in metadata.	R1C; Must
RD-826	13.2.0-3.0-8	The system shall have the capability to record intended use in metadata.	R1B; Must
RD-827	13.2.0-3.0-9	The system shall have the capability to use PKI for the establishment of a trust model for converted content.	R1C; Must
RD-828	13.2.0-4	The system shall provide the capability to recognize and validate integrity marks at pre-ingest.	R1C; Must
RD-829	13.2.0-4.0-1	The system shall provide the capability to recognize integrity marks at pre-ingest.	R1C; Must
RD-830	13.2.0-4.0-2	The system shall provide the capability to validate integrity marks at pre-ingest.	R1C; Must
RD-831	13.2.0-4.0-3	The system shall have the capability to retain integrity marks in accordance with GPO business rules.	R1C; Must
RD-832	13.2.0-4.0-4	Where public key cryptography and digital certificates are used by a Content Originator to create a digital signature integrity mark on content that is submitted to GPO for ingest into the system, the system shall record in metadata that a digital signature was present and make this information available to End Users.	R1C; Must
RD-833	13.2.0-4.0-4.0-1	Where public key cryptography and digital certificates are used by a Content Originator to create a digital signature integrity mark on content that is submitted to GPO for ingest into the system, the system shall record in metadata that a digital signature was present.	R1C; Must
RD-834	13.2.0-4.0-4.0-2	Where public key cryptography and digital certificates are used by a Content Originator to create a digital signature integrity mark on content that is submitted to GPO for ingest into the system, the system shall make metadata information concerning the presence of a digital signature available to End Users.	R1C; Must
RD-835	13.2.0-5	The system shall provide the capability to process encrypted files at pre-ingest.	R1C; Could / R2; Must
RD-836	13.2.0-6	The system shall record chain of custody information.	R1C; Must
RD-837	13.2.0-6.0-1	Chain of custody information shall be recorded in metadata.	R1C; Must
RD-838	13.2.0-6.0-2	The system shall have the capability to gather relevant information from integrity marks (e.g., digital signatures, digital certificates) for use as part of the chain of custody.	R1C; Must
RD-839	13.2.0-6.0-2.0-1	The system shall have the ability to gather Distinguished Name information from integrity marks for use as part of the chain of custody.	R1C; Must

RD-840	13.2.0-6.0-2.0-2	The system shall have the ability to gather information from integrity marks regarding the date the integrity mark was applied for use as part of the chain of custody.	R1C; Must
RD-841	13.2.0-6.0-2.0-3	The system shall have the ability to gather information from integrity marks regarding the time the integrity mark was applied for use as part of the chain of custody.	R1C; Must
RD-842	13.2.0-6.0-2.0-4	The system shall have the capability to record chain of custody in WIP.	R1C; Must
RD-843	13.2.0-6.0-2.0-5	The system shall have the ability to gather chain of custody from content metadata when it is not available from integrity marks.	R1C; Must
RD-844	13.2.0-6.0-2.0-6	The system shall update chain of custody information in metadata at ingest.	R1C; Must
RD-845	13.2.0-7	The system shall provide the capability to perform redundancy checking (e.g., checksum) on content at ingest.	R1C; Must
RD-846	13.2.0-7.0-1	The system shall provide the capability to record checksum type and value in metadata.	R1C; Must
RD-847	13.2.0-7.0-1.0-1	The system shall provide the capability to record checksum type in metadata.	R1C; Must
RD-848	13.2.0-7.0-1.0-2	The system shall provide the capability to record checksum value in metadata.	R1C; Must
RD-849	13.2.0-8	The system shall provide the capability to apply a digital timestamp to content at ingest.	R1C; Must

RD-851	13.3	***13.3 Authentication – User Credentials***	

RD-855	13.4	***13.4 Authentication – Content Integrity***	
RD-856	13.4.0-1	The system shall provide the capability to maintain content integrity by ensuring that content has not been altered or destroyed in an unauthorized manner.	R1B; Must
RD-857	13.4.0-1.0-1	The system shall provide the capability to certify content integrity within the system by ensuring that content has not been altered in an unauthorized manner.	R1B; Must
RD-858	13.4.0-1.0-2	The system shall provide the capability to certify content integrity within the system by ensuring that content has not been destroyed in an unauthorized manner.	R1B; Must
RD-859	13.4.0-1.0-3	The system shall have the capability to ensure integrity of content within the system at a definable frequency.	R1B; Must
RD-860	13.4.0-1.0-4	The system shall have the capability to ensure integrity of work in progress content.	R1B; Must
RD-863	13.4.0-2.0-2	The system shall not allow critical transaction and system log files to be adjusted by any unauthorized party.	R1B; Must
RD-864	13.4.0-2.0-2.0-1	The system shall not allow critical transaction files to be adjusted by any unauthorized party.	R1B; Must
RD-865	13.4.0-2.0-2.0-2	The system shall not allow system log files to be adjusted by any unauthorized party.	R1B; Must
RD-866	13.4.0-2.0-3	The system shall have the capability to certify integrity of content during backup and other system processes.	R1B; Must
RD-867	13.4.0-3	The system shall certify integrity of pre-ingested and ingested content.	R1C; Must
RD-868	13.4.0-3.0-1	The system shall certify integrity of pre-ingested content.	R1C; Must
RD-869	13.4.0-3.0-2	The system shall certify integrity of ingested content.	R1C; Must
RD-870	13.4.0-3.0-3	Content integrity shall be maintained during transmission from the Content Originator to the system.	R1C; Must
RD-871	13.4.0-3.0-4	The system shall have the capability to validate a cryptographic digital signature, in accordance with IETF RFC 3447 on content in pre-ingest, to ensure that the content has not been altered, and that the signer's certificate is valid before ingesting the content.	R1C; Must
RD-872	13.4.0-4	The system shall have the capability to certify integrity of delivered content.	R2; Must
RD-873	13.4.0-4.0-1	The system shall have the capability to apply a cryptographic digital signature, in accordance with IETF RFC 3447, to content delivered from the system.	R2; Must
RD-874	13.4.0-4.0-2	The system shall have the capability to verify that the electronic content is valid, uncorrupted, and free of malicious code.	R2; Must
RD-875	13.4.0-4.0-2.0-1	The system shall have the capability to verify that the electronic content is valid.	R2; Must
RD-876	13.4.0-4.0-2.0-2	The system shall have the capability to verify that the electronic content is	R2; Must

		uncorrupted.	
RD-877	13.4.0-4.0-2.0-3	The system shall have the capability to verify that the electronic content is free of malicious code.	R2; Must
RD-878	13.4.0-5	The system shall provide the capability to provide notification that a change has occurred to content within the system.	R2; Must
RD-879	13.4.0-5.0-1	The system shall provide the capability to notify designated users if content has been altered or destroyed in an unauthorized manner.	R2; Must
RD-880	13.4.0-5.0-1.0-1	The system shall provide the capability to notify designated users if content has been altered in an unauthorized manner.	R2; Must
RD-881	13.4.0-5.0-1.0-2	The system shall provide the capability to notify designated users if content has been destroyed in an unauthorized manner.	R2; Must
RD-882	13.4.0-5.0-2	The system shall provide the capability to notify designated users if content has been altered or destroyed in an authorized manner.	R2; Must
RD-883	13.4.0-5.0-2.0-1	The system shall provide the capability to notify designated users if content has been altered in an authorized manner.	R2; Must
RD-884	13.4.0-5.0-2.0-2	The system shall provide the capability to notify designated users if content has been destroyed in an authorized manner.	R2; Must
RD-885	13.4.0-5.0-3	The system shall provide the capability to notify designated users when changes were made to content.	R2; Must
RD-886	13.4.0-5.0-4	The system shall provide the capability to notify designated users where changes were made to content.	R2; Must
RD-887	13.4.0-5.0-5	The system shall provide the capability to notify designated users by whom changes were made to content.	R2; Must
RD-888	13.4.0-5.0-6	The system shall provide the capability to notify designated users what changes were made to content.	R2; Must
RD-889	13.4.0-5.0-7	The system shall log changes to content in metadata.	R2; Must
RD-890	13.4.0-6	The system shall provide the capability of demonstrating continued integrity of content packages when authorized changes are made (such as to the metadata).	R2; Must

RD-891	13.5	***13.5 Authentication – Time Stamps***	
RD-892	13.5.0-1	The system shall support digital time stamping.	R1C; Must
RD-893	13.5.0-2	The system shall provide the capability to provide date and time verification.	R1C; Must
RD-894	13.5.0-3	The system shall be flexible enough to provide date and time verification through various mechanisms including a time certification authority, network server, or the signerstem.	R1C; Must
RD-895	13.5.0-3.0-1	The system shall be flexible enough to provide date and time verification through a time certification authority.	R1C; Must
RD-896	13.5.0-3.0-2	The system shall be flexible enough to provide date and time verification through a network time server.	R1C; Must
RD-897	13.5.0-3.0-3	The system shall be flexible enough to provide date and time verification through the signer's system.	R1C; Must

RD-898	13.6	***13.6 Authentication – Integrity Marks***	
RD-899	13.6.0-1	The system shall support the use of integrity marks.	R2; Must
RD-900	13.6.0-2	Integrity marks shall include certification information.	R2; Must
RD-901	13.6.0-3	Integrity marks shall employ widely accepted information security mechanisms (e.g., public key cryptography, digital certificates, digital signatures, XML signatures, digital watermarks, or traditional watermarks).	R2; Must
RD-902	13.6.0-4	The system shall support the capability to manually add integrity marks to content.	R2; Could
RD-903	13.6.0-5	The system shall support the capability to automatically add integrity marks to content.	R2; Must
RD-904	13.6.0-6	The system shall support the use of visible integrity marks.	R1C; Must
RD-905	13.6.0-7	The system shall support the use of invisible integrity marks.	R1C; Must
RD-906	13.6.0-8	The system shall provide flexibility regarding where the integrity mark is applied through automated and manual processes.	R2; Must
RD-907	13.6.0-8.0-1	The system shall provide flexibility regarding where the integrity mark is applied through automated processes.	R2; Must
RD-908	13.6.0-8.0-2	The system shall provide flexibility regarding where the integrity mark is	R2; Must

		applied through manual processes.	
RD-909	13.6.0-9	The system shall provide the capability to automatically position the exact location (x, y coordinates) of where an integrity mark is applied for any set number of documents.	R2; Must
RD-910	13.6.0-10	The system shall support the application of multiple integrity marks on the same content.	R2; Must
RD-911	13.6.0-11	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.	R2; Must

RD-912	13.7	***13.7 Authentication – Content Delivery***	
RD-913	13.7.0-1	The system shall provide the capability for users to validate the authenticity, integrity, and official status of the content packages that are delivered from the system.	R2; Must
RD-914	13.7.0-1.0-1	The system shall provide the capability for users to validate the authenticity of the content packages that are delivered from the system.	R2; Must
RD-915	13.7.0-1.0-2	The system shall provide the capability for users to validate the integrity of the content packages that are delivered from the system.	R2; Must
RD-916	13.7.0-1.0-3	The system shall provide the capability for users to validate the official status of the content packages that are delivered from the system.	R2; Must
RD-917	13.7.0-2	The system shall enable GPO to add integrity marks to FDsys content that is delivered to End Users in the form of electronic presentation, hard copy output, and digital media.	R2; Must
RD-918	13.7.0-2.0-1	The system shall enable GPO to add integrity marks to FDsys content that is delivered to End Users in the form of electronic presentation.	R2; Must
RD-919	13.7.0-2.0-2	The system shall enable GPO to add integrity marks to FDsys content that is delivered to End Users in the form of hard copy output.	R2; Must
RD-920	13.7.0-2.0-3	The system shall enable GPO to add integrity marks to FDsys content that is delivered to End Users in the form of digital media.	R2; Must
RD-921	13.7.0-2.0-4	When electronic content in PDF format has been authenticated prior to ingest into FDsys (e.g., via the bulk signing tool), the system shall maintain that externally provided authentication.	R1C; Must
RD-922	13.7.0-2.0-5	When electronic content in PDF format has been authenticated prior to ingest into FDsys (e.g., via the bulk signing tool), the system shall deliver the integrity mark to End Users with that externally provided authentication still intact.	R1C; Must
RD-923	13.7.0-3	Where public key cryptography and digital certificates are used to create a digital signature integrity mark on delivered content the following shall apply:	R2; Must
RD-924	13.7.0-3.0-1	The integrity mark shall provide the capability to include the GPO Seal of Authenticity logo if the digital signature is a visible digital signature.	R2; Could
RD-925	13.7.0-3.0-2	The integrity mark shall include certification information.	R2; Must
RD-926	13.7.0-3.0-2.0-1	The integrity mark shall include the name of the certifying organization.	R2; Must
RD-927	13.7.0-3.0-2.0-2	The integrity mark shall include the date on the signer's digital certificate.	R2; Must
RD-928	13.7.0-3.0-2.0-3	The integrity mark shall include the digital time stamp.	R2; Must
RD-929	13.7.0-3.0-2.0-4	The integrity mark shall include the public key value of the signer.	R2; Must
RD-930	13.7.0-3.0-2.0-5	The integrity mark shall include identification of the hash algorithm used.	R2; Must
RD-931	13.7.0-3.0-2.0-6	The integrity mark shall include the reason for signing.	R2; Must
RD-932	13.7.0-3.0-2.0-7	The integrity mark shall include the signer's location.	R2; Must
RD-933	13.7.0-3.0-2.0-8	The integrity mark shall include the signer's contact information.	R2; Must
RD-934	13.7.0-3.0-2.0-9	The integrity mark shall include the name of the entity that certified the content.	R2; Must
RD-935	13.7.0-3.0-2.0-10	The integrity mark shall include the expiration date of the digital certificate used to sign the content.	R2; Must
RD-936	13.7.0-3.0-2.0-11	The integrity mark shall be flexible enough to include additional, GPO-defined certification information.	R2; Must
RD-937	13.7.0-3.0-3	The values for the integrity mark fields shall be extracted from the digital certificate that was used to create the digital signature.	R2; Must
RD-939	13.7.0-3.0-5	The system shall have the capability to confirm that the digital certificate that was used to create the digital signature is valid and accurate. As a result of the validation check, the system should notify users if the digital certificate is valid, invalid, or can not be validated.	R2; Must
RD-940	13.7.0-3.0-5.0-1	The system shall have the capability to confirm that the digital certificate that	R2; Must

		was used to create the digital signature is valid and accurate.	
RD-941	13.7.0-3.0-5.0-2	As a result of the digital signature validation check, the system should notify users if the digital certificate is valid, invalid, or cannot be validated.	R2; Must
RD-942	13.7.0-3.0-6	The system shall have the capability to perform a bit for bit comparison of the digital object as it was at the time of signing against the document as it was at the time of the validation check. As a result of the validation check, the system should notify users if the content has been modified, has not been modified, or if the system cannot determine if the content has been modified.	R2; Must
RD-943	13.7.0-3.0-6.0-1	The system shall have the capability to perform a bit for bit comparison of the digital object as it was at the time of signing against the document as it was at the time of the validation check.	R2; Must
RD-944	13.7.0-3.0-6.0-2	As a result of the validation check, the system should notify users if the content has been modified, has not been modified, or if the system cannot determine if the content has been modified.	R2; Must
RD-945	13.7.0-3.0-7	The digital signature shall include the date and time that the digital signature was applied to content, and the expiration date of the digital certificate.	R2; Must
RD-946	13.7.0-3.0-7.0-1	The digital signature shall include the date and time that the digital signature was applied to content.	R2; Must
RD-947	13.7.0-3.0-7.0-2	The digital signature shall include the expiration date of the digital certificate.	R2; Must
RD-948	13.7.0-3.0-8	Non-revoked certificates shall display a valid status regardless of the expiration date of the digital certificate. The validity of the digital certificate shall be based on the certificate validity at the time and date the content was digitally signed.	R1C; Should / R2; Must
RD-949	13.7.0-3.0-8.0-1	Non-revoked certificates shall display a valid status regardless of the expiration date of the digital certificate.	R1C; Should / R2; Must
RD-950	13.7.0-3.0-8.0-2	The validity of the digital certificate shall be based on the certificate validity at the time and date the content was digitally signed.	R1C; Should / R2; Must
RD-951	13.7.0-3.0-9	For electronic presentation, validation shall be done automatically without End User intervention.	R1C; Should / R2; Must

RD-952	13.8	***13.8 Re-authentication of Content***	
RD-953	13.8.0-1	The system shall provide the capability to re-authenticate content that has already been authenticated (e.g., expired certificate).	R1B; Could / R2; Must
RD-954	13.8.0-2	The system shall provide the capability to notify GPO System Administrators when content needs to be re-authenticated.	R1B; Could / R2; Must
RD-955	13.8.0-3	The system shall provide the capability for GPO to change or revoke the authentication status of content.	R1B; Must

RD-956	13.9	***13.9 Authentication Standards/Best Practices***	

RD-978	13.10	***13.10 Authentication Records Management***	
RD-979	13.10.0-1	The system shall create administrative records of authentication processes.	R2; Must
RD-980	13.10.0-2	The system shall create transaction records of administrative processes.	R2; Must
RD-981	13.10.0-3	The system shall support an audit capability for content certification.	R2; Must
RD-982	13.10.0-4	The system shall support an audit capability for content validation.	R2; Must
RD-983	13.10.0-5	The system shall comply with GPO and Federal records management policies.	R2; Must
RD-984	13.10.0-5.0-1	The system shall comply with GPO records management policies, as document in GPO Publication 840.7.	R2; Must
RD-985	13.10.0-5.0-2	The system shall comply with Federal records management policies (e.g., NARA's Records Management Guidance for Agencies Implementing	R2; Must

		Electronic Signature Technologies, 2000).	

RD-986	13.11	***13.11 Authentication Metadata***	
RD-987	13.11.0-1	The system shall provide the capability to include authentication and certification information in metadata.	R1C; Must
RD-988	13.11.0-1.0-1	The system shall provide the capability to include authenticity information in metadata.	R1C; Must
RD-989	13.11.0-1.0-1.0-1	Authenticity metadata shall have the capability to include the source of deposited, harvested, and converted content.	R1C; Must
RD-990	13.11.0-1.0-1.0-2	Authenticity metadata shall have the capability to include the Content Originator identity and authority to publish deposited content.	R1C; Must
RD-991	13.11.0-1.0-1.0-3	Authenticity metadata shall have the capability to include the source of tangible content that was used to create converted content.	R1C; Must
RD-992	13.11.0-1.0-1.0-4	Authenticity metadata shall have the capability to include the chain of custody information excluding information about End User chain of custody.	R1C; Must
RD-993	13.11.0-1.0-2	The system shall provide the capability to include integrity information in metadata.	R1C; Must
RD-994	13.11.0-1.0-2.0-1	Integrity metadata shall have the capability to include information about any pre-ingest and ingest integrity checks for transmission to the system.	R1C; Must
RD-995	13.11.0-1.0-2.0-2	Integrity metadata shall have the capability to include information about any integrity checks within the system.	R1C; Must
RD-996	13.11.0-1.0-2.0-3	Integrity metadata shall have the capability to include information about changes that are made.	R1C; Must
RD-997	13.11.0-1.0-2.0-4	Integrity metadata shall have the capability to include information about who makes a change.	R1C; Must
RD-998	13.11.0-1.0-2.0-5	Integrity metadata shall have the capability to include information about where a change is made.	R1C; Must
RD-999	13.11.0-1.0-2.0-6	Integrity metadata shall have the capability to include information about when a change is made.	R1C; Must
RD-1000	13.11.0-1.0-3	The system shall provide the capability to include non-repudiation information in metadata.	R1C; Must
RD-1001	13.11.0-1.0-3.0-1	Non-repudiation metadata shall have the capability to include the sender's identity and proof.	R1C; Must
RD-1002	13.11.0-1.0-3.0-2	Non-repudiation metadata shall have the capability to include the recipient's identity and proof.	R1C; Must
RD-1003	13.11.0-1.0-4	The system shall provide the capability to include intended use information in metadata.	R1C; Must
RD-1004	13.11.0-1.0-4.0-1	Intended Use metadata shall have the capability to identify the content delivery method designated by the Content Originator that must be used for the purpose of citation in court.	R1C; Must
RD-1005	13.11.0-1.0-4.0-2	Intended Use metadata shall have the capability to identify the file format designated by the Content Originator that must be used for the purpose of citation in court.	R1C; Must
RD-1006	13.11.0-1.0-4.0-3	Intended Use metadata shall have the capability to identify the content presentation designated by the Content Originator that must be used for the purpose of citation in court.	R1C; Must

RD-1007	14	**14 Requirements for Version Control**	
RD-1008	14.1	***14.1 Version Control Core Capabilities***	
RD-1013	14.1.0-5	The system shall allow authorized users to input, view, and manage version information.	R1C; Must
RD-1014	14.1.0-5.0-1	The system shall allow authorized users to input, view, and manage version information.	R1C; Must
RD-1015	14.1.0-5.0-1.0-1	The system shall allow authorized users to input version information.	R1C; Must
RD-1016	14.1.0-5.0-1.0-2	The system shall allow authorized users to view version information.	R1C; Must

RD-1017	14.1.0-5.0-1.0-3	The system shall allow authorized users to manage version information.	R1C; Must
RD-1018	14.1.0-5.0-2	The system shall allow authorized users to input, view, and manage version identifiers.	R1C; Must
RD-1019	14.1.0-5.0-2.0-1	The system shall allow authorized users to input version identifiers.	R1C; Must
RD-1020	14.1.0-5.0-2.0-2	The system shall allow authorized users to view version identifiers.	R1C; Must
RD-1021	14.1.0-5.0-2.0-3	The system shall allow authorized users to manage version identifiers.	R1C; Must
RD-1022	14.1.0-6	The system shall have the capability to alert authorized users when duplicate content is rejected.	R1C; Must
RD-1023	14.1.0-7	The system shall log all version history.	R2; Must
RD-1024	14.1.0-7.0-1	The version history log shall be incorporated into the package's metadata.	R2; Must

RD-1029	14.2	***14.2 Version Triggers***	
RD-1030	14.2.0-1	The system shall apply rules for version triggers.	R2; Must
RD-1031	14.2.0-1.0-1	The system shall apply rules for version triggers to groups of related content as defined in the GPO document Version Control in Relation to Government Documents.	R2; Must
RD-1032	14.2.0-1.0-2	Authorized users shall be able to modify rules for version triggers.	R2; Must
RD-1033	14.2.0-2	The system shall detect the following version triggers.	
RD-1034	14.2.0-2.0-1	Modifications to content	R2; Must
RD-1035	14.2.0-2.0-2	Changes to the "last updated" data provided within the document	R2; Must
RD-1036	14.2.0-2.0-3	Changes to a flat date provided within the document	R2; Must
RD-1037	14.2.0-2.0-4	Changes to a publication's title	R2; Must
RD-1038	14.2.0-2.0-5	Changes to a publication's edition statement and/or metadata	R2; Must
RD-1039	14.2.0-2.0-6	Changes in the issuing agency of a publication	R2; Must
RD-1040	14.2.0-2.0-7	Changes in file size or format	R2; Must
RD-1041	14.2.0-2.0-8	Changes in the publication's numbering scheme	R2; Must
RD-1042	14.2.0-2.0-9	Notification of the publisher (i.e., issuing agency)	R2; Must
RD-1043	14.2.0-3	The system shall provide the capability to notify users when version triggers have been activated.	R2; Must
RD-1045	14.2.0-5	The system shall provide the capability to notify designated authorized users when a version cannot be determined.	R2; Must

RD-1046	14.3	***14.3 Version Detection***	
RD-1047	14.3.0-1	The system shall determine if version identifiers are present in content packages.	R2; Must
RD-1048	14.3.0-1.0-1	Version identifiers shall be stored in metadata.	R1C; Must

RD-1049	14.4	***14.4 Version Metadata***	
RD-1050	14.4.0-1	The system shall express version information in metadata.	R1C; Must
RD-1051	14.4.0-1.0-1	The system shall update the metadata to indicate changes to attributes.	R1C; Must
RD-1052	14.4.0-2	The system shall record chain of custody information in metadata .	R1C; Must

RD-1053	14.5	***14.5 Version Relationships***	
RD-1054	14.5.0-1	The system shall determine and record relationships between versions.	R2; Must
RD-1056	14.5.0-1.0-1	The system shall make links to related documents permanently available.	R2; Must
RD-1057	14.5.0-1.0-2	The system shall be able to render relationship information so that it is human-readable.	R2; Must
RD-1055	14.5.0-2	The system shall establish links to related documents identified through version information in metadata.	R2; Must

RD-1058	14.6	***14.6 Version Notification***	
RD-1059	14.6.0-1	The system shall have the capability to notify users which version of content	R2; Must

		they are accessing.	
RD-1060	14.6.0-1.0-1	The system shall have the capability to notify users of the number of available versions of selected content.	R2; Must
RD-1061	14.6.0-1.0-2	The system shall have the capability to notify users that they are not viewing the latest available version of selected content.	R2; Must
RD-1062	14.6.0-1.0-3	The system shall have the capability to notify users of the relationship between the version of the content they are accessing and the latest version.	R2; Must
RD-1063	14.6.0-1.0-4	The system shall have the capability for users to view the difference in the content between versions.	R3; Must
RD-1064	14.6.0-1.0-5	The system shall have the capability to notify users that access to a version is restricted.	R2; Must
RD-1065	15	**15 Requirements for Workflow**	
RD-1066	15.1	***15.1 Workflow Core Capabilities***	
RD-1067	15.1.0-1	The system shall provide the capability to define workflows.	R1B; Must
RD-1068	15.1.0-1.0-1	The workflow definition shall be in the XML form conforming to a well established schema, such as XML Process Definition Language (XPDL) of Workflow Management Coalition (WfMC) or the Business Process Execution Language (BPEL) schema.	R1B; Must
RD-1069	15.1.0-1.0-2	The system shall provide the capability to validate workflow definitions against the established schema.	R1B; Must
RD-1070	15.1.0-2	The system shall provide the capability to create new versions of workflow definitions.	R1B; Must
RD-1071	15.1.0-3	The system shall provide the capability to test new versions of workflow definitions without interfering with any existing workflow instances.	R1B; Must
RD-1072	15.1.0-4	The system shall provide the capability to place new versions of workflow definitions into production.	R1B; Must
RD-1073	15.1.0-4.0-1	The system shall provide the capability to deploy newly developed or modified workflow definitions without interfering with existing workflow instances.	R1B; Must
RD-1074	15.1.0-5	The system shall provide the capability to revert to previous workflow definitions without interfering with existing workflow instances or other non-completed instances of workflows.	R1B; Must
RD-1075	15.1.0-5.0-1	The system shall provide the capability to revert to previous workflow definitions without interfering with existing workflow instances.	R1B; Must
RD-1076	15.1.0-5.0-2	The system shall provide the capability to revert to previous workflow definitions without interfering with other non-completed instances of workflows.	R1B; Must
RD-1077	15.1.0-6	The system shall provide the capability to manage business rules.	R1B; Must
RD-1078	15.1.0-6.0-1	The workflow-related business rules shall be configurable by the user to control the order in which the rules are applied.	R2; Must
RD-1079	15.1.0-7	The system shall provide the capability to manage manual activities.	R1B; Must
RD-1080	15.1.0-8	The system shall provide the capability to manage automated activities.	R2; Must
RD-1081	15.1.0-9	The system shall provide the capability to assign comments on jobs/activities.	R1B; Must
RD-1082	15.1.0-9.0-1	The system shall provide the capability to assign optional comments on jobs.	R1B; Must
RD-1083	15.1.0-9.0-2	The system shall provide the capability to assign optional comments on activities.	R1B; Must
RD-1084	15.1.0-9.0-3	The system shall provide the capability to assign optional comments on workflow instances.	R1B; Must
RD-1085	15.1.0-10	The system shall prevent the loss of workflow data.	R1B; Must
RD-1086	15.1.0-10.0-1	The system shall replicate workflow data to failover location(s).	R1C; Must
RD-1087	15.1.0-10.0-2	The system shall allow the frequency of backup processes to be controlled by the user.	R1C; Must
RD-1088	15.1.0-10.0-2.0-1	The system shall allow the backup processes to be controlled automatically or manually.	R2; Must
RD-1089	15.1.0-10.0-3	The system shall backup all necessary data required to retrieve workflow data to its original state in the event of a system failure.	R1C; Must
RD-1090	15.1.0-10.0-4	The system shall perform workflow backup processes without interruption to users.	R1C; Must
RD-1091	15.1.0-11	The system shall store information related to workflows in BPI.	R1B; Must

RD-1092	15.1.0-11.0-1	The system shall store information about workflows in BPI.	R1B; Must
RD-1093	15.1.0-11.0-2	The system shall store information about jobs in BPI.	R1B; Must
RD-1094	15.1.0-11.0-3	The system shall store information about activities in BPI.	R1B; Must

RD-1095	15.2	***15.2 Workflow – Control of Execution***	
RD-1096	15.2.0-1	The system shall provide the capability to control the execution of workflow instances.	R1B; Must
RD-1097	15.2.0-1.0-1	The system shall provide the capability to assign priorities to workflow instances.	R1B; Must
RD-1098	15.2.0-1.0-2	The system shall provide the capability to schedule for manual and automated activities.	R1B; Could / R1C; Must
RD-1099	15.2.0-1.0-2.0-1	The system shall provide the capability to assign deadlines for jobs/activities.	R1B; Could / R1C; Must
RD-1100	15.2.0-1.0-2.0-1.0-1	The system shall provide the capability to assign deadlines for jobs.	R1B; Could / R1C; Must
RD-1101	15.2.0-1.0-2.0-1.0-2	The system shall provide the capability to assign deadlines for activities.	R1B; Could / R1C; Must
RD-1102	15.2.0-1.0-2.0-2	The system shall provide the capability to assign estimated completion times for jobs/activities.	R1B; Could / R1C; Must
RD-1103	15.2.0-1.0-2.0-2.0-1	The system shall provide the capability to assign estimated completion times for jobs.	R1B; Could / R1C; Must
RD-1104	15.2.0-1.0-2.0-2.0-2	The system shall provide the capability to assign estimated completion times for activities.	R1B; Could / R1C; Must
RD-1105	15.2.0-1.0-3	The system shall provide the capability to assign human resources to manual activities.	R1C; Must
RD-1106	15.2.0-1.0-4	The system shall provide the capability to suspend activities/workflow instances.	R1B; Must
RD-1107	15.2.0-1.0-4.0-1	The system shall provide the capability to suspend activities.	R1B; Must
RD-1108	15.2.0-1.0-4.0-2	The system shall provide the capability to suspend workflow instances.	R1B; Must
RD-1109	15.2.0-1.0-5	The system shall provide the capability to resume activities/workflow instances.	R1B; Must
RD-1110	15.2.0-1.0-5.0-1	The system shall provide the capability to resume activities.	R1B; Must
RD-1111	15.2.0-1.0-5.0-2	The system shall provide the capability to resume workflow instances.	R1B; Must
RD-1112	15.2.0-1.0-6	The system shall provide the capability to cancel activities/workflow instances.	R1B; Must
RD-1113	15.2.0-1.0-6.0-1	The system shall provide the capability to cancel activities.	R1B; Must
RD-1114	15.2.0-1.0-6.0-2	The system shall provide the capability to cancel workflow instances.	R1B; Must
RD-1115	15.2.0-1.0-7	The system shall provide the capability to log activities.	R1B; Must
RD-1116	15.2.0-1.0-7.0-1	The system shall provide the capability to log activity start time.	R1B; Must
RD-1117	15.2.0-1.0-7.0-2	The system shall provide the capability to log activity end time.	R1B; Must
RD-1118	15.2.0-1.0-7.0-3	The system shall provide the capability to log the person(s) performing the activity.	R1B; Must
RD-1119	15.2.0-1.0-7.0-4	The system shall provide the capability to log the resources associated with an activity .	R1B; Must
RD-1120	15.2.0-1.0-8	The system shall provide the capability to manage lists of workflow instances.	R1B; Must
RD-1121	15.2.0-1.0-8.0-1	The system shall provide the capability for a user to view lists of workflow instances.	R1B; Must
RD-1122	15.2.0-1.0-8.0-2	The system shall provide the capability for a user to assign lists of workflow instances to other users.	R1B; Must
RD-1123	15.2.0-1.0-9	The system shall provide the capability to perform actions on a batch of workflow instances.	R2; Must
RD-1124	15.2.0-2	The system shall provide the capability to control the execution of jobs.	R1B; Must
RD-1125	15.2.0-2.0-1	The system shall provide the capability to assign priorities to jobs.	R1C; Must
RD-1126	15.2.0-2.0-1.0-1	The priority of a job shall be inherited by workflow instances associated with the job.	R1C; Must
RD-1127	15.2.0-2.0-2	The system shall provide the capability to suspend and resume jobs.	R1B; Must
RD-1128	15.2.0-2.0-2.0-1	The system shall provide the capability to suspend jobs.	R1B; Must
RD-1129	15.2.0-2.0-2.0-2	The system shall provide the capability to resume jobs.	R1B; Must
RD-1130	15.2.0-2.0-3	The system shall provide the capability to cancel a job.	R1B; Must
RD-1131	15.2.0-2.0-4	The system shall provide the capability to adjust the priority of a job at any time.	R2; Must
RD-1132	15.2.0-2.0-4.0-1	The system shall provide the capability to adjust the priority of a job manually or automatically.	R2; Must

RD-1133	15.2.0-2.0-5	The system shall provide the capability to log jobs.	R1B; Must
RD-1134	15.2.0-2.0-6	The system shall provide the capability to manage work lists of jobs.	R1B; Must
RD-1135	15.2.0-2.0-7	The system shall provide the capability to perform actions on a batch of jobs.	R2; Must

RD-1136	15.3	***15.3 Workflow – Monitoring***	
RD-1137	15.3.0-1	The system shall provide a monitoring tool for all workflow instances.	R1B; Must
RD-1138	15.3.0-1.0-1	The monitoring tool shall provide the capability to see how many instances of a workflow exist as well as the status of the workflow instances.	R1C; Must
RD-1139	15.3.0-1.0-1.0-1	The monitoring tool shall provide the capability to see how many instances of a workflow exist.	R1C; Must
RD-1140	15.3.0-1.0-1.0-2	The monitoring tool shall provide the capability to see the status of the workflow instances.	R1C; Must
RD-1141	15.3.0-1.0-2	The monitoring tool shall provide the capability for the user to customize views.	R1B; Could / R1C; Must
RD-1142	15.3.0-1.0-3	The monitoring tool shall provide the capability to save customized views for future use.	R1B; Could / R1C; Must
RD-1143	15.3.0-1.0-4	The monitoring tool shall provide the capability for users to monitor processing history of workflow instances.	R1B; Must
RD-1144	15.3.0-1.0-4.0-1	The monitoring tool shall provide the capability for users to monitor processing history over a specified time period.	R1B; Could / R1C; Must
RD-1145	15.3.0-1.0-5	The monitoring tool shall report throughput, delay, load, and additional performance measures in the future.	R2; Must
RD-1146	15.3.0-1.0-5.0-1	The monitoring tool shall report the throughput for workflow instances.	R1C; Must
RD-1147	15.3.0-1.0-5.0-2	The monitoring tool shall report any delays for workflow instances.	R1C; Must
RD-1148	15.3.0-1.0-5.0-3	The monitoring tool shall report the loads for workflow instances.	R1C; Must
RD-1149	15.3.0-1.0-5.0-4	The monitoring tool shall report additional performance measures in the future.	R2; Must
RD-1150	15.3.0-2	The system shall provide the capability for users to monitor jobs or a list of jobs.	R1B; Must
RD-1151	15.3.0-2.0-1	The system shall provide the capability for users to monitor jobs.	R1B; Must
RD-1152	15.3.0-2.0-2	The system shall provide the capability for users to monitor a list of jobs.	R1B; Must
RD-1153	15.3.0-2.0-3	The system shall provide the capability for users to monitor a batch of jobs.	R1B; Must
RD-1154	15.3.0-2.0-4	The system shall provide the capability to monitor planned, scheduled and actual times for selected jobs.	R2; Must
RD-1155	15.3.0-2.0-4.0-1	The system shall provide the capability to monitor planned times for selected jobs.	R2; Must
RD-1156	15.3.0-2.0-4.0-2	The system shall provide the capability to monitor scheduled times for selected jobs.	R2; Must
RD-1157	15.3.0-2.0-4.0-3	The system shall provide the capability to monitor actual times for selected jobs.	R2; Must
RD-1158	15.3.0-2.0-5	The system shall provide the capability to group jobs with a defined status.	R1B; Must
RD-1159	15.3.0-3	The system shall provide the capability for users to monitor workflow instances or a list of workflow instances.	R1B; Must
RD-1160	15.3.0-3.0-1	The system shall provide the capability for users to monitor workflow instances.	R1B; Must
RD-1161	15.3.0-3.0-2	The system shall provide the capability for users to monitor workflow instances or a list of workflow instances.	R1B; Must
RD-1162	15.3.0-3.0-3	The system shall provide the capability for users to monitor a batch of workflow instances.	R1B; Must
RD-1163	15.3.0-3.0-4	The system shall provide the capability to monitor planned, scheduled and actual times for selected workflow instances.	R2; Must
RD-1164	15.3.0-3.0-4.0-1	The system shall provide the capability to monitor planned times for selected workflow instances.	R2; Must
RD-1165	15.3.0-3.0-4.0-2	The system shall provide the capability to monitor scheduled times for selected workflow instances.	R2; Must
RD-1166	15.3.0-3.0-5	The system shall provide the capability to monitor actual times for selected workflow instances.	R2; Must
RD-1167	15.3.0-4	The system shall provide the capability to group workflow instances with a defined status.	R2; Must

RD-1168	15.4	***15.4 Workflow – Resource Requirements***	
RD-1169	15.4.0-1	The system shall provide the capability to estimate resource requirements associated with internal workflow.	R1B; Could / R1C; Must
RD-1170	15.4.0-2	The system shall provide the capability to estimate resource requirements associated with external workflow.	R1C; Could / R2; Must
RD-1171	15.4.0-3	The system shall provide the capability to estimate resource requirements for automated and manual activities.	R1C; Could / R2; Must
RD-1172	15.4.0-3.0-1	The system shall provide the capability to estimate resource requirements for automated activities.	R1C; Could / R2; Must
RD-1173	15.4.0-3.0-2	The system shall provide the capability to estimate resource requirements for manual activities.	R1C; Could / R2; Must

RD-1174	15.5	***15.5 Workflow – Notification***	
RD-1175	15.5.0-1	The system shall provide the capability to associate notifications with workflows.	R1B; Must
RD-1176	15.5.0-2	The system shall provide the capability to manage notifications attached to workflows.	R1B; Must
RD-1177	15.5.0-3	The system shall send notifications via e-mail, the user's screen, and additional methods in the future.	R2; Must
RD-1178	15.5.0-3.0-1	The system shall send notifications via e-mail.	R1B; Must
RD-1179	15.5.0-3.0-2	The system shall send notifications via the user's screen.	R1B; Must
RD-1180	15.5.0-3.0-3	The system shall send notifications via additional methods in the future.	R2; Must
RD-1181	15.5.0-4	The system shall provide the capability to configure the list of recipients of notifications.	R1B; Must
RD-1182	15.5.0-5	The system shall provide the capability to escalate notifications.	R3; Should

RD-1183	15.6	***15.6 Workflow – Security***	
RD-1184	15.6.0-1	The system shall provide the capability to have security controls on workflow activities.	R1B; Must
RD-1185	15.6.0-1.0-1	The security control (allow or deny actions) shall be rule based.	R2; Must
RD-1186	15.6.0-1.0-2	Manual activities in the workflows shall be assigned with one or more security rules.	R2; Must

RD-1187	15.7	***15.7 Workflow – Interface***	
RD-1188	15.7.0-1	The system shall provide a Graphical User Interface (GUI) edit tool to manage workflow definitions and executions.	R1B; Must
RD-1189	15.7.0-2	The Monitoring Tool shall contain a GUI for all workflow monitoring capabilities.	R1B; Must

RD-1190	16	**16 Requirements for Storage Management**	
RD-1191	16.1	***16.1 Storage Core Capabilities***	
RD-1192	16.1.0-1	The system shall support retrieval of data from online storage at error rates of (TBR-1192a).	R1B; Must
RD-1193	16.1.0-2	The system shall be capable of providing a secure repository environment for all storage.	R1C; Must
RD-1194	16.1.0-2.0-1	Near-line storage media shall preserve data integrity and quality for no less than 10 years in a data center environment.	R1C; Must
RD-1195	16.1.0-2.0-2	Each data center in the system shall be housed in a facility protected by	R1C; Must

		physical security measures.	
RD-1196	16.1.0-2.0-3	Each data center in the system shall be protected from power failures for the time required to safely power down all system components.	R1C; Must
RD-1197	16.1.0-2.0-4	Each data center in the system shall be equipped with power failure sensors capable of notifying users when grid power has failed.	R1C; Must
RD-1198	16.1.0-2.0-5	Each data center in the system shall be equipped with HVAC capacity equal to 50% greater than the sum of the BTUs produced by all system equipment located in that data center.	R1C; Must
RD-1199	16.1.0-2.0-6	Each data center in the system shall be equipped with environment sensors capable of notifying users when out of tolerance conditions are imminent.	R1C; Must
RD-1200	16.1.0-3	The system shall support the capability to include multiple storage classes.	R1C; Must
RD-1201	16.1.0-3.0-1	The system shall support the capability to add additional storage classes in the future without a major redesign.	R1C; Must
RD-1202	16.1.0-3.0-2	The system shall support the capability to transparently migrate data from one storage class to another based on system policies.	R1C; Must
RD-1203	16.1.0-3.0-3	The system shall support the capability for authorized users to configure the policies used by the system to migrate data from one class of storage to another.	R1C; Must
RD-1204	16.1.0-3.0-4	The system shall support the capability for authorized users to set storage policies for selected content packages.	R1C; Must
RD-1205	16.2	***16.2 Content Delivery Network Storage***	
RD-1206	16.2.0-1	The system shall have the capability to store data dynamically in external Content Delivery Networks (CDN) based on hit rate/criticality of content.	R2; Must
RD-1207	16.2.0-2	The system shall support the capability for authorized users to designate data for storage in a Content Delivery Network.	R1C; Must
RD-1210	16.2.0-5	The system shall have the capability to utilize external storage Service Providers.	R1C; Must
RD-1220	16.3	***16.3 Networked Moderate Performance Storage***	
RD-1226	16.4	***16.4 Low Criticality- Low Cost Storage***	
RD-1232	16.5	***16.5 Failover Storage***	
RD-1233	16.5.0-1	Failover Storage shall provide the fault tolerance required to allow the system to survive a localized disaster.	R1C; Must
RD-1234	16.5.0-2	Failover Storage shall be able to reconstitute and switch-over to alternate systems at a remote site in the event of local catastrophic damage.	R1C; Must
RD-1235	16.5.0-2.0-1	The system shall replicate all system data to a disaster recovery site.	R1C; Must
RD-1236	16.5.0-2.0-2	Failover Storage shall allow the switchover to redundant components via either user action or automatic in case of failure.	R1C; Must
RD-1237	16.5.0-2.0-2.0-1	Failover Storage shall allow the switchover to redundant components via user action.	R1C; Must
RD-1238	16.5.0-2.0-2.0-2	Failover Storage shall allow the switchover to redundant components automatically in case of failure.	R1C; Must
RD-1239	16.5.0-2.0-3	The system shall replicate all content packages to a disaster recovery site.	R1C; Must
RD-1240	16.5.0-2.0-4	The system shall replicate all BPI to a disaster recovery site.	R1C; Must
RD-1241	16.5.0-2.0-5	The system shall provide the capability to switchover operations from the primary to the backup site in the event of a disaster.	R1C; Must
RD-1243	16.5.0-4	Failover Storage 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).	R1C; Must

RD-1244	16.6	***16.6 Backup Retrieval Media Storage***	
RD-1245	16.6.0-1	Back-up Retrieval Media Storage shall be able to accomplish periodic backup on mass removable storage media.	R1B; Must
RD-1246	16.6.0-1.0-1	Back-up Retrieval Media Storage shall allow users to manage periodic backup schedules.	R1B; Must
RD-1247	16.6.0-1.0-2	Back-up Retrieval Media Storage shall allow backups on multiple types of mass removable storage media.	R1C; Must
RD-1248	16.6.0-2	Back-up Retrieval Media Storage shall be able to accomplish a full back-up of all critical data in less than six hours or scheduled periodically over 24 hours.	R1B; Must
RD-1249	16.6.0-2.0-1	Back-up Retrieval Media Storage shall allow users to manage which data is listed as critical.	R1C; Must
RD-1250	16.6.0-2.0-2	Back-up Retrieval Media Storage shall allow users to manage the backup schedule.	R1B; Must
RD-1251	16.6.0-2.0-3	Back-up Retrieval Media Storage shall not interfere with current system processes.	R1B; Must
RD-1253	16.6.0-4	Back-up Retrieval Media Storage shall support mirroring the write data in cache as a method of data protection.	R1C; Must
RD-1254	16.6.0-4.0-1	Back-up Retrieval Media Storage shall allow users to manage which data should be backed up.	R1C; Must
RD-1255	16.6.0-5	Back-up Retrieval Media Storage shall support 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.	R3; Must
RD-1256	16.6.0-5.0-1	Back-up Retrieval Media Storage shall allow users the ability to both schedule and manually test data for errors even when the cache or disk is inactive.	R3; Must
RD-1257	16.6.0-6	Back-up Retrieval Media Storage shall support the process of copying data to a second disk array, often housed in a separate location from the originating disk array.	R1C; Must

RD-1258	16.7	***16.7 Mid-term Archival Storage***	

RD-1261	16.8	***16.8 Long-term Permanent Archival Storage***	
RD-1262	16.8.0-1	Long-term Permanent Archival Storage shall have off-line storage and indexing capability for multiple Petabytes of data.	R1C; Must
RD-1263	16.8.0-1.0-1	Long-term Permanent Archival Storage shall have off-line storage capacity for multiple Petabytes of data.	R1C; Must
RD-1264	16.8.0-1.0-2	Long-term Permanent Archival Storage shall have indexing capability for multiple Petabytes of data.	R1C; Must
RD-1265	16.8.0-2	Long-term Permanent Archival Storage shall have a remote storage site over 600 miles from the main GPO facility.	R1C; Must
RD-1266	16.8.0-3	Long-term Permanent Archival Storage site shall preserve physical data integrity and quality for no less than 100 Years under controlled storage conditions (e.g., 70º F, 60% Humidity).	R3; Must

RD-1267	16.9	***16.9 Functional Data Storage***	
RD-1268	16.9.0-1	Work In Progress (WIP) Storage	R1C; Must
RD-1269	16.9.0-1.0-1	The average access time for WIPs shall be 2 seconds or less.	R1C; Must
RD-1270	16.9.0-1.0-2	WIPs shall be protected from unauthorized alteration by user actions.	R1C; Must
RD-1275	16.9.0-1.0-7	WIP Storage shall contain both content and metadata.	R1C; Must
RD-1276	16.9.0-2	Archival Information Package (AIP) Storage	R1C; Must
RD-1277	16.9.0-2.0-1	The system shall write all AIPs to archival media for off site storage.	R1C; Must
RD-1278	16.9.0-2.0-2	The average access time for SIPs after submission to the system shall be 2 seconds or less.	R1C; Must
RD-1279	16.9.0-2.0-3	The average access time for AIPs stored in on line storage shall be 2 seconds	R1C; Must

		or less.	
RD-1281	16.9.0-2.0-5	SIPs shall be protected from unauthorized alteration by user actions.	R1C; Must
RD-1282	16.9.0-2.0-6	AIPs shall be protected from unauthorized alteration by user actions.	R1C; Must
RD-1287	16.9.0-2.0-11	AIP Storage shall exist in isolation of other system stores.	R1C; Must
RD-1288	16.9.0-2.0-12	The system shall support the capability to migrate AIP content to future storage technologies.	R1C; Must
RD-1289	16.9.0-2.0-13	AIP Storage shall contain both content and metadata.	R1C; Must
RD-1290	16.9.0-3	Access Content Storage (ACS)	R1C; Must
RD-1291	16.9.0-3.0-1	The average access time for ACPs shall be 2 seconds or less.	R1C; Must
RD-1292	16.9.0-3.0-2	ACPs shall be protected from unauthorized alteration by user actions.	R1C; Must
RD-1300	16.9.0-3.0-10	ACS shall contain both content and metadata.	R1C; Must
RD-1301	16.9.0-4	Business Process information (BPI) Storage.	R1C; Must
RD-1302	16.9.0-4.0-1	The average access time for BPI shall be 2 seconds or less.	R1C; Must
RD-1303	16.9.0-4.0-2	BPI shall be protected from unauthorized alteration by user actions.	R1C; Must
RD-1309	16.9.0-4.0-8	BPS shall contain Failover Storage.	R1C; Must

RD-1311	16.10	***16.10 Storage System Standards***	
RD-1312	16.10.0-1	The system shall integrate with Unix and Windows based Directory Services (Lightweight Directory Access Protocol, Active Directory), and role based access.	R1B; Must
RD-1313	16.10.0-1.0-1	The system shall integrate with Lightweight Directory Access Protocol (LDAP).	R1B; Must
RD-1314	16.10.0-1.0-2	The system shall control access to data in storage based on the user's role.	R1C; Must
RD-1315	16.10.0-1.0-3	The system shall prefer the use of Lightweight Directory Access Protocol over Active Directory wherever possible.	R1C; Must
RD-1316	16.10.0-2	The system shall be able to ingest files stored on disk systems connected directly to the system.	R2; Must
RD-1317	16.10.0-2.0-1	The system shall provide the capability to read files stored in common operating system formats.	R2; Must
RD-1318	16.10.0-2.0-1.0-1	The system shall be able to ingest files stored in a FAT filesystem.	R2; Must
RD-1319	16.10.0-2.0-1.0-2	The system shall be able to ingest files stored in a FAT32 filesystem.	R2; Must
RD-1320	16.10.0-2.0-1.0-3	The system shall be able to ingest files stored in a VFAT filesystem.	R2; Must
RD-1321	16.10.0-2.0-1.0-4	The system shall be able to ingest files stored in a NTFS filesystem.	R2; Must
RD-1322	16.10.0-2.0-1.0-5	The system shall be able to ingest files stored in a HPFS filesystem.	R2; Must
RD-1323	16.10.0-2.0-1.0-6	The system shall be able to ingest files stored in a EXT2 filesystem.	R2; Must
RD-1324	16.10.0-2.0-1.0-7	The system shall be able to ingest files stored in a EXT3 filesystem.	R2; Must
RD-1325	16.10.0-2.0-1.0-8	The system shall be able to ingest files stored in a EXT4 filesystem.	R2; Must
RD-1326	16.10.0-2.0-1.0-9	The system shall be able to ingest files stored in a HFS Plus filesystem.	R2; Must
RD-1327	16.10.0-2.0-1.0-10	The system shall be able to ingest files stored in a JFS2 filesystem.	R2; Must
RD-1328	16.10.0-2.0-1.0-11	The system shall be able to ingest files stored in a UFS filesystem.	R2; Must
RD-1329	16.10.0-3	The system shall utilize common Redundant Array of Independent Disks (RAID) Disk Data Format (DDF) architecture.	R1C; Must
RD-1330	16.10.0-4	The system shall conform to commonly used, industry standard protocols.	R2; Must
RD-1331	16.10.0-4.0-1	The system shall support the capability to interface with industry standard protocols.	R2; Must
RD-1332	16.10.0-4.0-2	The system shall use industry standard protocols when there is one that meets the system requirements.	R2; Must
RD-1333	16.10.0-4.0-3	The system shall use of non-standard protocols only when there is no industry standard that meets the system requirements.	R2; Must
RD-1334	16.10.0-5	The system shall allow interaction with management information bases (MIB) via SNMP, and shall conform to or interoperate within Object-based Storage Device (OSD) specification.	R1C; Must
RD-1335	16.10.0-5.0-1	The system shall allow interaction with management information bases (MIB) via SNMP.	R1C; Must
RD-1336	16.10.0-5.0-2	The system shall conform to or interoperate within Object-based Storage Device (OSD) specification.	R1C; Must
RD-1337	16.10.0-6	The system storage shall support ANSI INCITS 388-2004 Storage Management Initiative Specification.	R2; Must
RD-1338	16.10.0-7	The system back-up tapes shall conform to Linear Tape-Open (LTO) standard.	R1C; Must

RD-1339	16.11	***16.11 Storage – Monitoring***	
RD-1340	16.11.0-1	The system shall provide the capability to monitor the health of system components in real time.	R1C; Must
RD-1341	16.11.0-1.0-1	The system shall monitor the health of the network components in real-time.	R1C; Must
RD-1342	16.11.0-1.0-2	The system shall monitor the health of the system applications in real-time.	R1C; Must
RD-1343	16.11.0-1.0-3	The system shall monitor the health of the storage components in real-time.	R1C; Must
RD-1344	16.11.0-1.0-4	The system monitor the health of the processing components in real-time.	R1C; Must
RD-1345	16.11.0-1.0-5	The system shall monitor the health of the operating system in real-time.	R1C; Must
RD-1346	16.11.0-2	The system shall provide the capability for the user to configure the upper and lower bounds for system parameters being monitored.	R1C; Must
RD-1347	16.11.0-3	The system shall have the ability to send alerts to users via multiple channels should a performance problem, failure condition or impending failure be detected.	R1C; Must
RD-1348	16.11.0-3.0-1	The system shall send a notification to users when a performance problem is detected.	R1C; Must
RD-1349	16.11.0-3.0-2	The system shall send a notification to users when a failure condition is detected.	R1C; Must
RD-1350	16.11.0-3.0-3	The system shall send a notification to users when a failure is impending.	R1C; Must
RD-1351	16.11.0-3.0-4	The system shall send notifications to appropriate user screen, e-mail, and via additional methods in the future.	R2; Must
RD-1352	16.11.0-3.0-4.0-1	The system shall send notifications to the appropriate user screen.	R1C; Must
RD-1353	16.11.0-3.0-4.0-2	The system shall send notifications to the appropriate e-mail.	R1C; Must
RD-1354	16.11.0-3.0-4.0-3	The system shall send notifications via additional methods in the future.	R2; Must
RD-1355	16.11.0-3.0-5	The system shall allow the users to configure the problem severity level that triggers a user notification.	R1C; Must
RD-1356	16.11.0-4	The system shall have the capability to monitor real-time performance of the system in terms of service levels.	R1C; Must
RD-1357	16.11.0-5	The system shall provide storage usage metrics that allow projection of future storage needs.	R3; Must
RD-1358	16.11.0-6	The system shall monitor a Service Level Agreement for an externally hosted data store.	R1C; Must
RD-1359	16.11.0-7	The system shall allow users to reconfigure RAID levels without vendor assistance.	R2; Must

RD-1360	16.12	***16.12 Storage – Preventive Action***	
RD-1361	16.12.0-1	The system shall automatically allocate stand-by drives to replace drives that have failed.	R1C; Must
RD-1362	16.12.0-2	The system shall have the ability to allow hot swapping of components should a failure condition be detected.	R1C; Must
RD-1363	16.12.0-2.0-1	The system shall provide the capability to hot swap power supplies when a power supply has failed.	R1C; Must
RD-1364	16.12.0-2.0-2	The system shall provide the capability to hot swap cooling fans when a cooling fan has failed.	R1C; Must
RD-1365	16.12.0-2.0-3	The system shall provide the capability to hot swap disk drives in disk storage systems when a disk drive has failed.	R1C; Must
RD-1366	16.12.0-2.0-4	The system shall provide the capability to hot swap blade servers when a blade server has failed.	R1C; Must
RD-1367	16.12.0-3	The system shall have the ability to dynamically move data to improve system performance.	R1C; Must
RD-1368	16.12.0-4	The storage systems shall provide the capability to upgrade controller microcode without shutting down the storage system.	R2; Must

RD-1369	16.13	***16.13 Storage – Data Integrity***	
RD-1370	16.13.0-1	The system shall allow for securing of partitions.	R1C; Must
RD-1371	16.13.0-2	The system shall allow encryption of logical content.	R1C; Must

RD-1373	16.14	***16.14 Storage – Allocation***	
RD-1374	16.14.0-1	The system shall support the management of heterogeneous storage architectures (e.g. direct attached storage (DAS), network attached storage (NAS), storage area network (SAN)).	R1C; Must
RD-1375	16.14.0-2	The system shall provide the capability to automatically allocate additional storage when a user configurable threshold is crossed.	R1C; Must
RD-1376	16.14.0-3	The system shall be able to manage any infrastructure storage device attached to the system.	R1C; Must
RD-1377	16.14.0-4	The system shall allow both manual and automated compression of data at various compression levels for infrequently accessed data.	R1C; Must
RD-1378	16.14.0-5	The system shall provide the capability to allocate storage on new devices after they have been identified by the system and formatted for use.	R1C; Must

RD-1379	17	**17 Requirements for Security**	
RD-1380	17.1	***17.1 Security – System User Authentication***	
RD-1381	17.1.0-1	The system shall have the capability to authenticate users based on a unique user identity.	R1B; Must
RD-1382	17.1.0-1.0-1	The system shall authenticate system and security administrators.	R1B; Must
RD-1383	17.1.0-1.0-2	The system shall authenticate system administrators.	R1B; Must
RD-1384	17.1.0-1.0-3	The system shall authenticate security administrators.	R1B; Must
RD-1385	17.1.0-1.0-4	The system shall support user ID and password authentication.	R1B; Must
RD-1386	17.1.0-1.0-5	The system shall support a configurable minimum password length parameter, settable by authorized system administrators. The minimum value allowable for this parameter is eight (8).	R1C; Must
RD-1387	17.1.0-1.0-6	The system shall permit stronger authentication techniques to be used for system and security administrators (such as longer and/or more complex passwords, public key certificate, and token based authentication).	R1C; Must
RD-1388	17.1.0-2	The system shall permit users to create a unique user identity for access to the system.	R1B; Must
RD-1389	17.1.0-2.0-1	The system shall enforce uniqueness of user identity so that no two users can use the exact same identity.	R1B; Must
RD-1390	17.1.0-2.0-2	The system shall be capable of Identity Management system functionality to facilitate provisioning of user identities for users and system administrators.	R1B; Must
RD-1391	17.1.0-2.0-2.0-1	The system shall be capable of Identity Management system functionality to provide users and system administrators with one single interface and control point for provisioning and managing user identities.	R2; Must
RD-1392	17.1.0-2.0-2.0-1.0-1	The system shall be capable of Identity Management system functionality to provide users and system administrators with one single interface and control point for provisioning and managing user identities that will be used to support the system's access control decisions.	R2; Must
RD-1393	17.1.0-2.0-2.0-1.0-2	The system shall deploy an initial Identity Management capability to provide users and system administrators with one single interface and control point for provisioning and managing user identities.	R1C; Must
RD-1394	17.1.0-2.0-3	A user shall only be allowed to manage attributes associated with their own user identity.	R1C; Must
RD-1395	17.1.0-3	The system shall display a message to users if they fail to authenticate.	R1B; Must
RD-1396	17.1.0-4	The system shall permit access to a default workbench for public End Users, which does not require them to login.	R1B; Must
RD-1398	17.1.0-6	The system shall comply with GPO and Federal authentication policies.	R1C; Must
RD-1399	17.1.0-6.0-1	The system shall comply with GPO authentication policies specified in P825.33.	R1C; Must
RD-1400	17.1.0-6.0-2	The system shall comply with Federal authentication policies.	R1C; Must
RD-1401	17.1.0-7	The system shall have the capability to support up to 2048-bit RSA public/private key generation (asymmetric algorithm).	R1C; Must
RD-770	17.1.0-8	The system shall provide the capability to use passwords to verify the identity of authorized users.	R1B; Must

RD-771	17.1.0-9	The system shall provide the capability to use PKI certificates to verify the identity of authorized users.	R1C; Must
RD-772	17.1.0-10	The system shall provide the capability to verify the authorization level of authorized users to perform requested functions.	R1B; Must
RD-773	17.1.0-11	The system shall provide the capability to validate credentials (e.g. digital certificate) of authorized users.	R1C; Must

RD-1402	17.2	***17.2 Security – User Access Control***	
RD-1403	17.2.0-1	The system shall have the capability to arbitrate access based on a role-based access model driven by policy.	R1C; Must
RD-1404	17.2.0-1.0-1	The system shall permit authorized system administrators to create and assign customized roles.	R1C; Must
RD-1405	17.2.0-1.0-1.0-1	The system shall permit authorized system administrators to create customized roles.	R1C; Must
RD-1406	17.2.0-1.0-1.0-2	The system shall permit authorized system administrators to assign customized roles.	R1C; Must
RD-1407	17.2.0-1.0-1.0-3	The system shall provide access control limitations to support data mining .	R2; Must
RD-1408	17.2.0-1.0-2	The system shall allow authorized system administrators to assign and customize roles for access to system data objects and transactions.	R1C; Must
RD-1409	17.2.0-1.0-2.0-1	The system shall allow authorized system administrators to assign roles for access to system data objects and transactions.	R1C; Must
RD-1410	17.2.0-1.0-2.0-2	The system shall allow authorized system administrators to customize roles for access to system data objects and transactions.	R1C; Must
RD-1411	17.2.0-1.0-3	The system shall allow the use of standards based LDAP technology for the role based access model.	R1B; Must
RD-1412	17.2.0-2	The system shall manage user accounts.	R1B; Must
RD-1413	17.2.0-3	The system shall provide the capability to create user accounts.	R1B; Must
RD-1414	17.2.0-3.0-1	The system shall provide the capability to create group accounts. This will allow individual users to log into the system but provide access to an entire group of users.	R1B; Must
RD-1415	17.2.0-4	The system shall provide the capability to access user accounts.	R1B; Must
RD-1416	17.2.0-5	The system shall provide the capability to delete user accounts.	R1B; Must
RD-1417	17.2.0-6	The system shall provide the capability to suspend user accounts.	R1C; Must
RD-1418	17.2.0-7	The system shall provide the capability to reactivate suspended user accounts.	R1C; Must
RD-1419	17.2.0-8	The system shall provide the capability for the renewal of user registrations.	R1C; Must
RD-1420	17.2.0-9	The system shall have the capability to expire user accounts.	R1C; Must
RD-1421	17.2.0-10	The system shall provide the capability for users to cancel their accounts.	R1C; Must
RD-1422	17.2.0-11	The system shall provide the capability for users to update their account information.	R1C; Must
RD-1423	17.2.0-12	The system shall provide a means to ensure that users cannot view or modify information of other users unless authorized.	R1B; Must
RD-1424	17.2.0-12.0-1	The system shall provide a means to ensure that users cannot view information of other users unless authorized.	R1B; Must
RD-1425	17.2.0-12.0-2	The system shall provide a means to ensure that users cannot modify information of other users unless authorized.	R1B; Must
RD-1426	17.2.0-13	The system shall securely store personal information (e.g. user names and passwords).	R1B; Must
RD-1427	17.2.0-14	The system shall provide the capability for authorized users to manage (add, modify, delete) information.	R1B; Must
RD-1428	17.2.0-15	The system shall have the capability to provide secure interfaces for FDsys operations.	R1C; Must

RD-1429	17.3	***17.3 Security – Capture and Analysis of Audit Logs***	
RD-1430	17.3.0-1	The system shall keep an audit log of all transactions in the system.	R1C; Must
RD-1431	17.3.0-1.0-1	The system shall create audit logs which contain sufficient information to establish what events occurred, the source(s) of the events, and the outcomes of the events.	R1C; Must

RD-1432	17.3.0-1.0-1.0-1	Audit logs shall contain logged events which each contain the date the event occurred.	R1C; Must
RD-1433	17.3.0-1.0-1.0-2	Audit logs shall contain logged events which each contain the time the event occurred.	R1C; Must
RD-1434	17.3.0-1.0-1.0-3	Audit logs shall contain logged events which each contain the software module (source) that logged the event, which can be either an application name or a component of the system or of a large application, such as a service name.	R1C; Must
RD-1435	17.3.0-1.0-1.0-4	Audit logs shall contain logged events which each contain a classification of the event by the event source.	R1C; Must
RD-1436	17.3.0-1.0-1.0-5	Audit logs shall contain logged events which each contain a classification of the event severity: Error, Information, or Warning in the system and application logs; Success Audit or Failure Audit in the security log.	R1C; Must
RD-1437	17.3.0-1.0-1.0-6	Audit logs shall contain logged events which each contain a number identifying the particular event type.	R1C; Must
RD-1438	17.3.0-1.0-2	Audit logs shall contain a description of the event.	R1C; Must
RD-1439	17.3.0-1.0-2.0-1	Audit logs shall contain a description of the event containing the user name of the user on whose behalf the event occurred.	R1C; Must
RD-1440	17.3.0-1.0-2.0-2	Audit logs shall contain a description of the event containing the name (IP address and DNS name) of the system on which the event occurred.	R1C; Must
RD-1441	17.3.0-1.0-2.0-3	Audit logs shall contain a description of the event containing a description of any significant problems, such as a loss of data or loss of functions.	R1C; Must
RD-1442	17.3.0-1.0-2.0-4	Audit logs shall contain a description of the event containing information about infrequent significant events that describe successful operations of major server services.	R1C; Must
RD-1443	17.3.0-1.0-2.0-5	Audit logs shall contain a description of the event containing warnings, events that are not necessarily significant, but that indicate possible future problems.	R1C; Must
RD-1444	17.3.0-1.0-2.0-6	Audit logs shall contain a description of the event containing an audit of the security access attempts that were successful.	R1C; Must
RD-1445	17.3.0-1.0-2.0-7	Audit logs shall contain a description of the event containing an audit of the security access attempts that failed.	R1C; Must
RD-1446	17.3.0-1.0-3	Audit logs shall contain additional data fields where binary data can be displayed in bytes or words.	R2; Must
RD-1447	17.3.0-1.0-4	The system shall maintain a system log containing events logged by the system components.	R1B; Must
RD-1448	17.3.0-1.0-4.0-1	The system shall allow system logs to be viewed by all authorized users.	R1B; Must
RD-1449	17.3.0-1.0-5	The system shall maintain a security log containing valid and invalid logon attempts as well as events related to resource use, such as creating, opening, or deleting files or other objects.	R1C; Must
RD-1450	17.3.0-1.0-5.0-1	The system shall allow security logs to be viewed by all authorized users.	R1C; Must
RD-1451	17.3.0-1.0-5.0-2	The system shall maintain a security log containing logon attempts (both valid and invalid).	R1C; Must
RD-1452	17.3.0-1.0-5.0-3	The system shall maintain a security log containing events related to resource use, such as creating, opening, or deleting files or other objects.	R1C; Must
RD-1453	17.3.0-1.0-6	The system shall maintain an application log containing events logged by applications.	R1C; Must
RD-1454	17.3.0-1.0-6.0-1	The system shall allow applications logs to be viewed by all authorized users.	R1C; Must
RD-1455	17.3.0-1.0-7	The system shall have an Audit Log manager for system administrator functions.	R1C; Must
RD-1456	17.3.0-1.0-7.0-1	The Audit Log manager shall be searchable.	R1C; Must
RD-1457	17.3.0-1.0-8	The system shall provide the capability to log completed transaction information.	R1C; Must
RD-1458	17.3.0-1.0-8.0-1	The system shall provide the capability to view completed transaction.	R1C; Must
RD-1459	17.3.0-1.0-9	The system shall keep an audit log of user ordering (request) transactions.	R1C; Must
RD-1460	17.3.0-1.0-10	The system shall keep an audit log of system administration transactions.	R1C; Must
RD-1461	17.3.0-1.0-11	The system shall keep an audit log of security administrator transactions.	R1C; Must
RD-1462	17.3.0-1.0-12	The system shall keep an audit log of system access rights.	R1C; Must
RD-1463	17.3.0-1.0-13	The system shall keep an audit log of preservation processes.	R1C; Must
RD-1464	17.3.0-1.0-13.0-1	The system shall keep an audit log of deposited content activities.	R1C; Must
RD-1465	17.3.0-1.0-13.0-2	The system shall keep an audit log of harvested content activities.	R1C; Must
RD-1466	17.3.0-1.0-13.0-3	The system shall keep an audit log of converted content activities.	R1C; Must
RD-1467	17.3.0-1.0-14	The system shall keep an audit log of Content Originator ordering activities.	R1C; Must
RD-1468	17.3.0-1.0-15	The system shall keep an audit log of content authentication activities.	R1C; Must
RD-1469	17.3.0-1.0-16	The system shall keep an audit log of version control activities.	R1C; Must

RD-1470	17.3.0-1.0-17	The system shall keep an audit log of cataloging activities.	R1C; Must
RD-1471	17.3.0-1.0-18	The system shall keep an audit log of support activities (e.g., support status).	R1C; Must
RD-1472	17.3.0-1.0-19	The system shall keep an audit log for data mining.	R2; Must
RD-1473	17.3.0-2	The system shall have the capability to maintain integrity of audit logs.	R1C; Must
RD-1474	17.3.0-2.0-1	The system shall protect the audit log from unauthorized user modification.	R1C; Must
RD-1475	17.3.0-2.0-2	The system shall detect user attempts to edit audit logs.	R1C; Must
RD-1476	17.3.0-3	The system shall keep an audit log of attempts to access the system.	R1C; Must
RD-1477	17.3.0-3.0-1	The system shall keep an audit log of any detected breaches of security policy.	R1C; Must
RD-1478	17.3.0-4	The system shall keep and store audit logs (e.g. audit trails) and utilize records management processes on these stores.	R1C; Must
RD-1479	17.3.0-4.0-1	The system shall keep audit logs (e.g. audit trails) per GPO P825.33.	R1C; Must
RD-1480	17.3.0-4.0-2	The system shall store audit logs (e.g. audit trails) per GPO P825.33.	R1C; Must
RD-1481	17.3.0-4.0-3	The system shall utilize records management processes on audit log stores.	R1C; Must
RD-1482	17.3.0-4.0-4	The system shall save audit logs as specified in GPO Publication 825.33.	R1C; Must

RD-1483	17.4	***17.4 Security – User Privacy***	
RD-1484	17.4.0-1	The system shall support the capability of maintaining user privacy in accordance with GPO's privacy policy and Federal privacy laws and regulations.	R1C; Must
RD-1485	17.4.0-1.0-1	The system shall conform to guidelines set forth in GPO Publication 825.33.	R1C; Must
RD-1486	17.4.0-1.0-2	The system shall support compliance outlined in Title 5 USC Sec. 552a (Records maintained on individuals).	R1C; Must
RD-1487	17.4.0-1.0-3	The system shall support the capability of maintaining access privacy (e.g., Search, Request).	R1C; Must
RD-1488	17.4.0-1.0-4	The system shall support the capability of maintaining support privacy (e.g., user identity).	R1C; Must
RD-1489	17.4.0-1.0-5	The system shall support the capability of maintaining Content Originator ordering privacy.	R1C; Must
RD-1490	17.4.0-1.0-6	The system shall provide measures that preclude a single authorized administrator from listing an end user's orders.	R1C; Must

RD-1491	17.5	***17.5 Security – Confidentiality***	
RD-1492	17.5.0-1	The system shall support the capability of maintaining confidentiality of user data (e.g., passwords).	R1B; Must
RD-1493	17.5.0-1.0-1	The system shall have the capability to provide confidentiality of user data, including user authentication data exchanged through external interfaces.	R1C; Must
RD-1496	17.5.0-1.0-1.0-3	The system shall use a minimum 128 bit key length for all symmetric encryption operations.	R1C; Must
RD-1497	17.5.0-1.0-2	The system shall have the capability to provide confidentiality of user data, including confidentiality of user authentication data stored within the system (e.g., passwords).	R1B; Must
RD-1498	17.5.0-2	The system shall support the capability of maintaining confidentiality of sensitive content in accordance with NIST and FIPS requirements for Sensitive But Unclassified (SBU) content.	R1C; Must
RD-1499	17.5.0-2.0-1	The system shall provide a method of protecting confidential and private Fdsys system data. (e.g., passwords, private user data, PII, credit cards numbers)	R1C; Must

RD-1502	17.6	***17.6 Security Administration***	
RD-1503	17.6.0-1	The system shall provide an administrative graphical user interface to perform user administration and security administration.	R1C; Must
RD-1504	17.6.0-1.0-1	The system shall provide an administrative graphical user interface to perform user administration.	R1C; Must
RD-1505	17.6.0-1.0-2	The system shall provide an administrative graphical user interface to perform security administration.	R1C; Must
RD-1506	17.6.0-2	The system shall have the capability for authorized security administrators to	R1C; Must

		set and maintain system security policy.	
RD-1507	17.6.0-2.0-1	The system shall have the capability for authorized security administrators to set system security policy.	R1C; Must
RD-1508	17.6.0-2.0-2	System security policy parameters shall include the capability to support various authentication methods.	R1C; Must
RD-1509	17.6.0-2.0-2.0-1	System security policy parameters shall include authorized user authentication methods.	R1C; Must
RD-1510	17.6.0-2.0-2.0-2	System security policy parameters shall include administrator authentication methods.	R1C; Must
RD-1511	17.6.0-2.0-2.0-3	System security policy parameters shall include minimum passwords lengths.	R1C; Must
RD-1512	17.6.0-2.0-2.0-4	System security policy parameters shall include authorized encryption algorithms.	R1C; Must
RD-1513	17.6.0-2.0-2.0-5	The system shall be flexible enough to incorporate additional, GPO-defined system security policy parameters.	R1C; Must
RD-1514	17.6.0-2.0-3	The system shall have the capability for authorized security administrators to maintain system security policy.	R1C; Must
RD-1515	17.6.0-3	The system shall provide the capability for authorized security administrators to monitor system security policy settings and policy enforcement.	R1C; Must
RD-1516	17.6.0-3.0-1	The system shall provide the capability for authorized security administrators to monitor system security policy settings.	R1C; Must
RD-1517	17.6.0-3.0-2	The system shall provide the capability for authorized security administrators to monitor system security policy enforcement.	R1C; Must
RD-1518	17.6.0-4	The system shall provide the capability to define tasks that require more than one authorized administrator to perform (e.g., setting or changing critical system security policies, two person integrity (TPI)).	R1C; Must
RD-1519	17.6.0-4.0-1	The system shall have the capability to enforce the separation of functions through assigned roles.	R1C; Must
RD-1520	17.6.0-4.0-2	The system shall provide the capability to partition security administration into logical elements such that security administrators can be assigned accordingly.	R1C; Must
RD-1521	17.6.0-4.0-3	The system shall provide the capability to limit security administrator's authority to assigned logical elements.	R1C; Must

RD-1522	17.7	***17.7 Security – Availability***	
RD-1523	17.7.0-1	The system shall provide appropriate backup and redundant components to ensure availability to meet customer and GPO needs.	R1C; Must
RD-1524	17.7.0-1.0-1	The system shall provide appropriate backup components to ensure availability to meet customer and GPO needs.	R1C; Must
RD-1525	17.7.0-1.0-2	The system shall provide appropriate redundant components to ensure availability to meet customer and GPO needs.	R1C; Must
RD-1526	17.7.0-1.0-3	The system shall be operational in the event of disaster situations with minimal business interruption to business functions.	R1C; Must
RD-1527	17.7.0-1.0-3.0-1	The system shall return to normal operations post-disaster.	R1C; Must
RD-1528	17.7.0-1.0-4	The system shall adhere to GPO's Continuity of Operations (COOP) plans.	R1C; Must
RD-1529	17.7.0-1.0-4.0-1	The system shall adhere to system development guidelines set forth in Office of Management and Budget Circular A-130.	R1C; Must
RD-1530	17.7.0-1.0-4.0-2	The system shall adhere to guidelines set forth in Federal Preparedness Circular 65.	R1C; Must
RD-1531	17.7.0-1.0-5	The system shall have appropriate failover components.	R1C; Must
RD-1532	17.7.0-1.0-6	The system shall be operational at appropriate GPO alternate facilities.	R1C; Must
RD-1533	17.7.0-1.0-7	The system shall back up system applications and data at a frequency as determined by business requirements.	R1C; Must
RD-1534	17.7.0-1.0-7.0-1	The system shall back up system applications at a frequency as determined by business requirements.	R1C; Must
RD-1535	17.7.0-1.0-7.0-2	The system shall back up system data at a frequency as determined by business requirements.	R1C; Must
RD-1536	17.7.0-1.0-7.0-3	The system applications and data shall be backed up at off-site storage location.	R1C; Must
RD-1537	17.7.0-1.0-7.0-4	The system applications shall be backed up at off-site storage location.	R1C; Must
RD-1538	17.7.0-1.0-7.0-5	The system data shall be backed up at off-site storage location.	R1C; Must
RD-1539	17.7.0-1.0-8	The system shall interface with designated GPO Service Providers (e.g. Oracle).	R1C; Must

RD-1540	17.7.0-1.0-9	The system shall maintain data integrity during backup processing.	R1B; Must
RD-1541	17.7.0-1.0-10	The system shall have no restrictions that would prevent the system from being operated at a hosting vendor site, at GPO's sole discretion, at any point in the future.	R1B; Must
RD-1542	17.7.0-1.0-11	The system shall have the following security capabilities to permit the system to be operated at a hosting vendor site, at GPO's sole discretion.	R1C; Must
RD-1543	17.7.0-1.0-11.0-1	Mutually authenticated, high speed connection between GPO offices and hosting site shall be utilized.	R1C; Must
RD-1544	17.7.0-1.0-11.0-2	Encrypted connection using industry standard IPSEC Virtual Private Network (VPN) and strong (128 bit key minimum) encryption shall be utilized.	R1C; Must

RD-1545	17.8	***17.8 Security – Integrity***	
RD-1546	17.8.0-1	The system shall have the capability to assure integrity of business process information (BPI).	R1C; Must
RD-1547	17.8.0-2	The system shall check content for malicious code (e.g., worms and viruses) prior to ingest to maintain integrity.	R1B; Must
RD-1548	17.8.0-2.0-1	The system shall utilize GPO virus scanner technology.	R1B; Must
RD-1549	17.8.0-2.0-2	If malicious code is detected in content, it shall be placed into a quarantine area for GPO inspection.	R1B; Must

RD-1550	17.9	***17.9 Security Standards***	
RD-1551	17.9.0-1	The system shall have the capability to support the following industry integrity standards.	
RD-1552	17.9.0-1.0-1	The system shall have the capability to support the RSA Digital Signature in accordance with IETF RFC 3447.	R1C; Must
RD-1553	17.9.0-1.0-2	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #1 standards.	R1C; Must
RD-1554	17.9.0-1.0-3	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #7 standards.	R1C; Must
RD-1555	17.9.0-1.0-4	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #11 standards.	R1C; Must
RD-1556	17.9.0-1.0-5	The system shall have the capability to support Public Key Infrastructure (PKI) PKCS #12 standards.	R1C; Must
RD-1557	17.9.0-1.0-6	The system shall have the capability to support the International Telephone Union (ITU) X.509 v3 standard for certificate format.	R1C; Must
RD-1558	17.9.0-1.0-7	The system shall have the capability to support the IETF Public Key Infrastructure Exchange (PKIX) X.509 v3 standards for certificate compatibility.	R1C; Must
RD-1559	17.9.0-1.0-8	The system shall have the capability to support the Keyed-Hash Message Authentication Code (HMAC) standard as specified in FIPS Pub 198.	R1C; Must
RD-1560	17.9.0-1.0-9	The system shall have the capability to support the Cyclical Redundancy Checking (CRC) 32 (CRC-32) standard, to include Cyclic Redundancy Checking (CRC) and checksum.	R1C; Must
RD-1561	17.9.0-1.0-10	The system shall have the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-1 standard.	R1C; Must
RD-1562	17.9.0-1.0-11	The system shall the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-256 standard.	R1C; Must
RD-1563	17.9.0-1.0-12	The system shall have the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-384 standard.	R1C; Must
RD-1564	17.9.0-1.0-13	The system shall have the capability to support the FIPS 180-2 Secure Hash Algorithm (SHA) SHA-512 standard.	R3; Must
RD-1565	17.9.0-1.0-14	The system shall have the capability to support the XML Digital Signature standards defined in RFC 3275 and XMLDSIG.	R1C; Must
RD-1566	17.9.0-2	The system shall have the capability to support the following confidentiality standards.	R1C; Must
RD-1567	17.9.0-2.0-1	The system shall have the capability to support the FIPS 197 Advanced Encryption Standard (AES).	R1C; Must
RD-1568	17.9.0-2.0-2	The system shall have the capability to support the ANSI X9.52 Triple Data Encryption Standard (TDES).	R1C; Must
RD-1569	17.9.0-2.0-3	The system shall have the capability to support the Secure Sockets Layer	R1C; Must

		(SSL) version 3 / Transport Layer Security (TLS) standards per the guidelines in NIST SP 800-52.	
RD-1570	17.9.0-2.0-4	The system shall have the capability to comply with FIPS 140-2.	R1C; Must
RD-1571	17.9.0-2.0-5	The system shall have the capability to support the W3C XML Encryption standard XMLENC.	R1C; Must
RD-1572	17.9.0-3	The system shall have the capability to support the following access control standards.	R1C; Must
RD-1573	17.9.0-3.0-1	The system shall have the capability to support the Lightweight Directory Access Protocol (LDAP) Internet Engineering Task Force (IETF) Request for Comments (RFC) 2251.	R1C; Must
RD-1574	17.9.0-3.0-2	The system shall have the capability to support the International Telephone Union (ITU) X.500 standards.	R1C; Must
RD-1575	17.9.0-3.0-3	The system shall have the capability to support the Security and Access Markup Language (SAML) version 2 standard as specified by OASIS.	R1C; Must
RD-1576	18	**18 Requirements for Enterprise Service Bus**	
RD-1577	18.1	***18.1 ESB Core Capabilities***	
RD-1578	18.1.0-1	The system shall provide the capability to interoperate with services or applications deployed in different hardware and software platforms.	R1C; Must
RD-1579	18.1.0-1.0-1	The ESB shall support interoperability with Java Enterprise Edition (JEE).	R1B; Must
RD-1580	18.1.0-1.0-2	The ESB shall support interoperability with .Net.	R1C; Must
RD-1581	18.1.0-1.0-3	The ESB shall support interoperability with Web Services.	R1B; Must
RD-1582	18.1.0-1.0-4	The ESB shall support interoperability with Java Message Service (JMS).	R1B; Must
RD-1583	18.1.0-1.0-5	The ESB shall support common operating systems.	R1B; Must
RD-1584	18.1.0-1.0-5.0-1	The ESB shall support Microsoft Windows Server 2003.	R1B; Must
RD-1585	18.1.0-1.0-5.0-2	The ESB shall support Red Hat Enterprise Advanced Server 2.1.	R1B; Must
RD-1586	18.1.0-1.0-6	The ESB shall support application programmer interfaces in common programming languages.	R1C; Must
RD-1587	18.1.0-1.0-6.0-1	The ESB shall support application programmer interfaces in C.	R1B; Must
RD-1588	18.1.0-1.0-6.0-2	The ESB shall support application programmer interfaces in C++.	R1B; Must
RD-1589	18.1.0-1.0-6.0-3	The ESB shall support application programmer interfaces in Java.	R1B; Must
RD-1590	18.1.0-1.0-6.0-4	The ESB shall support application programmer interfaces in C#.	R1C; Must
RD-1591	18.1.0-2	The system shall support the ability to authenticate applications and services and control which applications can invoke a service.	R2; Must
RD-1592	18.1.0-2.0-1	The system shall support the capability to authenticate internal processes attempting to invoke a service provided by the system.	R2; Must
RD-1593	18.1.0-2.0-2	The system shall support the capability to authenticate external processes attempting to invoke a service provided by the system.	R2; Must
RD-1594	18.1.0-3	The system shall provide the capability to integrate newly developed (or acquired) services or applications (e.g. ILS, Oracle).	R1C; Must
RD-1595	18.1.0-3.0-1	The system shall provide the capability to integrate with Oracle applications and services.	R1C; Must
RD-1596	18.1.0-4	The system shall provide the capability to integrate existing (or legacy) services or applications.	R1B; Must
RD-1597	18.1.0-4.0-1	The system shall provide the capability to integrate with the ILS.	R1B; Must
RD-1598	18.1.0-5	The system shall provide the capability to coordinate and manage services or applications in the form of enterprise business processes.	R1C; Must
RD-1599	18.1.0-6	The system shall provide the capability to support synchronous and asynchronous communications between services or applications.	R1C; Must
RD-1600	18.1.0-6.0-1	The system shall provide the capability to support synchronous communications between services or applications.	R1B; Must
RD-1601	18.1.0-6.0-2	The system shall provide the capability to support asynchronous communications between services or applications.	R1C; Must
RD-1602	18.1.0-6.0-3	The system shall provide the capability to support reliable communications between services or applications.	R1C; Must
RD-1603	18.1.0-6.0-4	The system shall provide the capability to specify the quality of service for communications between services or applications.	R1C; Must

RD-1604	18.1.0-6.0-5	The system shall provide the capability to queue communications between services and applications.	R1C; Must
RD-1605	18.1.0-7	The system shall provide the capability to run process transactions.	R1C; Must
RD-1606	18.1.0-7.0-1	The system shall provide the capability to manage process transactions declaratively via system configurations.	R1C; Must
RD-1607	18.1.0-7.0-1.0-1	The system shall provide the capability to manage process transactions declaratively using a GUI.	R1C; Must
RD-1608	18.1.0-7.0-1.0-2	The system shall provide the capability to store process transactions configuration information in XML.	R1C; Must
RD-1609	18.1.0-7.0-2	The system shall provide the capability to execute pre-defined process transactions.	R1C; Must
RD-1610	18.1.0-7.0-3	The system shall provide the capability to manually commit and roll back process transactions.	R1C; Must
RD-1611	18.1.0-8	The system shall provide the capability to create communications between services or applications, internal or external, in XML form with published schemas.	R1C; Must
RD-1612	18.1.0-8.0-1	The system shall provide the capability to validate communications against the appropriate published schema.	R1C; Must
RD-1613	18.1.0-8.0-2	The system shall provide the capability to transform communications to different published schemas.	R1C; Must
RD-1614	18.1.0-9	The system shall provide the capability to perform XML document-based routing between services or applications.	R1B; Must
RD-1615	18.1.0-10	The system shall provide the capability to support incremental implementations.	R1C; Must
RD-1616	18.1.0-10.0-1	The ESB shall support the capability to deploy services without disrupting system operations.	R1C; Must
RD-1617	18.1.0-10.0-2	The ESB shall support the capability to undeploy services without disrupting system operations that do not rely on the service which is being undeployed.	R1C; Must
RD-1618	18.1.0-10.0-3	The ESB shall support the capability to deploy applications without disrupting system operations.	R1C; Must
RD-1619	18.1.0-10.0-4	The ESB shall support the capability to undeploy applications without disrupting system operations that do not rely on the application which is being undeployed.	R1C; Must
RD-1620	18.1.0-11	The system shall provide the capability to support exception handling.	R1C; Must
RD-1621	18.1.0-11.0-1	The system shall provide the capability to generate compensating transactions for exceptions where possible.	R3; Should
RD-1622	18.1.0-12	The system shall store information related to the ESB in metadata.	R1B; Must
RD-1623	18.1.0-12.0-1	The system shall store information about schemas in metadata.	R1C; Must
RD-1624	18.1.0-12.0-1.0-1	The ESB shall support WSDL.	R1B; Must
RD-1625	18.1.0-12.0-1.0-2	The ESB shall support WS-Security.	R1C; Must
RD-1626	18.1.0-12.0-1.0-3	The ESB shall support WS-Reliability or WS-Reliable Messaging	R1C; Must
RD-1627	18.1.0-12.0-2	The system shall store information about transactional operations in metadata.	R1B; Must
RD-1628	18.1.0-12.0-2.0-1	The system shall support the capability to record information about transactions in logs.	R1B; Must
RD-1629	18.1.0-12.0-3	The system shall store information about communications in metadata.	R1B; Must
RD-1630	18.1.0-12.0-3.0-1	The system shall support the capability to record information about message traffic in logs.	R1B; Must
RD-1631	18.1.0-12.0-4	The system shall store information about business processes in metadata.	R1B; Must
RD-1632	18.1.0-12.0-4.0-1	The system shall support the capability to record information about business process execution in logs.	R1B; Must

RD-1633	18.2	***18.2 ESB Configuration***	
RD-1634	18.2.0-1	The system shall provide the capability to perform integration configurations.	R1C; Must
RD-1635	18.2.0-1.0-1	The system shall provide the capability to manage integration configurations using a GUI.	R1C; Must
RD-1636	18.2.0-1.0-2	The system shall provide the capability to perform integration configurations in XML.	R1C; Must
RD-1637	18.2.0-1.0-3	The system shall provide the capability to store integration configuration information in XML.	R1C; Must
RD-1638	18.2.0-2	The system shall provide the capability to add redundancy to critical ESB functions.	R2; Must

RD-1639	18.3	***18.3 ESB Administration***	
RD-1640	18.3.0-1	The system shall provide the capability to impose rule-based security control over administrative tasks.	R3; Must
RD-1641	18.3.0-2	The system shall provide the capability to manage services or applications dynamically.	R1C; Must
RD-1642	18.3.0-3	The system shall provide the capability to enable and disable services dynamically.	R2; Must
RD-1643	18.3.0-3.0-1	The system shall provide the capability to enable services dynamically.	R2; Must
RD-1644	18.3.0-3.0-2	The system shall provide the capability to disable services dynamically.	R2; Must
RD-1645	18.3.0-4	The system shall provide the capability to manage business processes.	R1C; Must
RD-1646	18.3.0-4.0-1	The system shall provide the capability to support business process orchestration.	R1C; Must
RD-1647	18.3.0-5	The system shall provide the capability to terminate, suspend and resume business processes.	R1C; Must
RD-1648	18.3.0-5.0-1	The system shall provide the capability to terminate business processes that are being orchestrated.	R1C; Must
RD-1649	18.3.0-5.0-2	The system shall provide the capability to suspend business processes that are being orchestrated.	R1C; Must
RD-1650	18.3.0-5.0-3	The system shall provide the capability to resume business processes that are suspended.	R1C; Must
RD-1651	18.3.0-6	The system shall provide the capability to monitor ESB processes that are being orchestrated.	R1C; Must
RD-1652	18.3.0-6.0-1	The system shall provide the capability to monitor the business processes at all available statuses: active, suspended, terminated, and completed.	R1C; Must
RD-1653	18.3.0-6.0-2	The system shall provide the capability to monitor communication latencies.	R1C; Must
RD-1654	18.3.0-6.0-3	The system shall provide the capability to send notifications in the event of problems with ESB functions.	R1C; Must

RD-1655	18.4	***18.4 ESB Interface***	
RD-1656	18.4.0-1	The system shall provide the capability to perform configuration tasks via a Graphical User Interface (GUI) tool.	R1C; Must
RD-1657	18.4.0-2	The system shall provide the capability to perform administrative tasks via a GUI tool.	R1C; Must

RD-1658	19	**19 Requirements for Data Mining**	
RD-1659	19.1	***19.1 Data Mining – Data Extraction***	
RD-1660	19.1.0-1	The system shall be capable of extracting data from the entire collection of BPI.	R2; Must
RD-1661	19.1.0-2	The system shall be capable of extracting data from the entire collection of metadata.	R2; Must
RD-1662	19.1.0-3	The system shall be capable of extracting data from select GPO data sources (e.g., Oracle).	R3; Must
RD-1663	19.1.0-3.0-1	The system shall be capable of extracting data from Oracle.	R2; Must
RD-1664	19.1.0-3.0-2	The system shall be capable of extracting data from additional GPO data sources in the future.	R3; Must
RD-1665	19.1.0-4	The system shall be capable of extracting data according to a schedule defined by users.	R1C; Should / R2; Must
RD-1666	19.1.0-5	The system shall be able to extract data according to user defined queries.	R2; Must
RD-1667	19.1.0-6	The system shall be able to extract random samples of data.	R1C; Could / R2; Must
RD-1668	19.1.0-7	The system shall allow users to input data to supplement system data (e.g., Web log, historical sales data).	R1C; Should / R2; Must

RD-1669	19.1.0-7.0-1	The system shall allow users to upload files from which data will be extracted for analysis.	R1C; Should / R2; Must
RD-1670	19.1.0-7.0-2	The system shall allow users to enter supplemental historical data.	R1C; Should / R2; Must
RD-1671	19.1.0-7.0-3	The system shall allow users to restrict access to supplemental data.	R1C; Should / R2; Must
RD-1672	19.1.0-7.0-4	The system shall allow users to store supplemental data for future use.	R1C; Should / R2; Must
RD-1673	19.1.0-8	The system shall be capable of extracting data from multiple formats.	R2; Must
RD-1674	19.1.0-8.0-1	The system shall be capable of extracting data from data sources in XML format.	R2; Must
RD-1675	19.1.0-8.0-2	The system shall be capable of extracting data from data sources in PDF format.	R2; Must
RD-1676	19.1.0-8.0-3	The system shall be capable of extracting data from data sources in XLS format.	R2; Must
RD-1677	19.1.0-8.0-4	The system shall be capable of extracting data from data sources in CSV format.	R2; Must
RD-1678	19.1.0-8.0-5	The system shall be support the capability of extracting data from data sources in additional formats in the future.	R3; Must
RD-1679	19.1.0-9	The system shall be capable of data extraction at speeds sufficient to support the creation of real-time reports.	R1C; Should / R2; Must

RD-1680	19.2	***19.2 Data Mining – Data Normalization***	
RD-1681	19.2.0-1	The system shall be able to normalize data based on additional administrator defined parameters in the future.	R2; Must
RD-1682	19.2.0-1.0-1	The system shall be able to identify missing values or metadata elements.	R2; Must
RD-1683	19.2.0-1.0-2	The system shall be able to identify data anomalies in BPI and metadata.	R2; Must
RD-1684	19.2.0-1.0-3	The system shall be able to identify data formats.	R2; Must
RD-1685	19.2.0-1.0-4	The system shall be able to identify format discrepancies.	R2; Must
RD-1686	19.2.0-1.0-5	The system shall be able to identify standard data elements.	R2; Must
RD-1687	19.2.0-1.0-6	The system shall be able to identify data types.	R2; Must
RD-1688	19.2.0-2	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).	R2; Must

RD-1689	19.3	***19.3 Data Mining – Data Analysis and Modeling***	
RD-1690	19.3.0-1	The system shall be able to perform single variable and multivariable analysis operations on extracted data.	R2; Must
RD-1691	19.3.0-1.0-1	The system shall be able to perform single variable analysis operations on extracted data.	R2; Must
RD-1692	19.3.0-1.0-2	The system shall be able to perform multivariable analysis operations on extracted data.	R2; Must
RD-1693	19.3.0-1.0-3	The system shall be able to calculate averages (mean, median, mode).	R2; Must
RD-1694	19.3.0-1.0-3.0-1	The system shall be able to calculate means.	R2; Must
RD-1695	19.3.0-1.0-3.0-2	The system shall be able to calculate medians.	R2; Must
RD-1696	19.3.0-1.0-3.0-3	The system shall be able to calculate modes.	R2; Must
RD-1697	19.3.0-1.0-4	The system shall be able to perform cross tabulations.	R1C; Could / R2; Must
RD-1698	19.3.0-1.0-5	The system shall be able to perform clusterization.	R1C; Could / R2; Must
RD-1699	19.3.0-1.0-6	The system shall be able to perform categorization.	R1C; Could / R2; Must
RD-1700	19.3.0-1.0-7	The system shall be able to perform association and link analyses.	R1C; Could

			/ R2; Must
RD-1701	19.3.0-1.0-8	The system shall be able to perform regression analysis.	R1C; Could / R2; Must
RD-1702	19.3.0-1.0-9	The system shall be able to expose hierarchical or parent/child relationships.	R1C; Could / R2; Must
RD-1703	19.3.0-1.0-10	The system shall be able to expose sequential relationships and patterns.	R1C; Could / R2; Must
RD-1704	19.3.0-1.0-10.0-1	The system shall be able to expose sequential relationships.	R1C; Could / R2; Must
RD-1705	19.3.0-1.0-10.0-2	The system shall be able to expose sequential patterns.	R1C; Could / R2; Must
RD-1706	19.3.0-1.0-11	The system shall be able to expose temporal relationships and patterns.	R1C; Could / R2; Must
RD-1707	19.3.0-1.0-11.0-1	The system shall be able to expose temporal relationships.	R1C; Could / R2; Must
RD-1708	19.3.0-1.0-11.0-2	The system shall be able to expose temporal patterns.	R1C; Could / R2; Must
RD-1709	19.3.0-1.0-12	The system shall be able to expose inferences and rules that led to a result set.	R2; Could / R3; Must
RD-1710	19.3.0-2	The system shall be able to warn users attempting illogical operations (e.g., calculating averages out of categorical data).	R2; Could
RD-1711	19.3.0-2.0-1	The system shall be capable of showing the user the rule violation that led to the warning.	R2; Could
RD-1712	19.3.0-3	The system shall allow users to suspend, resume, or restart analysis	R1C; Should / R2; Must
RD-1713	19.3.0-3.0-1	The system shall allow users to suspend an analysis that is in progress.	R1C; Should / R2; Must
RD-1714	19.3.0-3.0-2	The system shall allow users to resume a suspended analysis.	R1C; Should / R2; Must
RD-1715	19.3.0-3.0-3	The system shall allow users to restart an analysis from the beginning.	R1C; Should / R2; Must
RD-1716	19.3.0-4	The system shall be capable of providing the user with an estimated analysis time.	R2; Could

RD-1717	19.4	***19.4 Data Mining – Report Creation and Data Presentation***	
RD-1718	19.4.0-1	The system shall be able to produce reports summarizing the analysis of BPI and metadata.	R2; Must
RD-1719	19.4.0-1.0-1	The system shall allow users to choose from the data types available in BPI and metadata and choose operations performed on that data.	R2; Must
RD-1720	19.4.0-1.0-2	The system shall be able to produce a report summarizing system usage for a user-defined time range.	R2; Must
RD-1721	19.4.0-1.0-3	The system shall be able to produce a report analyzing the usage of search terms.	R2; Must
RD-1722	19.4.0-2	The system shall be capable of including graphical analysis in reports, including charts, tables, and graphs.	R1C; Should / R2; Must
RD-1723	19.4.0-2.0-1	The system shall be capable of including charts in reports.	R1C; Should / R2; Must
RD-1724	19.4.0-2.0-2	The system shall be capable of including tables in reports.	R1C; Should / R2; Must
RD-1725	19.4.0-2.0-3	The system shall be capable of including graphs in reports.	R1C; Should / R2; Must
RD-1726	19.4.0-3	The system shall allow a set of default report templates to be accessible for each user class.	R2; Must

RD-1727	19.4.0-3.0-1	The system shall allow users to manage the default templates.	R2; Must
RD-1728	19.4.0-4	The system shall allow users to create custom reports and report templates based on access rights to BPI and metadata.	R1C; Should / R2; Must
RD-1729	19.4.0-4.0-1	The system shall allow users to create custom report templates.	R1C; Should / R2; Must
RD-1730	19.4.0-4.0-2	The system shall allow users to update custom report templates.	R1C; Should / R2; Must
RD-1731	19.4.0-4.0-3	The system shall allow users to delete custom report templates.	R1C; Should / R2; Must
RD-1732	19.4.0-5	The system shall be capable of real-time population of report templates.	R1C; Should / R2; Must
RD-1733	19.4.0-6	The system shall be capable of automatically creating reports using report templates according to a schedule defined by users.	R1C; Could / R2; Must
RD-1734	19.4.0-6.0-1	The system shall allow users to request notification that a scheduled report is available.	R1C; Could / R2; Must
RD-1735	19.4.0-6.0-2	The system shall enable GPO users to restrict view/modify access to customized report templates.	R1C; Could / R2; Must
RD-1736	19.4.0-6.0-2.0-1	The system shall enable GPO users to control which users can view a report template.	R1C; Could / R2; Must
RD-1737	19.4.0-6.0-2.0-2	The system shall enable GPO users to control which users can modify a report template.	R1C; Could / R2; Must
RD-1738	19.4.0-7	The system shall be capable of delivering reports to users.	R1C; Could / R2; Must
RD-1739	19.4.0-7.0-1	The system shall allow users to specify delivery method (e.g., e-mail, RSS, FTP).	R1C; Could / R2; Must
RD-1740	19.4.0-7.0-1.0-1	The system shall support the capability to deliver reports to users using E-mail.	R1C; Could / R2; Must
RD-1741	19.4.0-7.0-1.0-2	The system shall support the capability to deliver reports to users using RSS.	R1C; Could / R2; Must
RD-1742	19.4.0-7.0-1.0-3	The system shall support the capability to deliver reports to users using FTP.	R1C; Could / R2; Must
RD-1743	19.4.0-8	The system shall be capable of supporting real-time reporting.	R1C; Should / R2; Must
RD-1744	19.4.0-9	The system shall allow users to create notifications based on real-time analysis of BPI or metadata.	R1C; Should / R2; Must
RD-1745	19.4.0-10	The system shall be able to link analysis results to data.	R2; Could
RD-1746	19.4.0-11	The system shall be able to expose analysis criteria and algorithms.	R2; Could
RD-1747	19.4.0-12	The system shall be able to export results in a format specified by the user (e.g., HTML, MS Word, MS Excel, character-delimited text file, XML, PDF).	R2; Must
RD-1748	19.4.0-12.0-1	The system shall be able to export reports in HTML format.	R2; Must
RD-1749	19.4.0-13	The system shall support customization and personalization functions as defined in the FDsys access, search, request, interface, cataloging and reference tools, and user support requirements.	R2; Must
RD-1750	19.4.0-13.0-1	The system shall support user interface customization and personalization based on the interactions of a user with the system.	R2; Must
RD-1751	19.4.0-13.0-2	The system shall support user interface customization by aggregating the interactions of many users with the system.	R2; Must

RD-1752	19.5	***19.5 Data Mining – Security and Administration***	
RD-1753	19.5.0-1	The system shall restrict access to extracted data based on user groups.	R2; Must
RD-1754	19.5.0-1.0-1	The system shall allow users to extract data from security audit logs for data mining	R2; Must
RD-1767	19.5.0-14	The system shall perform records management functions on logs.	R2; Must

RD-1768	19.6	***19.6 Data Mining – Storage***	
RD-1769	19.6.0-1	The system shall store extracted data.	R2; Must
RD-1770	19.6.0-1.0-1	Extracted data shall be held in temporary storage. Once analysis is complete, extracted data is deleted from temporary storage.	R2; Must
RD-1771	19.6.0-1.0-1.0-1	The system shall provide the capability to store the corpus of extracted data.	R2; Must
RD-1772	19.6.0-1.0-1.0-2	The system shall provide the capability to delete selected portions of the corpus of extracted data.	R2; Must
RD-1773	19.6.0-1.0-1.0-3	The system shall provide the capability to reload selected portions of the corpus of extracted data by re-extracting the data.	R2; Must
RD-1774	19.6.0-2	The system shall store metadata, supplemental data, reports, report templates, analysis criteria, and algorithms in Business Process Storage.	R2; Must
RD-1775	19.6.0-2.0-1	The system shall store metadata in Business Process Storage.	R2; Must
RD-1776	19.6.0-2.0-2	The system shall store supplemental data in Business Process Storage.	R2; Must
RD-1777	19.6.0-2.0-3	The system shall store reports in Business Process Storage.	R2; Must
RD-1778	19.6.0-2.0-4	The system shall store report templates in Business Process Storage.	R2; Must
RD-1779	19.6.0-2.0-5	The system shall store analysis criteria in Business Process Storage.	R2; Must
RD-1780	19.6.0-2.0-6	The system shall store algorithms in Business Process Storage.	R2; Must
RD-1781	19.6.0-2.0-7	The system shall have a records management process (e.g., delete files and reports at a defined time).	R2; Must

RD-1782	20	**20 Requirements for Content Submission**	
RD-1783	20.1	***20.1 Content Submission Core Capabilities***	
RD-1784	20.1.0-1	The system shall accept digital content and metadata.	R1B; Must
RD-1785	20.1.0-2	The system shall create a SIP from content and metadata.	R1B; Must

RD-1786	20.2	***20.2 Content Submission – System Administration***	
RD-1787	20.2.0-1	The system shall to be able to accept, store, and deliver encrypted files.	R2; Could
RD-1788	20.2.0-2	The system shall provide notification to the submission agency/authority that the content has been received by Fdsys.	R1C; Must
RD-1789	20.2.0-2.0-1	The system shall notify submission agency/authority if content is not received.	R1C; Must
RD-1790	20.2.0-3	The system shall have the capability to provide notification to the submission agency/authority that the content has been released to the intended users.	R1B; Could / R1C; Must
RD-1791	20.2.0-4	The system shall identify files with security restrictions upon submission.	R1C; Must
RD-1792	20.2.0-4.0-1	Information about the files will be recorded in metadata.	R1B; Must
RD-1793	20.2.0-5	The system shall have the capability to allow users to indicate that content contains copyrighted material.	R1C; Must
RD-1794	20.2.0-5.0-1	The system shall have the capability to allow users to specify what the intended use and access rights to the content should be.	R1C; Must
RD-1795	20.2.0-5.0-2	The system shall have the capability to allow users to specify what the intended distribution of the content should be.	R1C; Must
RD-1796	20.2.0-5.0-3	The system shall have the capability to allow authorized users to modify access rights to content based on copyright information provided by Content Originators.	R1C; Must
RD-1797	20.2.0-5.0-4	The system shall have the capability to notify authorized users that copyrighted content has been submitted.	R1C; Must
RD-1798	20.2.0-5.0-5	Copyright information will be recorded in metadata.	R1C; Must
RD-1799	20.2.0-6	The system shall provide WIP storage for content prior to ingest.	R1B; Must
RD-1800	20.2.0-7	The system shall check content prior to ingest.	R1B; Must
RD-1803	20.2.0-7.0-3	Zipped files (.zip) shall be unzipped.	R1C; Must

RD-1804	20.2.0-7.0-4	Stuffed files (.sit) shall be unstuffed.	R1C; Must
RD-1805	20.2.0-8	The system shall accept content with specialized character sets (e.g., non-Roman, scientific notations)	R1B; Must

RD-1806	20.3	***20.3 Content Submission Metadata***	
RD-1807	20.3.0-1	The system shall accept all administrative and descriptive metadata supplied by the submission agency/authority.	R1B; Must
RD-1808	20.3.0-1.0-1	The system shall provide the capability to record Title or caption of content.	R1B; Must
RD-1809	20.3.0-1.0-2	The system shall provide the capability to record content identifiers assigned to content.	R1B; Must
RD-1810	20.3.0-1.0-2.0-1	The system shall provide the capability to record the Persistent names assigned to content.	R1B; Must
RD-1811	20.3.0-1.0-2.0-2	The system shall provide the capability to record the filenames assigned to content.	R1B; Must
RD-1812	20.3.0-1.0-2.0-3	The system shall provide the capability to record the ISBN/ISSNs assigned to content.	R1B; Must
RD-1813	20.3.0-1.0-2.0-4	The system shall provide the capability to record the Agency requisition numbers assigned to content.	R1B; Must
RD-1814	20.3.0-1.0-2.0-5	The system shall support the capability to record additional content identifiers in the future.	R3; Must
RD-1815	20.3.0-1.0-3	The system shall provide the capability to record Author/Creator of the content.	R1B; Must
RD-1816	20.3.0-1.0-4	The system shall provide the capability to record Publisher/Authority of the content.	R1B; Must
RD-1817	20.3.0-1.0-5	The system shall provide the capability to record Rights Owner of the content.	R1B; Must
RD-1818	20.3.0-1.0-6	The system shall provide the capability to record version information of the content.	R1B; Must
RD-1819	20.3.0-1.0-7	The system shall provide the capability to record relationships between content packages and digital objects.	R1B; Must
RD-1820	20.3.0-1.0-7.0-1	The system shall provide the capability to record superseded document information (i.e. publication title(s), series number, and stock number(s) of replaced versions).	R1B; Must
RD-1821	20.3.0-1.0-8	The system shall provide the capability to record content description information (e.g., abstract, summary).	R1B; Must
RD-1822	20.3.0-1.0-9	The system shall provide the capability to record Structure Information of the content.	R1B; Must
RD-1823	20.3.0-1.0-10	The system shall provide the capability to record Intended Output of the content.	R1B; Must
RD-1824	20.3.0-1.0-11	The system shall provide the capability to record Intended Audience of the content.	R1B; Must
RD-1825	20.3.0-1.0-12	The system shall provide the capability to record 13 Digit ISBN Numbers to content.	R1B; Must
RD-1826	20.3.0-2	The system shall record or ascertain the following information when available and applicable.	R2; Must
RD-1827	20.3.0-3	The system shall record or ascertain elements relating to documents.	R1B; Must
RD-1828	20.3.0-4	The system shall record the software applications and versions used to create the digital objects.	R1B; Must
RD-1829	20.3.0-4.0-1	The system shall ascertain the software applications and versions used to create the digital objects.	R1C; Should/ R2; Must
RD-1830	20.3.0-4.0-2	The system shall ascertain the page size of the publication.	R1C; Should/ R2; Must
RD-1888	20.3.0-4.0-3	The system shall record the page size of the publication.	R1B; Must
RD-1831	20.3.0-4.0-4	The system shall ascertain the trim size of the publication.	R1C; Should/ R2; Must
RD-1889	20.3.0-4.0-5	The system shall record the trim size of the publication.	R1B; Must
RD-1832	20.3.0-4.0-6	The system shall ascertain the number of pages.	R1C; Should/ R2; Must
RD-1890	20.3.0-4.0-7	The system shall record the number of pages.	R1B; Must

RD-1833	20.3.0-4.0-8	The system shall ascertain the file formats.	R1C; Should/ R2; Must
RD-1891	20.3.0-4.0-9	The system shall record the file formats.	R1B; Must
RD-1834	20.3.0-4.0-10	The system shall ascertain file sizes.	R1C; Should/ R2; Must
RD-1892	20.3.0-4.0-11	The system shall record file sizes.	R1B; Must
RD-1835	20.3.0-4.0-12	The system shall ascertain what fonts are used in the publication.	R1C; Should/ R2; Must
RD-1893	20.3.0-4.0-13	The system shall record what fonts are used in the publication.	R1B; Must
RD-1836	20.3.0-4.0-14	The system shall ascertain if the fonts are furnished or embedded.	R1C; Should/ R2; Must
RD-1894	20.3.0-4.0-15	The system shall record if the fonts are furnished or embedded.	R1B; Must
RD-1837	20.3.0-4.0-16	The system shall ascertain font types.	R1C; Should/ R2; Must
RD-1895	20.3.0-4.0-17	The system shall record font types.	R1B; Must
RD-1838	20.3.0-4.0-18	The system shall ascertain what color mode(s) are used in the publication.	R1C; Should/ R2; Must
RD-1896	20.3.0-4.0-19	The system shall record what color mode(s) are used in the publication.	R1B; Must
RD-1839	20.3.0-4.0-20	The system shall ascertain whether bleed is required/provided for.	R1C; Should/ R2; Must
RD-1897	20.3.0-4.0-20.0-1	The system shall record whether bleed is required/provided for.	R1B; Must
RD-1840	20.3.0-4.0-21	The system shall ascertain information about the construction of a publication.	R1C; Should/ R2; Must
RD-1898	20.3.0-4.0-22	The system shall record information about the construction of a publication.	R1B; Must
RD-1841	20.3.0-4.0-23	The system shall ascertain image resolutions.	R1C; Should/ R2; Must
RD-1899	20.3.0-4.0-24	The system shall record image resolutions.	R1B; Must
RD-1842	20.3.0-4.0-25	The system shall ascertain the language of the publication.	R1C; Should/ R2; Must
RD-1900	20.3.0-4.0-26	The system shall record the language of the publication.	R1B; Must
RD-1843	20.3.0-4.0-27	The system shall ascertain file compression information.	R1C; Should/ R2; Must
RD-1901	20.3.0-4.0-28	The system shall record file compression information.	R1B; Must
RD-1844	20.3.0-4.0-29	The system shall ascertain audio file formats.	R1C; Should/ R2; Must
RD-1904	20.3.0-4.0-30	The system shall record audio file formats.	R1C; Must
RD-1845	20.3.0-4.0-31	The system shall ascertain the size of audio files.	R1C; Should/ R2; Must
RD-1905	20.3.0-4.0-32	The system shall record the size of audio files.	R1C; Must
RD-1846	20.3.0-4.0-33	The system shall ascertain audio playing time.	R1C; Should/ R2; Must
RD-1906	20.3.0-4.0-34	The system shall record audio playing time.	R1C; Must
RD-1847	20.3.0-4.0-35	The system shall ascertain the language of audio.	R1C; Should/ R2; Must
RD-1907	20.3.0-4.0-36	The system shall record the language of audio.	R1C; Must
RD-1848	20.3.0-4.0-37	The system shall ascertain audio file compression information.	R1C; Should/ R2; Must
RD-1908	20.3.0-4.0-38	The system shall record audio file compression information.	R1C; Must

RD-1849	20.3.0-4.0-39	The system shall support the capability to ascertain the bit rate of audio.	R1C; Should/ R2; Must
RD-1909	20.3.0-4.0-40	The system shall support the capability to record the bit rate of audio.	R1C; Must
RD-1850	20.3.0-4.0-41	The system shall ascertain video file formats.	R1C; Should/ R2; Must
RD-1912	20.3.0-4.0-42	The system shall record video file formats.	R1C; Must
RD-1851	20.3.0-4.0-43	The system shall ascertain video file sizes.	R1C; Should/ R2; Must
RD-1913	20.3.0-4.0-44	The system shall record video files sizes.	R1C; Must
RD-1852	20.3.0-4.0-45	The system shall ascertain closed captioning information.	R1C; Should/ R2; Must
RD-1914	20.3.0-4.0-46	The system shall record closed captioning information.	R1C; Must
RD-1853	20.3.0-4.0-47	The system shall ascertain video runtime.	R1C; Should/ R2; Must
RD-1915	20.3.0-4.0-48	The system shall record video runtime.	R1C; Must
RD-1854	20.3.0-4.0-49	The system shall ascertain video encoding scheme.	R1C; Should/ R2; Must
RD-1916	20.3.0-4.0-50	The system shall record video encoding scheme.	R1C; Must
RD-1855	20.3.0-4.0-51	The system shall ascertain the language of the video.	R1C; Should/ R2; Must
RD-1917	20.3.0-4.0-52	The system shall record the language of the video.	R1C; Must
RD-1856	20.3.0-4.0-53	The system shall ascertain video file compression information.	R1C; Should/ R2; Must
RD-1918	20.3.0-4.0-54	The system shall record video file compression information.	R1C; Must
RD-1902	20.3.0-5	The system shall record and ascertain other document elements in the future.	R3; Must
RD-1903	20.3.0-6	The system shall record or ascertain elements relating to audio.	R1C; Must
RD-1910	20.3.0-7	The system shall record or ascertain additional audio elements in the future.	R3; Must
RD-1911	20.3.0-8	The system shall record or ascertain elements relating to video.	R2; Must
RD-1919	20.3.0-9	The system shall record or ascertain additional video elements in the future.	R3; Must
RD-1920	20.3.0-10	The system shall provide the capability to support other formats in the future.	R3; Must

RD-1921	21	**21 Requirements for Deposited Content**	
RD-1922	21.1	***21.1 Deposited Content Core Capabilities***	
RD-1923	21.1.0-1	The system shall accept digital content and metadata provided by Content Originators.	R1C; Must
RD-1924	21.1.0-2	The system shall have the capability to notify Content Evaluators that new content has been received by the system.	R1C; Must
RD-1925	21.2	***21.2 Deposited Content Metadata***	
RD-1926	21.2.0-1	The system shall accept "approved for release" information for release rmation provided by the content originating agency.	R1C; Must
RD-1927	21.3	***21.3 Deposited Content Interfaces***	
RD-1928	21.3.0-1	Deposited content interface shall enable Congressional Content Originators and Agency Content Originators to:	R1C; Must

RD-1929	21.3.0-1.0-1	Submit digital content and metadata	R1C; Must
RD-1930	21.3.0-1.0-2	Submit content chain of custody information to the system	R1C; Must
RD-1931	21.3.0-1.0-3	Submit intended use information to the system	R1C; Must
RD-1932	21.3.0-1.0-4	Submit aved for release rmation	R1C; Must
RD-1933	21.3.0-1.0-5	Receive notification of receipt of content and content ID	R1C; Must
RD-1934	21.3.0-1.0-6	Receive notification if content is not received, explanation for why content was not received, and options for proceeding	R1C; Must
RD-1935	21.3.0-1.0-7	Receive notification of release of content	R1C; Must
RD-1937	21.3.0-2	Deposited content interface shall enable GPO Service Providers and external Service Providers to:	R1C; Must
RD-1938	21.3.0-2.0-1	Submit digital content and metadata	R1C; Must
RD-1939	21.3.0-2.0-2	Receive notification of receipt of content and content ID	R1C; Must
RD-1940	21.3.0-2.0-3	Receive notification if content is not received, explanation for why content was not received, and options for proceeding	R1C; Must

RD-1942	22	**22 Requirements for Converted Content**	
RD-1943	22.1	***22.1 Converted Content Core Capabilities***	
RD-1944	22.1.0-1	The system shall have capability to accept converted content.	R1C; Must
RD-1945	22.1.0-1.0-1	Digital content may be provided in file formats for digitized tangible documents as specified in Appendix B: Operational Specification for Converted Content.	R1C; Must

RD-1946	22.2	***22.2 Converted Content Interfaces***	
RD-1947	22.2.0-1	Converted content interface shall enable GPO Service Providers and external Service Providers to:	R1C; Must
RD-1948	22.2.0-1.0-1	Submit approved content and metadata.	R1C; Must
RD-1949	22.2.0-1.0-2	Receive notification of receipt of content and content ID	R1C; Must
RD-1950	22.2.0-1.0-3	Provide notification of release of content	R1C; Must
RD-1951	22.2.0-1.0-4	Receive notification if content is not received, explanation for why content was not received, and options for proceeding	R1C; Must
RD-1952	22.2.0-1.0-5	Manage converted content	R1C; Must

RD-1953	23	**23 Requirements for Harvested Content**	
RD-1954	23.1	***23.1 Harvested Content Core Capabilities***	
RD-1955	23.1.0-1	The system shall accept digital content and metadata delivered by the harvesting function.	R2; Must

RD-1956	23.2	***23.2 Harvested Content Metadata***	
RD-1957	23.2.0-1	The system shall provide the capability to record the date and time of harvest of content.	R2; Must

RD-1958	23.3	***23.3 Harvester Requirements***	
RD-1959	23.3.0-1	The harvester shall have the capability to discover, assess, and harvest in-scope content from targeted Web sites.	R2; Must

RD-1960	23.3.0-2	The harvester shall have the capability to ensure that it does not harvest the same content more than once.	R2; Must
RD-1961	23.3.0-3	The harvester shall have the capability to perform the discovery, assessment, and harvesting processes on target Web sites based on update schedules.	R2; Must
RD-1962	23.3.0-4	The harvester shall have capability to perform simultaneous harvests.	R2; Must
RD-1963	23.3.0-5	The harvester shall locate and harvest all levels of Web pages within a Web site.	R2; Must
RD-1964	23.3.0-6	The harvester shall go outside the target domains or Web sites only when the external domain contains in-scope content.	R1C; Should / R2; Must
RD-1965	23.3.0-7	The harvester shall stop the discovery process when a Robots.txt is present and prevents the harvester from accessing a Web directory, consistent with GPO business rules.	R2; Must
RD-1966	23.3.0-8	The harvester shall stop the discovery process when a linked Web page does not contain in-scope content.	R2; Must
RD-1967	23.3.0-9	The harvester shall flag content and URLs that are only partially harvested by the automated harvester for manual follow-up.	R2; Must
RD-1968	23.3.0-10	The harvester shall determine if the discovered content is within the scope of GPO dissemination programs as defined in 44USC1901, 1902, 1903, and by GPO.	R2; Must
RD-1969	23.3.0-11	The harvester shall collect in-scope discovered content and available metadata.	R2; Must
RD-1970	23.3.0-11.0-1	The harvester shall deliver all in-scope content and metadata to WIP storage.	R2; Must
RD-1971	23.3.0-11.0-2	The harvester shall have the ability to discover and collect all file types that may reside on target Web sites.	R2; Must
RD-1972	23.3.0-12	The harvester shall be able to harvest and transfer a complete, fully faithful copy of the original content (e.g., publication, digital object, audio and video streams).	R2; Must
RD-1973	23.3.0-13	The harvester shall have the ability to maintain the directory structure of Web sites that constitute entire publications.	R2; Must
RD-1974	23.3.0-14	The harvester shall have the capability to re-configure directory structures of harvested content based on GPO rules and instructions (e.g., all PDF files are placed in one folder).	R2; Must
RD-1975	23.3.0-15	The harvester shall be able to harvest hidden Web information.	R2; Must
RD-1976	23.3.0-15.0-1	The harvester shall be able to harvest content contained in query-based databases.	R2; Must
RD-1977	23.3.0-15.0-2	The harvester shall be able to harvest content contained in agency content management systems.	R2; Must
RD-1978	23.3.0-15.0-3	The harvester shall be able to harvest content contained on dynamically generated Web pages.	R2; Must
RD-1979	23.3.0-15.0-4	The harvester shall be able to harvest content contained on FTP servers.	R2; Must
RD-1980	23.3.0-15.0-5	The harvester shall be able to harvest content contained behind proxy servers.	R2; Must
RD-1981	23.3.0-15.0-6	The harvester shall be able to harvest content contained behind firewalls.	R2; Must
RD-1982	23.3.0-16	The harvester shall provide the capability to automatically route specific content for which scope determinations could not be made to Content Evaluators. These situations include, but are not limited to: . Content that could not be reached by the harvester (e.g., content behind robots.txt files and firewalls, restricted access databases, etc). . Duplicate content that appears on more than one official Federal Government Web site. . Content for which not enough information or metadata exists to make scope determinations based on harvester rules and instructions alone.	R2; Must
RD-1983	23.3.0-17	The harvester shall have the capability to time and date stamp content that has been harvested.	R2; Must

RD-1984	23.4	***23.4 Metadata Requirements for Harvester***	
RD-1985	23.4.0-1	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.	R2; Must
RD-1986	23.4.0-2	The harvester shall have the ability to locate and collect unique ID and	R2; Must

		title/caption information.	
RD-1987	23.4.0-3	The harvester shall have the ability to locate and collect author/creator, publisher/authority, and rights owner information.	R2; Must
RD-1988	23.4.0-4	The harvester shall have the ability to locate and collect topical information and bibliographic descriptions.	R2; Must
RD-1989	23.4.0-5	The harvester shall have the ability to locate and collect version, fixity, relationship, and provenance information.	R2; Must
RD-1990	23.4.0-6	The harvester shall have the ability to locate and collect technical, structural, file format, packaging and representation information.	R2; Must
RD-1991	23.4.0-7	The harvester shall have the ability to locate and collect administrative metadata	R2; Must
RD-1992	23.4.0-8	The harvester shall have the capability to record the time and date of harvest.	R2; Must

RD-1993	23.5	***23.5 Harvester Rules and Instructions***	
RD-1994	23.5.0-1	The harvester shall discover and identify Federal content (e.g., publications, digital objects, audio and video) on Web sites using criteria specified by GPO Business Units.	R2; Must
RD-1995	23.5.0-2	The harvester shall accept and apply rules and instructions that will be used to assess whether discovered content is within scope of GPO dissemination programs.	R2; Must
RD-1996	23.5.0-3	The harvester shall be able to create and store rule and instruction profiles for individual targeted Web sites.	R1C; Could / R2; Must

RD-1997	23.6	***23.6 Harvester Interface***	
RD-1998	23.6.0-1	The harvester shall provide a user interface to accommodate workflow management and scheduling of harvesting activities.	R2; Must
RD-1999	23.6.0-2	The user interface shall allow authorized users (GPO-specified) to schedule harvesting activities based on update schedules for targeted sites to be harvested.	R2; Must
RD-2000	23.6.0-2.0-1	Shall accommodate the scheduling of harvests, including but not limited to hourly, daily, weekly, biweekly, monthly, and yearly.	R2; Must
RD-2001	23.6.0-3	The user interface shall be able to manage rule and instruction profiles.	R2; Must

RD-2002	23.7	***23.7 System Administration for Harvester***	
RD-2003	23.7.0-1	The harvester shall provide quality control functions to test accuracy/precision of rule application.	R2; Must
RD-2004	23.7.0-2	The harvester shall be able to incorporate results of quality control functions into rule and instruction creation/refinement.	R2; Must
RD-2005	23.7.0-2.0-1	The harvester shall have the capability to log and produce reports on harvesting activities.	R2; Must
RD-2006	23.7.0-2.0-1.0-1	The harvester shall have the capability to log and report on Web sites visited by the harvester (e.g., date, time, frequency).	R2; Must
RD-2007	23.7.0-2.0-1.0-2	The harvester shall have the capability to log and report on content discovered, including location, title, description, and other relevant information.	R2; Must
RD-2008	23.7.0-2.0-1.0-3	The harvester shall have the capability to log and report on scope assessment decisions made by the harvester.	R2; Must
RD-2009	23.7.0-2.0-1.0-4	The harvester shall have the capability to log and report on target Web site structure, hierarchy, relationships, and directories.	R2; Must
RD-2010	23.7.0-2.0-1.0-5	The harvester shall have the capability to log and report on harvester failure or error rates (e.g. network problems, broken links, security rules, firewalls, corrupted content).	R2; Must
RD-2011	23.7.0-2.0-1.0-5.0-1	The harvester shall have the capability to log harvester failure or error rates (e.g. network problems, broken links, security rules, firewalls, corrupted content).	R2; Must
RD-2012	23.7.0-2.0-1.0-5.0-2	The harvester shall have the capability to report on harvester failure or error rates (e.g. network problems, broken links, security rules, firewalls, corrupted content).	R2; Must

RD-2013	23.7.0-2.0-1.0-6	The harvester shall have the capability to log and report comparing target Web sites at different points in time (e.g., different times of harvest)	R2; Must
RD-2014	23.7.0-3	The discovery and harvesting tools shall have the ability to identify GPO as the owner of the tools.	R2; Must
RD-2015	23.7.0-4	The harvester's method of identification shall not be intrusive to targeted Web site.	R2; Must
RD-2016	23.7.0-5	The harvester shall have the ability to collect integrity marks associated with content as it is being harvested.	R2; Must

RD-2017	24	**24 Requirements for Style Tools**	
RD-2018	24.1	***24.1 Style Tools Core Capabilities***	
RD-2019	24.1.0-1	Style tools shall accept content from authorized Content Originators, Service Providers, and Service Specialists for document creation.	R2; Could / R3; Must
RD-2020	24.1.0-2	Style tools shall accept metadata from authorized users (e.g., title, author).	R2; Could / R3; Must
RD-2021	24.1.0-3	Style tools shall provide the capability for users to create new content for document creation.	R2; Could / R3; Must
RD-2022	24.1.0-4	Style tools shall provide the capability for users to compose content for document creation including but not limited to text, images, and graphics.	R2; Could / R3; Must
RD-2023	24.1.0-4.0-1	Style tools shall allow users to compose content based on pre-defined design rules.	R2; Could / R3; Must
RD-2024	24.1.0-4.0-2	Style tools shall allow users to compose content using templates based on rules (e.g., agency style manuals).	R2; Could / R3; Must
RD-2025	24.1.0-4.0-3	Style tools shall have the capability to prompt users to define layout parameters from best available or system presented options.	R2; Could / R3; Must
RD-2026	24.1.0-5	Style tools shall allow multiple users to work collaboratively on the same content, prior to publication.	R2; Could / R3; Must
RD-2027	24.1.0-5.0-1	Style tools shall allow authorized users to approve/reject content changes made by collaborators.	R2; Could / R3; Must
RD-2028	24.1.0-5.0-1.0-1	Style tools shall track approval/rejection of changes to content, prior to publication.	R2; Could / R3; Must
RD-2029	24.1.0-5.0-1.0-2	Style tools shall allow for approval of content.	R2; Could / R3; Must
RD-2030	24.1.0-5.0-1.0-3	Style tools shall allow for approval of content presentation.	R2; Could / R3; Must
RD-2031	24.1.0-6	Style tools shall provide the capability to revert to a previously saved version of a working file (e.g., History palette).	R2; Could / R3; Must
RD-2032	24.1.0-7	Style tools shall provide the capability to track and undo changes to WIP content.	R2; Could / R3; Must
RD-2033	24.1.0-8	Style tools shall allow users to select output methods for viewing preliminary composition (i.e. Preparatory representation of content format or structure).	R2; Could / R3; Must
RD-2034	24.1.0-9	Style tools shall interface with Content Originator ordering.	R2; Could / R3; Must

RD-2035	24.2	***24.2 Style Tools – Automated Composition***	
RD-2036	24.2.0-1	Style tools shall have the capability to automatically compose content.	R2; Could / R3; Must
RD-2037	24.2.0-1.0-1	Style tools shall have the capability to automatically compose content and place graphical elements in locations using GPO or Agency guidelines.	R2; Could / R3; Must
RD-2038	24.2.0-1.0-2	Style tools shall have the capability to automatically compose content based on user preferences.	R2; Could / R3; Must
RD-2039	24.2.0-1.0-3	Style tools shall have the capability to automatically compose content based on content analysis.	R2; Could / R3; Must
RD-2040	24.2.0-2	Style tools shall allow users to modify automatically composed content.	R2; Could / R3; Must

RD-2041	24.3	***24.3 Style Tools – System Administration***	
RD-2042	24.3.0-1	The system shall accept content based on the access rights and privileges of the user submitting the content.	R2; Could / R3; Must
RD-2043	24.3.0-2	The system shall assign unique IDs to digital objects created by style tools.	R2; Could / R3; Must
RD-2044	24.3.0-3	The system shall provide storage for WIP style tools content.	R2; Could / R3; Must
RD-2045	24.3.0-3.0-1	The system shall allow management of WIP content based on access rights and privileges.	R2; Could / R3; Must
RD-2046	24.3.0-3.0-2	The system shall provide tracking of all WIP activities.	R2; Could / R3; Must
RD-2047	24.3.0-3.0-3	The system shall provide search and retrieval capabilities for WIP content.	R2; Could / R3; Must
RD-2048	24.3.0-4	The system shall provide search and retrieval capabilities for content stored within ACP storage (e.g., to allow Content Originators to pull unique digital objects into the style tools creative process).	R2; Could / R3; Must
RD-2049	24.3.0-4.0-1	The system shall have the capability to provide authorized users with the ability to cancel a job.	R2; Should / R3; Must
RD-2050	24.3.0-4.0-2	The system shall have the capability to send or log notification of fulfillment to single or multiple users.	R2; Should / R3; Must
RD-2051	24.3.0-4.0-3	The system shall have the capability to provide notification of fulfillment based on the log of activities.	R2; Should / R3; Must
RD-2052	24.3.0-4.0-4	The system shall have the capability for users to specify the methods in which they receive fulfillment notification (e.g., email, alerts).	R2; Should / R3; Must
RD-2053	24.3.0-4.0-5	The system shall have the capability for users to elect not to receive notification of fulfillment.	R2; Should / R3; Must
RD-2054	24.3.0-4.0-6	The system shall allow authorized users to manage fulfillment notification.	R2; Should / R3; Must
RD-2055	24.3.0-4.0-7	The system shall have the capability to store multiple tracking numbers for each order.	R2; Should / R3; Must
RD-2056	24.3.0-4.0-8	The system shall provide a hyperlink to a fulfillment provider tracking website.	R2; Should / R3; Must
RD-2057	24.3.0-4.0-9	The system shall have the capability to receive multiple confirmations of fulfillment.	R2; Should / R3; Must

RD-2058	25	**25 Requirements for Content Originator Ordering**	
RD-2059	25.1	***25.1 Content Originator Ordering Core Capabilities***	
RD-2060	25.1.0-1	The system shall provide a user interface for Content Originator ordering.	R1B; Must
RD-1867	25.1.0-1.0-1	The system shall have the capability to interface with select external agency systems in order to accept content.	R3; Could
RD-1868	25.1.0-1.0-2	The system shall provide the capability to write specifications for jobs	R3; Must
RD-1869	25.1.0-1.0-3	The system shall provide the capability to create common phrases used in specifications.	R3; Must
RD-1870	25.1.0-1.0-4	The system shall provide the capability to save common phrases used in specifications.	R3; Must
RD-1871	25.1.0-1.0-5	The system shall provide the capability to edit common phrases used in specifications.	R3: Must
RD-1872	25.1.0-1.0-6	The system shall provide the capability to insert common phrases into specifications.	R3; Must
RD-2061	25.1.0-2	The system shall have the capability to process jobs prior to content being approved for ingest.	R3; Must
RD-1857	25.1.0-2.0-1	Users shall have the capability to submit jobs prior to content being approved for ingest.	R1C; Must
RD-1858	25.1.0-2.0-2	Users shall have the capability to write specifications for jobs prior to content	R3; Must

		being approved for ingest.	
RD-1859	25.1.0-2.0-3	Users shall have the capability to award jobs prior to content being approved for ingest.	R3; Must
RD-1860	25.1.0-2.0-4	Users shall have the capability to send awarded jobs to service providers prior to content being approved for ingest.	R3; Must
RD-2062	25.1.0-3	The system shall have the capability to process jobs prior to content being received.	R3; Must
RD-1861	25.1.0-3.0-1	Users shall have the capability to submit jobs prior to content being received.	R1C; Must
RD-1862	25.1.0-3.0-2	Users shall have the capability to write specifications for jobs prior to content being received.	R3; Must
RD-1863	25.1.0-3.0-3	Users shall have the capability to award jobs prior to content being received.	R3; Must
RD-1864	25.1.0-3.0-4	Users shall have the capability to send awarded jobs to service providers prior to content being received.	R3; Must
RD-2063	25.1.0-4	The system shall have the capability to track jobs using the job ID.	R3; Must
RD-1865	25.1.0-4.0-1	The system shall have the capability to track job submission status using the job ID.	R1C; Must
RD-2064	25.1.0-5	The system shall have the capability to accept and store a Content Originator supplied job tracking number in metadata.	R1B; Could / R1C; Must
RD-2065	25.1.0-6	The system shall have the capability to link the Content Originator supplied job tracking number to the Job ID.	R1B; Could / R1C; Must
RD-2066	25.1.0-7	The system shall allow users to update the Content Originator supplied job tracking number at any time.	R1C; Must
RD-2067	25.1.0-8	The system shall notify authorized allow users that a Content Originator supplied job tracking number has been updated.	R1B; Could / R1C; Must
RD-2068	25.1.0-9	The system shall allow users to search job BPI.	R1C; Must
RD-1866	25.1.0-9.0-1	The system shall allow users to search job BPI related to a user account or agency.	R1C; Must
RD-2069	25.1.0-10	The system shall have the capability to interface with select external agency systems in order to retrieve jobs.	R3; Could
RD-2070	25.1.0-11	The system shall adhere to policies set forth in GPO Publication 305.3.	R3; Must

RD-2071	25.2	***25.2 Content Originator Ordering – Job Management***	
RD-2072	25.2.0-1	The system shall provide the capability to acquire, store and edit BPI data on standard forms.	R1C; Must
RD-1873	25.2.0-1.0-1	The system shall provide the capability to acquire BPI data on standard forms.	R1C; Must
RD-1874	25.2.0-1.0-2	The system shall provide the capability to store BPI data on standard forms.	R1C; Must
RD-1875	25.2.0-1.0-3	The system shall provide the capability to edit BPI data on standard forms.	R1C; Must
RD-2073	25.2.0-1.0-4	The system shall provide the capability to acquire, store and edit BPI data specific fields contained on the Standard Form 1 (SF1).	R1C; Must
RD-1876	25.2.0-1.0-4.0-1	The system shall provide the capability to acquire BPI data specific fields contained on the Standard Form 1 (SF1).	R1C; Must
RD-1877	25.2.0-1.0-4.0-2	The system shall provide the capability to store BPI data specific fields contained on the Standard Form 1 (SF1).	R1C; Must
RD-1878	25.2.0-1.0-4.0-3	The system shall provide the capability to edit BPI data specific fields contained on the Standard Form 1 (SF1).	R1C; Must
RD-2074	25.2.0-1.0-5	The system shall provide the capability to acquire, store and edit BPI data specific fields contained on the GPO Form 952.	R1C; Must
RD-1879	25.2.0-1.0-5.0-1	The system shall provide the capability to acquire BPI data specific fields contained on the GPO Form 952.	R1C; Must
RD-1880	25.2.0-1.0-5.0-2	The system shall provide the capability to store BPI data specific fields contained on the GPO Form 952.	R1C; Must
RD-1881	25.2.0-1.0-5.0-3	The system shall provide the capability to edit BPI data specific fields contained on the GPO Form 952.	R1C; Must
RD-2075	25.2.0-1.0-6	The system shall provide the capability to acquire, store and edit BPI data specific fields contained on the GPO Form 2511.	R1C; Must
RD-1882	25.2.0-1.0-6.0-1	The system shall provide the capability to acquire BPI data specific fields contained on the GPO Form 2511.	R1C; Must
RD-1883	25.2.0-1.0-6.0-2	The system shall provide the capability to store BPI data specific fields contained on the GPO Form 2511.	R1C; Must
RD-1884	25.2.0-1.0-6.0-3	The system shall provide the capability to edit BPI data specific fields	R1C; Must

		contained on the GPO Form 2511.	
RD-2076	25.2.0-1.0-7	The system shall provide the capability to acquire, store and edit BPI data specific fields contained on the GPO Form 3868.	R1C; Must
RD-1885	25.2.0-1.0-7.0-1	The system shall provide the capability to acquire BPI data specific fields contained on the GPO Form 3868.	R1C; Must
RD-1886	25.2.0-1.0-7.0-2	The system shall provide the capability to store BPI data specific fields contained on the GPO Form 3868.	R1C; Must
RD-1887	25.2.0-1.0-7.0-3	The system shall provide the capability to edit BPI data specific fields contained on the GPO Form 3868.	R1C; Must
RD-2077	25.2.0-1.0-8	The system shall allow authorized users to add new BPI fields.	R1C; Must
RD-2078	25.2.0-1.0-9	The system shall provide the capability for a Content Originator to save BPI prior to submission to GPO.	R1C; Must
RD-2080	25.2.0-3	The system shall ensure users are authorized to submit jobs.	R1C; Must
RD-2081	25.2.0-3.0-1	The system shall ensure users are authorized to spend funds.	R1C; Must
RD-2084	25.2.0-6	The system shall provide the capability for users to search all job specifications.	R3; Must
RD-2085	25.2.0-6.0-1	The system shall provide the capability for users to search job specifications related to a user account or agency.	R3; Must
RD-2086	25.2.0-7	The system shall have the capability to strap jobs.	R3; Must
RD-2087	25.2.0-7.0-1	The system shall have the capability to detect similar jobs that have not been awarded for the purpose of strapping.	R3; Could
RD-2088	25.2.0-7.0-1.0-1	The system shall have the capability to notify users of similar jobs that have not been awarded for the purpose of strapping.	R3; Could
RD-2089	25.2.0-7.0-2	The system shall have the capability to allow users to indicate that two or more jobs should be strapped.	R1C; Must
RD-2090	25.2.0-8	The system shall have the capability to inform Content Evaluators and Service Specialists that a new job has been placed by a Content Originator.	R1C; Must
RD-2091	25.2.0-8.0-1	The system shall have the capability to send jobs to appropriate Service Specialists and Content Evaluators based upon business rules.	R1C; Must
RD-2092	25.2.0-9	The system shall have the capability to support job riders.	R2; Should / R3; Must
RD-2093	25.2.0-9.0-1	The system shall have the capability for Content Evaluators to add rider information to BPI.	R1C; Must
RD-2094	25.2.0-9.0-2	The system shall have the capability to add Content Evaluator rider quantity information to the Content Originator job.	R1C; Must
RD-2095	25.2.0-9.0-3	The system shall have the capability to add Content Evaluator rider fulfillment information to the Content Originator job.	R1C; Must
RD-2096	25.2.0-9.0-4	The system shall have the capability to add Content Evaluator rider billing information to the Content Originator job.	R1C; Must
RD-2097	25.2.0-9.0-5	The system shall have the capability for users to submit rider information to GPO.	R2; Should / R3; Must
RD-2098	25.2.0-10	The system shall provide the capability to notify authorized users that riders have been placed on their job.	R2; Should / R3; Must
RD-2099	25.2.0-11	The system shall provide the capability to notify users that GPO is accepting riders for a job.	R2; Should / R3; Must
RD-2100	25.2.0-12	The system shall have the capability to determine contract types (e.g., onetime bids, SPA, term contract) based upon BPI and business rules.	R3; Could
RD-2101	25.2.0-13	The system shall allow authorized users to specify a contract type.	R1C; Must
RD-2102	25.2.0-13.0-1	The system shall provide the capability for Content Originators to specify an existing contract (e.g., SPA, Term contract).	R1C; Must
RD-2103	25.2.0-14	The system shall allow authorized users to view a history of all previous jobs based on user rights.	R1C; Must
RD-2104	25.2.0-14.0-1	The system shall allow authorized users to view a history of their previous jobs based on user rights.	R1C; Must
RD-2105	25.2.0-15	The system shall provide estimated costs for GPO products and services for jobs to users based upon user provided BPI.	R2; Should / R3; Must
RD-2106	25.2.0-15.0-1	The system shall have the capability to allow authorized users to enter an estimate when submitting a job.	R1C; Must
RD-2107	25.2.0-15.0-2	The system shall have the capability to allow Content Originators to enter an estimate when submitting a job.	R1C; Must
RD-2108	25.2.0-15.0-3	The system shall have the capability to allow Service Specialists to enter an estimate when submitting a job.	R1C; Must
RD-2109	25.2.0-15.0-4	The system shall have the capability to allow Content Originators to enter a not to exceed price when submitting a job.	R1C; Must

RD-2110	25.2.0-15.0-5	The system shall have the capability to allow authorized users to provide an estimate for a job.	R3; Must
RD-2111	25.2.0-15.0-6	The system shall have the capability for users to request a price approval.	R1C; Must
RD-2112	25.2.0-15.0-7	The system shall have the capability for users to approve/disapprove a price.	R3; Must
RD-2113	25.2.0-16	The system shall provide the capability for authorized users to edit job specifications prior to contract award.	R3; Must
RD-2114	25.2.0-16.0-1	The system shall provide the capability for authorized users to edit BPI prior to contract award.	R1C; Must
RD-2115	25.2.0-16.0-2	The system shall provide the capability for authorized users to edit BPI prior to submission to GPO.	R1C; Must
RD-2116	25.2.0-16.0-3	The system shall have the capability to display BPI edits.	R1C; Must
RD-2117	25.2.0-16.0-4	The system shall have the capability to display the user name of who edited BPI.	R1C; Must
RD-2118	25.2.0-16.0-5	The system shall have the capability to save all BPI edits.	R1C; Must
RD-2119	25.2.0-17	The system shall have the capability to notify users that BPI for a job has been edited.	R3; Must
RD-2124	25.2.0-22	The system shall allow users to select fulfillment options for content delivery.	R3; Must
RD-2125	25.2.0-22.0-1	The system shall provide the capability to configure the tangible content delivery options.	R3; Must
RD-2126	25.2.0-22.0-2	The system shall provide the capability to enter multiple fulfillment destinations.	R1C; Must
RD-2127	25.2.0-22.0-2.0-1	The system shall allow users to attach distribution list files to a job.	R1C; Must
RD-2128	25.2.0-22.0-2.0-2	The system shall compile fulfillment destination into multiple standardized formats.	R3; Must
RD-2129	25.2.0-22.0-2.0-3	The system shall be capable of extracting fulfillment destinations from attached distribution list files.	R3; Must
RD-2130	25.2.0-22.0-2.0-4	The system shall provide the capability for users to store fulfillment destinations in their user profile.	R1C; Must
RD-2135	25.2.0-22.0-2.0-5	The system shall be able to provide distribution list information to authorized users.	R3; Must
RD-2136	25.2.0-22.0-2.0-5.0-1	The system shall provide the capability for authorized users to download distribution list information.	R1C; Must
RD-2137	25.2.0-22.0-2.0-5.0-2	The system shall provide the capability for Service Providers to download distribution list information for jobs that have been awarded to them.	R3; Must
RD-2131	25.2.0-22.0-3	The system shall provide the capability for Content Originators to select ship, delivery, mail, or pickup dates.	R1C; Must
RD-2138	25.2.0-22.0-3.0-1	The system shall provide the capability for users to select zero or more mail dates for each destination in an job.	R1C; Must
RD-2132	25.2.0-22.0-3.0-2	The system shall provide the capability for users to select zero or more ship dates for each destination in an job.	R1C; Must
RD-2133	25.2.0-22.0-3.0-3	The system shall provide the capability for users to select zero or more delivery dates for each destination in an job.	R1C; Must
RD-2134	25.2.0-22.0-3.0-4	The system shall provide the capability for users to select zero or more pickup dates for each destination in an job.	R1C; Must
RD-2139	25.2.0-22.0-4	The system shall provide the capability for users to select shipping providers from a configurable list.	R3; Must
RD-2140	25.2.0-22.0-5	The system shall have the capability to provide estimated shipping costs based upon BPI.	R3; Could
RD-2141	25.2.0-22.0-6	The system shall have the capability to allow Content Originators and Service Specialists to select the method for content fulfillment.	R1C; Must
RD-2142	25.2.0-23	The system shall maintain Service Provider information.	R3; Must
RD-2143	25.2.0-23.0-1	Authorized users shall have the capability to access Service Provider information.	R3; Must
RD-2144	25.2.0-23.0-2	The system shall provide the capability for users to create Service Provider information.	R3; Must
RD-2145	25.2.0-23.0-2.0-1	The system shall provide the capability for authorized users to edit Service Provider information.	R3; Must
RD-2146	25.2.0-23.0-2.0-2	The system shall provide the capability for authorized users to delete Service Provider information.	R3; Must
RD-2147	25.2.0-23.0-2.0-3	Service Provider contact information shall include the company name.	R3; Must
RD-2148	25.2.0-23.0-2.0-4	The system shall allow users to submit feedback on Service Providers.	R3; Could
RD-2149	25.2.0-23.0-2.0-5	Service Provider contact information shall include the physical address.	R3; Must
RD-2150	25.2.0-23.0-2.0-6	Service Provider contact information shall include the mailing address.	R3; Must
RD-2151	25.2.0-23.0-2.0-7	Service Provider contact information shall include the shipping address.	R3; Must

RD-2152	25.2.0-23.0-2.0-8	Service Provider contact information shall include the names of zero or more contact personnel.	R3; Must
RD-2153	25.2.0-23.0-2.0-9	Service Provider contact information shall include zero or more phone numbers.	R3; Must
RD-2154	25.2.0-23.0-2.0-10	Service Provider contact information shall include zero or more cell phone numbers.	R3; Must
RD-2155	25.2.0-23.0-2.0-11	Service Provider contact information shall include zero or more e-mail address.	R3; Must
RD-2156	25.2.0-23.0-2.0-12	Service Provider contact information shall include zero or more fax numbers.	R3; Must
RD-2157	25.2.0-23.0-2.0-13	Service Provider contact information shall include the state code.	R3; Must
RD-2158	25.2.0-23.0-2.0-14	Service Provider contact information shall include the contractor code.	R3; Must
RD-2161	25.2.0-23.0-4	The system shall allow authorized users to manage a list of equipment categories.	R3; Must
RD-2162	25.2.0-23.0-4.0-1	Service Providers shall be able to specify the equipment categories they meet from a predefined list.	R3; Must
RD-2163	25.2.0-23.0-4.0-2	Service Providers shall be able to manage their equipment categories from a predefined list.	R3; Must
RD-2164	25.2.0-23.0-4.0-3	The system shall provide a text field for Service Providers to specify specific equipment they utilize.	R3; Must
RD-2165	25.2.0-23.0-5	Service Providers shall be able to specify products and services that they are capable of providing from a configurable list.	R3; Must
RD-2166	25.2.0-23.0-5.0-1	The system shall allow authorized users to manage a configurable list of products and services.	R3; Must
RD-2167	25.2.0-23.0-5.0-2	The system shall allow Service Providers to input customized capabilities not included on the configurable list in a note field.	R3; Must
RD-2169	25.2.0-23.0-7	The system shall maintain Service Provider performance information comprised of quality history, quality level, compliance history, and notices.	R3; Must
RD-2170	25.2.0-23.0-7.0-1	The system shall allow authorized users to manage Service Provider performance information.	R3; Must
RD-2171	25.2.0-23.0-7.0-2	Quality levels shall be assigned by authorized GPO personnel in accordance with GPO Publication 310.1.	R3; Must
RD-2172	25.2.0-23.0-7.0-3	Service Provider information shall include quality history data.	R3; Must
RD-2173	25.2.0-23.0-7.0-3.0-1	Quality history data shall include the number of jobs completed at given quality levels.	R3; Must
RD-2174	25.2.0-23.0-7.0-3.0-2	Quality history data shall include the number of jobs inspected at given quality level	R3; Must
RD-2175	25.2.0-23.0-7.0-3.0-3	Quality history data shall include the number of jobs rejected at given quality levels	R3; Must
RD-2176	25.2.0-23.0-7.0-4	Service Provider information shall include compliance history data.	R3; Must
RD-2177	25.2.0-23.0-7.0-4.0-1	Compliance history shall include the number of jobs completed.	R3; Must
RD-2178	25.2.0-23.0-7.0-4.0-2	Compliance history shall include the number of jobs completed late	R3; Must
RD-2179	25.2.0-23.0-7.0-4.0-3	Compliance history shall include the percentage of job completed late.	R3; Must
RD-2180	25.2.0-23.0-7.0-5	Service Provider information shall include notices.	R3; Must
RD-2181	25.2.0-23.0-7.0-5.0-1	Notices received shall include the number of cure notices.	R3; Must
RD-2182	25.2.0-23.0-7.0-5.0-2	Notices received shall include the number of show-cause notices.	R3; Must
RD-2183	25.2.0-23.0-7.0-5.0-3	Notices received shall include the number of shipped short letters.	R3; Must
RD-2184	25.2.0-23.0-7.0-5.0-4	Notices received shall include the number of do not condone letters.	R3; Must
RD-2185	25.2.0-23.0-7.0-5.0-5	Notices received shall include the number of terminations for default (program).	R3; Must
RD-2186	25.2.0-23.0-7.0-5.0-6	Notices received shall include the number of terminations for default (jobs).	R3; Must
RD-2187	25.2.0-23.0-7.0-5.0-7	Notices received shall include the number of erroneous information letters.	R3; Must
RD-2188	25.2.0-23.0-7.0-5.0-8	Notices received shall include the number of non-responsible quality history letters.	R3; Must
RD-2189	25.2.0-23.0-7.0-5.0-9	Notices received shall include the number of non-responsible performance letters.	R3; Must

RD-2190	25.2.0-23.0-7.0-5.0-10	Notices received shall include the number of non-responsible other letters.	R3; Must
RD-2191	25.2.0-23.0-7.0-5.0-11	Notices received shall include the number of exception clause letters	R3; Must
RD-2192	25.2.0-23.0-7.0-6	Service Provider information shall include note text field.	R3; Must
RD-2193	25.2.0-24	The system shall provide the capability to search Service Provider information.	R3; Must
RD-2194	25.2.0-25	The system shall generate a list of Service Providers in response to a user search request.	R3; Must
RD-2196	25.2.0-26	The system shall allow authorized users to generate solicitations.	R3; Must
RD-2197	25.2.0-26.0-1	The system shall distribute solicitations.	R3; Must
RD-2198	25.2.0-27	The system shall accept bids from Service Providers for jobs.	R3; Must
RD-2199	25.2.0-27.0-1	The system shall allow authorized users to submit bid information.	R3; Must
RD-2200	25.2.0-27.0-2	The system shall accept bids with zero to many line items.	R3; Must
RD-2201	25.2.0-27.0-3	The system shall be able to accept bids in the form of a quantity based upon a fixed price (e.g., Service Provider submits quantity of a bid for a fixed dollar amount, How many copies can you print for $100).	R3; Must
RD-2202	25.2.0-27.0-4	The system shall electronically stamp bids with the time it was received.	R3; Must
RD-2203	25.2.0-27.0-4.0-1	The system shall electronically stamp bids with the date it was received.	R3; Must
RD-2204	25.2.0-27.0-4.0-2	The system shall electronically stamp bids with user profile information.	R3; Must
RD-2205	25.2.0-27.0-4.0-3	The system shall allow authorized users to enter electronic stamp information when tangible bids are received.	R3; Must
RD-2206	25.2.0-27.0-5	The system shall allow authorized users to electronically post bid results.	R3; Must
RD-2207	25.2.0-28	The system shall allow Service Specialists and Content Originators to award jobs to Service Providers.	R3; Must
RD-2209	25.2.0-30	The system shall allow authorized users to request contract modifications.	R2; Should / R3; Must
RD-2210	25.2.0-31	The system shall allow authorized users to approve contract modifications.	R2; Should / R3; Must
RD-2211	25.2.0-31.0-1	The system shall allow authorized users to manage contract modifications.	R2; Should / R3; Must
RD-2213	25.2.0-33	The system shall provide the capability for users to request re-orders.	R3; Must

RD-2214	25.3	***25.3 Content Originator Ordering – Job Tracking***	
RD-2215	25.3.0-1	The system shall have the capability for a user to inform the system that they have completed an activity.	Release 1; Must
RD-2216	25.3.0-1.0-1	Activities include that the job was made available to Service Provider.	R3; Must
RD-2217	25.3.0-1.0-2	Activities include that the job was received by Service Provider.	R3; Must
RD-2218	25.3.0-1.0-3	Activities include that the proofs were sent to Content Originator	R3; Must
RD-2219	25.3.0-1.0-4	Activities include that the proofs were received by Content Originator	R3; Must
RD-2220	25.3.0-1.0-5	Activities include that the proofs were approved.	R3; Must
RD-2221	25.3.0-1.0-6	Activities include that the proofs were approved with author's alterations.	R3; Must
RD-2222	25.3.0-1.0-7	Activities include that the proofs were approved with Service Provider's errors.	R3; Must
RD-2223	25.3.0-1.0-8	Activities include that new proofs were requested due to author's alterations.	R3; Must
RD-2224	25.3.0-1.0-9	Activities include that new proofs were requested due to Service Provider's errors.	R3; Must
RD-2225	25.3.0-1.0-10	Activities include that proofs were sent to Service Provider.	R3; Must
RD-2226	25.3.0-1.0-11	Activities include that proofs were received by Service Provider.	R3; Must
RD-2227	25.3.0-1.0-12	Activities include that changes were made by Content Originator.	R3; Must
RD-2228	25.3.0-1.0-13	Activities include that changes were made by Service Provider.	R3; Must
RD-2229	25.3.0-1.0-14	Activities include that the job is complete.	R3; Must
RD-2230	25.3.0-1.0-15	Activities include that the job is delivered to each individual destination.	R3; Must
RD-2231	25.3.0-1.0-16	Activities include job shipped to all destinations.	R3; Must
RD-2232	25.3.0-1.0-17	Activities include job delivered to all destinations.	R3; Must
RD-2233	25.3.0-1.0-18	Activities include job delivery receipts are available.	R3; Must
RD-2235	25.3.0-1.0-20	Activities include Job ID referenced,	R3; Must
RD-2236	25.3.0-1.0-21	Activities include approved for publication.	R3; Must
RD-2239	25.3.0-1.0-22	The system shall provide a means to add notes to each job.	R3; Must
RD-2240	25.3.0-2	The system shall provide the capability to automatically request job status information from users.	R3; Must

RD-2242	25.3.0-2.0-2	The system shall have the capability for authorized users to request automated notifications of job activities.	R3; Must
RD-2243	25.3.0-3	The system shall allow Service Specialists to generate notifications to Service Providers and Content Originators.	R3; Must
RD-2244	25.3.0-3.0-1	The system shall allow Service Specialists to distribute notification to Service Providers and Content Originators.	R3; Must
RD-2245	25.3.0-3.0-2	Notifications include show cause notices.	R3; Must
RD-2246	25.3.0-3.0-3	Notifications include cure notices.	R3; Must
RD-2247	25.3.0-3.0-4	Notifications include GPO Form 907.	R3; Must
RD-2248	25.3.0-4	The system shall have the capability to provide shipping notification to authorized users.	R3; Must
RD-2249	25.3.0-4.0-1	The system shall have the capability to provide delivery notification to authorized users.	R3; Must
RD-2250	25.3.0-4.0-2	Notification of delivery shall include tracking numbers from the Service Provider.	R3; Must
RD-2251	25.3.0-4.0-3	Notification of delivery shall include signed delivery receipts.	R3; Must
RD-2252	25.3.0-4.0-4	The system shall have the capability to upload digitized signed delivery receipts.	R3; Must
RD-2253	25.3.0-4.0-5	Notification of delivery shall include confirmation of delivery from agency recipients.	R3; Must
RD-2254	25.3.0-4.0-6	The system shall have the capability to provide users with options in response to undelivered content (e.g., resubmit content, cancel fulfillment).	R2; Should / R3; Must
RD-2256	25.3.0-5.0-1	The system shall have the capability to receive and store product delivery tracking numbers (e.g., Fed-Ex Tracking Number) from Service Providers.	R2; Should / R3; Must
RD-2257	25.3.0-5.0-2	The system shall have the capability to receive confirmation of delivery from the agency or end user.	R2; Should / R3; Must
RD-2258	25.3.0-6	The system shall have the capability to support Job Definition Format (JDF).	R3; Could
RD-2259	25.3.0-7	The system shall provide the capability for BPI to be rendered on the GPO forms.	R1C; Must
RD-2260	25.3.0-7.0-1	The system shall provide the capability for BPI to be rendered on the GPO Standard Form 1 (SF-1).	R1C; Must
RD-2261	25.3.0-7.0-2	The system shall provide the capability for BPI to be rendered on the GPO Form 952.	R1C; Must
RD-2262	25.3.0-7.0-3	The system shall provide the capability for BPI to be rendered on the GPO Form 2511.	R1C; Must
RD-2263	25.3.0-7.0-4	The system shall provide the capability for BPI to be rendered on the GPO Form 3868.	R1C; Must
RD-2237	25.3.0-8	The system shall allow the capability for authorized users to attach files and a description of the files to a job.	R1C; Must
RD-2238	25.3.0-9	The system shall have the capability to apply a timestamp to a job upon submission.	R1C; Must

RD-2264	25.4	***25.4 Requirements for Access Content Processing***	
RD-2265	25.4.1	**25.4.1 Access Core Capabilities**	
RD-2266	25.4.1.0-1	The system shall provide open and interoperable access to content.	R1B; Must
RD-2267	25.4.1.0-2	The system shall provide open and interoperable access to metadata.	R1B; Must
RD-2268	25.4.1.0-3	The system shall provide access to content at the minimum level of granularity that is specified in the Fdsys unique ID requirements.	R1B; Must
RD-2269	25.4.1.0-4	The system shall provide the capability for users to use persistent names to access content.	R1C; Must
RD-2270	25.4.1.0-5	The system shall provide the capability for users to access content that has been published in non-English languages and non-Roman character sets.	R3; Must
RD-2271	25.4.1.0-6	The system shall provide the capability for users to access information about content relationships.	R1B; Must
RD-2272	25.4.1.0-7	The system shall provide the capability for users to access information about relationships between content packages.	R1B; Must
RD-2273	25.4.1.0-8	The system shall provide the capability for users to access information about relationships between digital objects.	R1B; Must

RD-2274	25.4.1.0-9	The system shall provide the capability for users to access information about relationships between digital objects and content packages.	R1B; Must
RD-2275	25.4.1.0-10	The system shall enforce the continuity of content in context.	R1B; Must
RD-2276	25.4.1.0-11	The system shall provide the capability to access content based on relationships between versions of a Congressional bill.	R1C; Must
RD-2277	25.4.1.0-11.0-1	The system shall provide notification to users about all bill versions available for access.	R1C; Must
RD-2278	25.4.1.0-11.0-2	The system shall provide the capability to access content based on relationships between publications that are used in the Federal legislative process.	R1C; Must
RD-2279	25.4.1.0-11.0-2.0-1	The system shall provide notification to users about related legislative publications.	R1C; Must
RD-2280	25.4.1.0-11.0-2.0-2	The system shall provide the capability to access public laws based on public law citations in the House Calendar.	R1C; Must
RD-2281	25.4.1.0-11.0-2.0-3	The system shall provide the capability to access public laws based on public law citations in the Senate Calendar of Business.	R1C; Must
RD-2282	25.4.1.0-11.0-2.0-4	The system shall provide the capability to access Congressional bills based on bill citations in the House Calendar.	R1C; Must
RD-2283	25.4.1.0-11.0-2.0-5	The system shall provide the capability to access Congressional bills based on bill citations in the Senate Calendar of Business.	R1C; Must
RD-2284	25.4.1.0-11.0-2.0-6	The system shall provide the capability to access bill versions based on entries in the history of bills.	R1C; Must
RD-2285	25.4.1.0-11.0-2.0-7	The system shall provide the capability to access Congressional Record pages based on Congressional Record citations in the history of bills.	R1C; Must
RD-2286	25.4.1.0-11.0-2.0-8	The system shall provide the capability to access Congressional bills based on bill citations in the Congressional Record.	R1C; Must
RD-2287	25.4.1.0-11.0-2.0-9	The system shall provide the capability to access public laws based on public law citations in the history of bills.	R1C; Must
RD-2288	25.4.1.0-11.0-2.0-10	The system shall provide the capability to access history of bill entries based on bill citations in public laws.	R1C; Must
RD-2289	25.4.1.0-11.0-2.0-11	The system shall provide the capability to access Congressional Record entries based on Congressional Record citations in public laws.	R1C; Must
RD-2290	25.4.1.0-11.0-2.0-12	The system shall provide the capability to access U.S. Code entries based on U.S. Code citations in public laws.	R1C; Must
RD-2291	25.4.1.0-11.0-2.0-13	The system shall provide the capability to access public laws based on public law citations in the U.S. Code.	R1C; Must
RD-2292	25.4.1.0-11.0-2.0-14	The system shall provide the capability to access Congressional Reports based on Congressional Report citations in Congressional Documents.	R1C; Must
RD-2293	25.4.1.0-11.0-2.0-15	The system shall provide to capability to access Congressional Reports from related Congressional bills.	R1C; Must
RD-2294	25.4.1.0-11.0-2.0-16	The system shall provide access to Congressional hearings related to Congressional bills.	R1C; Must
RD-2295	25.4.1.0-11.0-2.0-17	The system shall provide the capability access entities referenced in the Congressional Record Index from the Congressional Record Index.	R1C; Must
RD-2296	25.4.1.0-11.0-2.0-18	The system shall provide the capability to access Statutes at Large entries based on Statutes at Large citations in public laws.	R1C; Must
RD-2297	25.4.1.0-11.0-3	The system shall provide the capability to access content based on relationships between publications that are used in the Federal regulatory process.	R1C; Must
RD-2298	25.4.1.0-11.0-3.0-1	The system shall provide notification to users about related regulatory publications.	R1C; Must
RD-2299	25.4.1.0-11.0-3.0-2	The system shall provide the capability to access Code of Federal Regulation sections based on Code of Federal Regulation citation in the Federal Register.	R1C; Must
RD-2300	25.4.1.0-11.0-3.0-3	The system shall provide the capability to access Federal Register entries based on Federal Register citations in the List of CFR Sections Affected.	R1C; Must
RD-2301	25.4.1.0-11.0-3.0-4	The system shall provide the capability to access Code of Federal Regulation sections based on Code of Federal Regulation citations in the List of CFR Sections Affected.	R1C; Must
RD-2302	25.4.1.0-11.0-3.0-5	The system shall provide the capability to access Code of Federal Regulation sections based on Code of Federal Regulation citations in the Unified Agenda.	R1C; Must
RD-2303	25.4.1.0-11.0-4	The system shall provide the capability to access content based on relationships between Supreme Court publications that are part of the opinion process.	R1C; Must
RD-2304	25.4.1.0-11.0-4.0-	The system shall provide notification to users about related Supreme Court	R1C; Must

	1	publications that are part of the opinion process.	
RD-2305	25.4.1.0-11.0-4.0-2	The system shall provide notification to users that informs them of the current version of an opinion.	R1C; Must
RD-2306	25.4.1.0-11.0-4.0-3	The system shall provide notification to users that informs them of superceded versions of an opinion.	R1C; Must
RD-2307	25.4.1.0-11.0-4.0-4	The system shall provide notification to users when a bench opinion has been superceded by a slip opinion.	R1C; Must
RD-2308	25.4.1.0-11.0-4.0-5	The system shall provide notification to users when a slip opinion has been superceded by a preliminary print of the U.S. Reports.	R1C; Must
RD-2309	25.4.1.0-11.0-4.0-6	The system shall provide notification to users when a preliminary print of the U.S. Reports has been superceded by the Bound Volume of U.S. Reports. _	R1C; Must
RD-2310	25.4.1.0-12	The system shall provide the capability to use GPOs ILS to access metadata repositories not resident within the system.	R2; Must
RD-2311	25.4.1.0-13	The system shall provide the capability to provide access to select external repositories with which GPO has formal partnership agreements including the following:	R1C; Must
RD-2312	25.4.1.0-13.0-1	Census 200 data (U.S. Census Bureau/Case Western Reserve University): Established a Web site specifically for depository library access to Census 2000 data issued by the Census Bureau in comma-delimited ASCII format.	R1C; Must
RD-2313	25.4.1.0-13.0-2	A partnership between GPO and the Indiana University, Bloomington Libraries on behalf of the Committee on Institutional Cooperation, making publications that were distributed to Federal Depository Libraries on floppy disk available over the Internet.	R1C; Must
RD-2314	25.4.1.0-13.0-3	CyberCemetery (University of North Texas): Provide permanent online access to electronic publications of selected federal Government agencies which have ceased operation.	R1C; Must
RD-2315	25.4.1.0-13.0-4	FRASER (Federal Reserve Bank of St. Louis): Provides for public access to content in the Federal Reserve Archival System for Economic Research (FRASER) service.	R1C; Must
RD-2316	25.4.1.0-13.0-5	National Library of Medicine: Provides permanent public access to Medline, Medical Subject Headings, and NLM LocatorPlus.	R1C; Must
RD-2317	25.4.1.0-13.0-6	National Renewable Energy Laboratory: Provides permanent public access to NREL's laboratory and outreach publications.	R1C; Must
RD-2318	25.4.1.0-13.0-7	The system shall provide the capability to provide access to additional select external repositories with which GPO has formal partnership agreements.	R2; Must

RD-2319	25.4.2	**25.4.2 Access to Content Packages**	
RD-2320	25.4.2.0-1	The system shall provide the capability for GPO to manage access to content packages according to GPO business rules.	R2; Must
RD-2321	25.4.2.0-2	The system shall accept access rules for content packages.	R1C; Must
RD-2322	25.4.2.0-3	The system shall provide the capability to limit access to content with re-dissemination restrictions as specified by authorized users.	R1C; Must
RD-2323	25.4.2.0-4	The system shall provide the capability to limit access to content with limited distribution as specified by authorized users.	R1C; Must
RD-2324	25.4.2.0-5	The system shall provide the capability to limit access to Sensitive But Unclassified (SBU) content as specified by authorized users.	R1C; Must
RD-2325	25.4.2.0-6	The system shall provide the capability to limit access to copyrighted content as specified by authorized users.	R1C; Must
RD-2326	25.4.2.0-7	The system shall provide the capability to limit access to content that is out of scope for GPO's dissemination programs.	R1C; Must
RD-2327	25.4.2.0-8	The system shall provide the capability to limit access to content that has not been approved by authorized users for public release.	R1C; Must
RD-2328	25.4.2.0-9	The system shall provide the capability to limit access to embargoed content until the appropriate release date and time as specified by authorized users.	R1C; Must
RD-2329	25.4.2.0-10	The system shall provide the capability to limit access to content based on criteria specified by the Content Originator.	R1C; Must
RD-2330	25.4.2.0-10.0-1	The system shall provide the capability to limit access to content based on criteria specified by authorized users.	R1C; Must
RD-2331	25.4.2.0-11	The system shall provide access to content currently available on GPO Access.	R1C; Must
RD-2332	25.4.2.0-11.0-1	The system shall provide the capability for users to access select publications enumerated in RD-2596 (list of GPO Access applications) at a level of	R1C; Must

		granularity that is less than a publication.	
RD-2333	25.4.2.0-11.0-2	The system shall provide the capability to create persistent links to renditions of publications listed in RD-2596 (list of GPO Access applications).	R1C; Must
RD-2334	25.4.2.0-11.0-2.0-1	The system shall provide the capability to create persistent links to renditions of the Code of Federal Regulations based on natural content boundaries at a level of granularity that is less than a publication.	R1C; Must
RD-2335	25.4.2.0-11.0-2.0-2	The system shall provide the capability to create persistent links to renditions of the Federal Register based on natural content boundaries at a level of granularity that is less than a publication.	R1C; Must
RD-2336	25.4.2.0-11.0-2.0-3	The system shall provide the capability to create persistent links to renditions of the Congressional Record based on natural content boundaries at a level of granularity that is less than a publication.	R1C; Must
RD-2337	25.4.2.0-11.0-2.0-4	The system shall provide the capability to create persistent links to renditions of the Congressional Bills based on natural content boundaries at a level of granularity that is less than a publication.	R1C; Must
RD-2338	25.4.2.0-11.0-2.0-5	The system shall provide the capability to create persistent links to renditions of the United States Code based on natural content boundaries at a level of granularity that is less than a publication.	R1C; Must
RD-2339	25.4.2.0-11.0-2.0-6	The system shall provide the capability to create predictable links to renditions of publications listed in RD-2596 (list of GPO Access applications).	R1C; Must
RD-2340	25.4.2.0-11.0-2.0-7	The system shall provide the capability for internal linking of publications listed in RD-2596 (list of GPO Access applications) at all available levels of granularity.	R1C; Must
RD-2341	25.4.2.0-11.0-2.0-8	The system shall provide the capability to link Congressional bill citations in digital objects to appropriate versions of Congressional bill renditions.	R1C; Must
RD-2342	25.4.2.0-11.0-2.0-9	The system shall provide the capability to link public law citations in digital objects to appropriate versions of public law renditions.	R1C; Must
RD-2343	25.4.2.0-11.0-2.0-10	The system shall provide the capability to link United States Code citations in digital objects to appropriate versions of United States Code renditions.	R1C; Must
RD-2344	25.4.2.0-11.0-2.0-11	The system shall provide the capability to link Statutes at Large citations in digital objects to appropriate versions of Statutes at Large renditions.	R1C; Must
RD-2345	25.4.2.0-11.0-2.0-12	The system shall provide the capability to link Code of Federal Regulations citations in digital objects to appropriate versions of Code of Federal Regulations renditions.	R1C; Must
RD-2346	25.4.2.0-11.0-2.0-13	The system shall provide the capability to link Congressional Record citations in digital objects to appropriate versions of Congressional Record renditions.	R1C; Must
RD-2347	25.4.2.0-11.0-2.0-14	The system shall provide the capability to link Congressional Record page number citations in digital objects to appropriate versions of Congressional Record pages in renditions.	R1C; Must
RD-2348	25.4.2.0-11.0-2.0-15	The system shall provide the capability to link Federal Register citations in digital objects to appropriate versions of Federal Register renditions.	R1C; Must
RD-2349	25.4.2.0-11.0-2.0-16	The system shall provide the capability to link Federal Register page number citations in digital objects to appropriate versions of Federal Register pages in renditions.	R1C; Must
RD-2350	25.4.2.0-11.0-2.0-17	The system shall provide the capability to link articles listed in the Federal Register Table of Contents to articles in the appropriate versions of Federal Register renditions.	R1C; Must
RD-2351	25.4.2.0-11.0-2.0-18	The system shall provide the capability to link Bound Congressional Record citations in digital objects to appropriate versions of Bound Congressional Record renditions.	R1C; Must
RD-2352	25.4.2.0-11.0-2.0-19	The system shall provide the capability to link Congressional Hearing citations in digital objects to appropriate versions of Congressional Hearing renditions.	R1C; Must
RD-2353	25.4.2.0-11.0-2.0-20	The system shall provide the capability to link Congressional Report citations in digital objects to appropriate versions of Congressional Report renditions.	R1C; Must
RD-2354	25.4.2.0-11.0-2.0-21	The system shall provide the capability to link Congressional Document citations in digital objects to appropriate versions of Congressional Document renditions.	R1C; Must
RD-2356	25.4.2.0-11.0-2.0-23	The system shall provide the capability to link Congressional Committee Print citations in digital objects to appropriate versions of Congressional Committee Print renditions.	R1C; Must
RD-2357	25.4.2.0-11.0-2.0-24	The system shall provide the capability to manage links as managed objects.	R1C; Must
RD-2358	25.4.2.0-12	The system shall provide the capability to notify users of limitations on access to content.	R1C; Must
RD-2359	25.4.2.0-13	The system shall provide the capability to provide customized access to	R1C;

		content packages.	Should / R2; Must
RD-2360	25.4.2.0-14	The system shall provide the capability to provide personalized access to content packages.	R1C; Could / R2; Must
RD-2361	25.4.2.0-15	The system shall provide the capability for users to access in scope final published versions of ACPs.	R1B; Could / R1C; Must
RD-2362	25.4.2.0-16	The system shall provide the capability for authorized users to access final approved versions of ACPs that are not in scope for GPO's dissemination programs.	R1C; Must

RD-2363	25.4.3	**25.4.3 Access to the System**	
RD-2364	25.4.3.0-1	The system shall have the capability to provide access to system functions by user class.	R1C; Must
RD-2365	25.4.3.0-2	The system shall provide access to public End Users that does not require them to log-in or register with the system.	R1B; Must
RD-2366	25.4.3.0-2.0-1	The system shall provide access to public End Users that does not require them to log-in to the system.	R1B; Must
RD-2367	25.4.3.0-2.0-2	The system shall provide access to public End Users that does not require them to register with the system.	R1B; Must
RD-2368	25.4.3.0-3	The system shall provide the capability for authorized users to access WIP storage.	R1B; Must
RD-2369	25.4.3.0-3.0-1	The system shall have the capability to allow authorized users to authorize access to content in WIP.	R1B; Must
RD-2370	25.4.3.0-3.0-2	The system shall provide "check in and check out" capabilities for content in WIP.	R1B; Could / R1C; Must
RD-2371	25.4.3.0-3.0-2.0-1	The system shall provide check out of work in progress content	R1B; Could / R1C; Must
RD-2372	25.4.3.0-3.0-2.0-1.0-1	The system shall not allow other users to modify content when one user has checked it out	R1B; Could / R1C; Must
RD-2373	25.4.3.0-3.0-2.0-1.0-2	The system shall provide notification when content has been checked out for longer than the allowed period defined by the workflow for the work in progress	R1B; Could / R1C; Must
RD-2374	25.4.3.0-3.0-2.0-1.0-3	The system shall allow authorized users to release locks on content	R1B; Could / R1C; Must
RD-2375	25.4.3.0-3.0-3	The system shall link all versions of work in progress content	R1B; Could / R1C; Must
RD-2376	25.4.3.0-3.0-4	The system shall allow users to check in content.	R1B; Could / R1C; Must

RD-2379	25.4.4	**25.4.4 Access – User Registration**	
RD-2380	25.4.4.0-1	The system shall provide the capability for users to register with the system.	R1B; Must
RD-2381	25.4.4.0-2	The system shall provide the capability to establish a user account for each registered user.	R1B; Must
RD-2382	25.4.4.0-3	The system shall provide the capability to create user records for registered users.	R1B; Must
RD-2383	25.4.4.0-4	The system shall provide the capability to store and manage a number of user records that is only limited by available storage.	R1B; Must
RD-2384	25.4.4.0-4.0-1	The system shall have the capability to store an unlimited number of user records without software re-design.	R1B; Must
RD-2385	25.4.4.0-4.0-2	The system shall have the capability to manage an unlimited number of user records without software redesign.	R1B; Must
RD-2386	25.4.4.0-5	The system shall provide the capability for authorized users to access user records.	R1B; Must
RD-2387	25.4.4.0-6	The system shall provide the capability for authorized users to set required fields in user records.	R1C; Must
RD-2388	25.4.4.0-7	The system shall provide the capability to record information submitted by users during registration with system.	R1B; Must
RD-2389	25.4.4.0-8	The system shall provide the capability for GPO to customize what information is collected during user registration.	R2; Must
RD-2390	25.4.4.0-8.0-1	The system shall have the capability to collect name from the user during	R1C; Must

		registration (e.g., honorific title, first name, last name, job title).	
RD-2391	25.4.4.0-8.0-2	The system shall have the capability to collect contact information from the user during registration (e.g., address, city, state, zip code, country, phone number, fax number, email address).	R1C; Must
RD-2393	25.4.4.0-8.0-4	The system shall provide the capability to collect information identifying the individual as a member of a user class during registration (e.g., agency, department, office, library, depository number, company, contractor code).	R2; Must
RD-2394	25.4.4.0-8.0-4.0-1	Users may be members of multiple user classes simultaneously.	R1B; Must
RD-2395	25.4.4.0-8.0-4.0-2	The system shall associate registered users with at least one user class.	R1C; Must
RD-2396	25.4.4.0-9	The system shall provide the capability to collect role-based information from the user during registration.	R1C; Must
RD-2397	25.4.4.0-10	The system shall provide the capability to collect proof of identity information from the user during registration.	R2; Must
RD-2398	25.4.4.0-11	The system shall provide the capability to collect authority to publish information from the user during registration.	R2; Must
RD-2399	25.4.4.0-12	The system shall provide the capability to perform records management functions on user records.	R1C; Must

RD-2400	25.4.5	**25.4.5 Access – User Preferences**	
RD-2401	25.4.5.0-1	The system shall provide the capability for authorized users to manage the following user preferences:	R1C; Should / R2; Must
RD-2402	25.4.5.0-1.0-1	Preferred contact methods	R2; Must
RD-2403	25.4.5.0-1.0-2	Delivery options	R2; Must
RD-2404	25.4.5.0-1.0-3	User interfaces	
RD-2405	25.4.5.0-1.0-4	Alert services	R2; Must
RD-2406	25.4.5.0-1.0-5	Help features	R2; Must
RD-2407	25.4.5.0-1.0-6	Frequently accessed tools	R2; Must
RD-2408	25.4.5.0-1.0-7	Search preferences	R2; Must
RD-2409	25.4.5.0-1.0-8	The system shall provide the capability for authorized users to manage future user preferences.	R2; Must
RD-2410	25.4.5.0-2	The system shall provide the capability for authorized users to manage other users' preferences.	R1C; Should / R2; Must
RD-2411	25.4.5.0-3	The system shall provide the capability for GPO to establish and manage default user preferences.	R1C; Should / R2; Must
RD-2412	25.4.5.0-4	The system shall have the capability to provide recommendations for content and services based on preferences and queries of users and groups of similar users.	R1C; Could / R2; Must

RD-2415	25.4.6	**25.4.6 Access Processing**	
RD-2416	25.4.6.0-1	The system shall provide the capability to process and manage ACPs.	R1C; Must
RD-2417	25.4.6.0-1.0-1	The system shall provide the capability to process and manage digital objects that are used for access.	R1C; Must
RD-2418	25.4.6.0-1.0-2	The system shall provide the capability to manage metadata that are used for access.	R1C; Must
RD-2419	25.4.6.0-2	The system shall provide the capability to create access derivatives.	R1C; Must
RD-2422	25.4.6.0-5	The system shall provide the capability for access processing to request that an ACP be modified or created from an AIP.	R1C; Must
RD-2423	25.4.6.0-5.0-1	The system shall provide the capability for an ACP to be created from an AIP.	R1C; Must
RD-2424	25.4.6.0-5.0-2	The system shall provide the capability for an existing ACP to be modified.	R1C; Must
RD-2425	25.4.6.0-6	The system shall provide the capability for access processing to provide content and/or metadata and/or business process information to delivery processing for the purpose of fulfilling an End User request or Content Originator order.	R2; Must
RD-2426	25.4.6.0-6.0-1	The system shall provide content to delivery processing for the purpose of fulfilling an End User request.	R1C; Must
RD-2427	25.4.6.0-6.0-2	The system shall provide metadata to delivery processing for the purpose of fulfilling an End User request.	R1C; Must

RD-2428	25.4.6.0-6.0-3	The system shall provide business process information to delivery processing for the purpose of fulfilling an End User request.	R2; Must
RD-2429	25.4.6.0-6.0-4	The system shall provide content, metadata and business process information in any combination to delivery processing for the purpose of fulfilling an End User request.	R2; Must
RD-2430	25.4.6.0-6.0-5	The system shall provide content to delivery processing for the purpose of fulfilling an Content Originator order.	R2; Must
RD-2431	25.4.6.0-6.0-6	The system shall provide metadata to delivery processing for the purpose of fulfilling an Content Originator order.	R2; Must
RD-2432	25.4.6.0-6.0-7	The system shall provide business process information to delivery processing for the purpose of fulfilling a Content Originator order.	R2; Must
RD-2433	25.4.6.0-6.0-8	The system shall provide content, metadata and business process information in any combination to delivery processing for the purpose of fulfilling an Content Originator order.	R2; Must
RD-2434	25.4.6.0-7	The system shall provide the capability to perform records management functions on ACPs.	R2; Must
RD-2435	25.4.6.0-7.0-1	Records management functions shall comply with GPO and Federal records management policies.	R2; Must
RD-2436	25.4.6.0-7.0-2	Records management functions shall be performed according to records management schedules for content and metadata within the system.	R2; Must
RD-2437	25.4.6.0-8	The system shall provide the capability to identify and manage relationships between digital objects, between content packages, and between digital objects and content packages.	R2; Must
RD-2438	25.4.6.0-8.0-1	The system shall provide the capability to identify and manage relationships between digital objects based on changes in content that occur as a result of the legislative process.	R2; Must x
RD-2439	25.4.6.0-8.0-2	The system shall provide the capability to identify and manage relationships between digital objects based on changes in content that occur as a result of the regulatory process.	R2; Must

RD-2440	26	**26 Requirements for Accessibility**	
RD-2441	26.1	***26.1 Accessibility Core Capabilities***	
RD-2442	26.1.0-1	The system shall provide the capability to assess content for compliance with Section 508 technical standards.	R2; Must
RD-2443	26.1.0-1.0-1	The system shall provide the capability to assess all content for compliance with Section 508 technical standards.	R2; Must
RD-2444	26.1.0-1.0-2	The system shall provide the capability to assess content available in R1C for compliance with Section 508 technical standards.	R1C; Must
RD-2445	26.1.0-2	The system shall provide the capability to create content that is compliant with Section 508 technical standards.	R2; Must
RD-2446	26.1.0-3	The system shall provide the capability to validate content for compliance with Section 508 technical standards.	R2; Must
RD-2447	26.1.0-4	The system shall accept accessibility requirements and implementation guidance from Content Originators.	R2; Must
RD-2448	26.1.0-5	The system shall provide Section 508 compliant access to the system.	R1C; Must
RD-2449	26.1.0-6	In order to achieve compliance with Section 508 technical standards, established best practices shall be followed.	R2; Could
RD-2450	26.1.0-7	The system shall create content that contains well formed code which conforms to World Wide Web Consortium (W3C) Guidelines.	R2; Must

RD-2451	26.2	***26.2 Accessibility – Section 508 Technical Standards***	
RD-2452	26.2.0-1	Fdsys software applications and operating systems shall be Section 508 compliant according to 36 CFR Part 1194.21.	R2; Should
RD-2453	26.2.0-1.0-1	When software is designed to run on a system that has a keyboard, product functions shall be executable from a keyboard where the function itself or the result of performing a function can be discerned textually.	R2; Should

RD-2454	26.2.0-1.0-2	Applications shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards. Applications also shall not disrupt or disable activated features of any operating system that are identified as accessibility features where the application programming interface for those accessibility features has been documented by the manufacturer of the operating system and is available to the product developer.	R2; Should
RD-2455	26.2.0-1.0-3	An on-screen indication of the current focus shall be provided that moves among interactive interface elements as the input focus changes.	R2; Should
RD-2456	26.2.0-1.0-3.0-1	The focus shall be programmatically exposed so that assistive technology can track focus and focus changes.	R2; Should
RD-2457	26.2.0-1.0-4	Sufficient information about a user interface element including the identity, operation and state of the element shall be available to assistive technology. When an image represents a program element, the information conveyed by the image shall also be available in text.	R2; Should
RD-2458	26.2.0-1.0-5	When images are used to identify controls, status indicators, or other programmatic elements, the meaning assigned to those images shall be consistent throughout an application's performance.	R2; Should
RD-2459	26.2.0-1.0-6	Textual information shall be provided through operating system functions for displaying text. The minimum information that shall be made available is text content, text input caret location, and text attributes.	R2; Should
RD-2460	26.2.0-1.0-7	Applications shall not override user selected contrast and color selections and other individual display attributes.	R2; Should
RD-2461	26.2.0-1.0-8	When animation is displayed, the information shall be displayable in at least one non-animated presentation mode at the option of the user.	R2; Should
RD-2462	26.2.0-1.0-9	Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	R2; Should
RD-2463	26.2.0-1.0-10	When a product permits a user to adjust color and contrast settings, a variety of color selections capable of producing a range of contrast levels shall be provided.	R2; Should
RD-2464	26.2.0-1.0-11	Software shall not use flashing or blinking text, objects, or other elements having a flash or blink frequency greater than 2 Hz and lower than 55 Hz.	R2; Should
RD-2465	26.2.0-1.0-12	When electronic forms are used, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	R2; Should
RD-2466	26.2.0-2	Fdsys Web-based intranet and internet information and applications shall be Section 508 compliant according to 36 CFR Part 1194.22.	R2; Should
RD-2467	26.2.0-2.0-1	A text equivalent for every non-text element shall be provided (e.g., via "alt", "longdesc", or in element content).	R2; Should
RD-2468	26.2.0-2.0-2	Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.	R2; Should
RD-2469	26.2.0-2.0-3	Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.	R2; Should
RD-2470	26.2.0-2.0-4	Documents shall be organized so they are readable without requiring an associated style sheet.	R2; Should
RD-2471	26.2.0-2.0-5	Redundant text links shall be provided for each active region of a server-side image map.	R2; Should
RD-2472	26.2.0-2.0-6	Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.	R2; Should
RD-2473	26.2.0-2.0-7	Row and column headers shall be identified for data tables.	R2; Should
RD-2474	26.2.0-2.0-8	Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.	R2; Should
RD-2475	26.2.0-2.0-9	Frames shall be titled with text that facilitates frame identification and navigation.	R2; Should
RD-2476	26.2.0-2.0-10	Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	R2; Should
RD-2477	26.2.0-2.0-11	A text-only page, with equivalent information or functionality, shall be provided to make a web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes	R2; Should
RD-2478	26.2.0-2.0-12	When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified	R2; Should

		with functional text that can be read by assistive technology.	
RD-2479	26.2.0-2.0-13	When a web page requires another application be present on the client system to interpret page content the page shall provide a link to the required tool that complies with §1194.21(a) through (l).	R2; Should
RD-2480	26.2.0-2.0-13.0-1	When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page shall provide a link to a plug-in or applet that complies with §1194.21(a).	R2; Should
RD-2481	26.2.0-2.0-13.0-2	When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page shall provide a link to a plug-in or applet that complies with §1194.21(b).	R2; Should
RD-2482	26.2.0-2.0-13.0-3	When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page shall provide a link to a plug-in or applet that complies with §1194.21I.	R2; Should
RD-2483	26.2.0-2.0-13.0-4	When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page shall provide a link to a plug-in or applet that complies with §1194.21(d).	R2; Should
RD-2484	26.2.0-2.0-13.0-5	When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page shall provide a link to a plug-in or applet that complies with §1194.21(e).	R2; Should
RD-2485	26.2.0-2.0-13.0-6	When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page shall provide a link to a plug-in or applet that complies with §1194.21(f).	R2; Should
RD-2486	26.2.0-2.0-13.0-7	When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page shall provide a link to a plug-in or applet that complies with §1194.21(g).	R2; Should
RD-2487	26.2.0-2.0-13.0-8	When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page shall provide a link to a plug-in or applet that complies with §1194.21(h).	R2; Should
RD-2488	26.2.0-2.0-13.0-9	When a web page requires that an applet, plug-in or other application be present on the client system to interpret page content, the page shall provide a link to a plug-in or applet that complies with §1194.21(i).	R2; Should
RD-2489	26.2.0-2.0-14	When electronic forms are designed to be completed on-line, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.	R2; Should
RD-2490	26.2.0-2.0-15	A method shall be provided that permits users to skip repetitive navigation links.	R2; Should
RD-2491	26.2.0-2.0-16	When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.	R2; Should
RD-2492	26.2.0-3	Fdsys telecommunications products shall be Section 508 compliant according to 36 CFR Part 1194.23.	R2; Should
RD-2493	26.2.0-3.0-1	Telecommunications products or systems which provide a function allowing voice communication and which do not themselves provide a TTY functionality shall provide a standard non-acoustic connection point for TTYs. Microphones shall be capable of being turned on and off to allow the user to intermix speech with TTY use.	R2; Should
RD-2494	26.2.0-3.0-2	Telecommunications products which include voice communication functionality shall support all commonly used cross-manufacturer nonproprietary standard TTY signal protocols.	R2; Should
RD-2495	26.2.0-3.0-3	Voice mail, auto-attendant, and interactive voice response telecommunications systems shall be usable by TTY users with their TTYs.	R2; Should
RD-2496	26.2.0-3.0-4	Voice mail, messaging, auto-attendant, and interactive voice response telecommunications systems that require a response from a user within a time interval, shall give an alert when the time interval is about to run out, and shall provide sufficient time for the user to indicate more time is required.	R2; Should
RD-2497	26.2.0-3.0-5	Where provided, caller identification and similar telecommunications functions shall also be available for users of TTYs, and for users who cannot see displays.	R2; Should
RD-2498	26.2.0-3.0-6	For transmitted voice signals, telecommunications products shall provide a gain adjustable up to a minimum of 20 dB. For incremental volume control, at least one intermediate step of 12 dB of gain shall be provided.	R2; Should
RD-2499	26.2.0-3.0-7	If the telecommunications product allows a user to adjust the receive volume, a function shall be provided to automatically reset the volume to the default level after every use.	R2; Should
RD-2500	26.2.0-3.0-8	Where a telecommunications product delivers output by an audio transducer	R2; Should

		which is normally held up to the ear, a means for effective magnetic wireless coupling to hearing technologies shall be provided.	
RD-2501	26.2.0-3.0-9	Interference to hearing technologies (including hearing aids, cochlear implants, and assistive listening devices) shall be reduced to the lowest possible level that allows a user of hearing technologies to utilize the telecommunications product.	R2; Should
RD-2502	26.2.0-3.0-10	Products that transmit or conduct information or communication, shall pass through cross-manufacturer, non-proprietary, industry-standard codes, translation protocols, formats or other information necessary to provide the information or communication in a usable format. Technologies which use encoding, signal compression, format transformation, or similar techniques shall not remove information needed for access or shall restore it upon delivery.	R2; Should
RD-2503	26.2.0-3.0-10.0-1	Products that transmit or conduct information or communication, shall pass through cross-manufacturer, non-proprietary, industry-standard codes, translation protocols or formats necessary to provide the information or communication in a usable format.	R2; Should
RD-2504	26.2.0-3.0-10.0-2	Technologies which use encoding, signal compression or format transformation shall not remove information needed for access or shall restore it upon delivery.	R2; Should
RD-2505	26.2.0-3.0-11	Products which have mechanically operated controls or keys, shall comply with the following:	R2; Should
RD-2506	26.2.0-3.0-11.0-1	Controls and keys shall be tactilely discernible without activating the controls or keys.	R2; Should
RD-2507	26.2.0-3.0-11.0-2	Controls and keys shall be operable with one hand and shall not require tight grasping, pinching, or twisting of the wrist. The force required to activate controls and keys shall be 5 lbs. (22.2 N) maximum.	R2; Should
RD-2508	26.2.0-3.0-11.0-3	If key repeat is supported, the delay before repeat shall be adjustable to at least 2 seconds. Key repeat rate shall be adjustable to 2 seconds per character.	R2; Should
RD-2509	26.2.0-3.0-11.0-4	The status of all locking or toggle controls or keys shall be visually discernible, and discernible either through touch or sound.	R2; Should
RD-2510	26.2.0-4	Fdsys video and multimedia products shall be Section 508 compliant according to 36 CFR Part 1194.24	R2; Should
RD-2511	26.2.0-4.0-1	All analog television displays 13 inches and larger, and computer equipment that includes analog television receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals. As soon as practicable, but not later than July 1, 2002, widescreen digital television (DTV) displays measuring at least 7.8 inches vertically, DTV sets with conventional displays measuring at least 13 inches vertically, and standalone DTV tuners, whether or not they are marketed with display screens, and computer equipment that includes DTV receiver or display circuitry, shall be equipped with caption decoder circuitry which appropriately receives, decodes, and displays closed captions from broadcast, cable, videotape, and DVD signals.	R2; Should
RD-2512	26.2.0-4.0-1.0-1	All analog television displays 13 inches and larger shall be equipped with caption decoder circuitry which displays closed captioning.	R2; Should
RD-2513	26.2.0-4.0-1.0-2	All computer equipment that includes analog television receiver or display circuitry shall be equipped with caption decoder circuitry which displays closed captioning.	R2; Should
RD-2514	26.2.0-4.0-1.0-3	Widescreen digital television (DTV) displays measuring at least 7.8 inches vertically shall display closed captions.	R2; Should
RD-2515	26.2.0-4.0-1.0-4	DTV sets with conventional displays measuring at least 13 inches vertically shall display closed captions.	R2; Should
RD-2516	26.2.0-4.0-1.0-5	standalone DTV tuners shall display closed captions.	R2; Should
RD-2517	26.2.0-4.0-1.0-6	Computer equipment that includes DTV receiver or display circuitry shall display closed captions.	R2; Should
RD-2518	26.2.0-4.0-2	Television tuners, including tuner cards for use in computers, shall be equipped with secondary audio program playback circuitry.	R2; Should
RD-2519	26.2.0-4.0-3	All training and informational video and multimedia productions which support the agency's mission, regardless of format, that contain speech or other audio information necessary for the comprehension of the content, shall be open or closed captioned.	R2; Should
RD-2520	26.2.0-4.0-4	All training and informational video and multimedia productions which support	R2; Should

		the agency's mission, regardless of format, that contain visual information necessary for the comprehension of the content, shall be audio described.	
RD-2521	26.2.0-4.0-5	Display or presentation of alternate text presentation or audio descriptions shall be user-selectable unless permanent.	R2; Should
RD-2522	26.2.0-5	Fdsys self contained, closed products shall be Section 508 compliant according to 36 CFR Part 1194.25	R2; Should
RD-2523	26.2.0-5.0-1	Self contained products shall be usable by people with disabilities without requiring an end-user to attach assistive technology to the product. Personal headsets for private listening are not assistive technology.	R2; Should
RD-2524	26.2.0-5.0-2	When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.	R2; Should
RD-2525	26.2.0-5.0-3	Where a product utilizes touch screens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (1) through (4).	R2; Should
RD-2526	26.2.0-5.0-3.0-1	Where a product utilizes touch screens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (1).	R2; Should
RD-2527	26.2.0-5.0-3.0-2	Where a product utilizes touch screens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (2).	R2; Should
RD-2528	26.2.0-5.0-3.0-3	Where a product utilizes touch screens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (3).	R2; Should
RD-2529	26.2.0-5.0-3.0-4	Where a product utilizes touch screens or contact-sensitive controls, an input method shall be provided that complies with §1194.23 (k) (4).	R2; Should
RD-2530	26.2.0-5.0-4	When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.	R2; Should
RD-2531	26.2.0-5.0-5	When products provide auditory output, the audio signal shall be provided at a standard signal level through an industry standard connector that will allow for private listening. The product shall provide the ability to interrupt, pause, and restart the audio at anytime.	R2; Should
RD-2532	26.2.0-5.0-6	When products deliver voice output in a public area, incremental volume control shall be provided with output amplification up to a level of at least 65 dB. Where the ambient noise level of the environment is above 45 dB, a volume gain of at least 20 dB above the ambient level shall be user selectable. A function shall be provided to automatically reset the volume to the default level after every use.	R2; Should
RD-2533	26.2.0-5.0-7	Color coding shall not be used as the only means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.	R2; Should
RD-2534	26.2.0-5.0-8	When a product permits a user to adjust color and contrast settings, a range of color selections capable of producing a variety of contrast levels shall be provided.	R2; Should
RD-2535	26.2.0-5.0-9	Products shall be designed to avoid causing the screen to flicker with a frequency greater than 2 Hz and lower than 55 Hz.	R2; Should
RD-2536	26.2.0-5.0-10	Products which are freestanding, non-portable, and intended to be used in one location and which have operable controls shall comply with the following:	R2; Should
RD-2537	26.2.0-5.0-10.0-1	The position of any operable control shall be determined with respect to a vertical plane, which is 48 inches in length, centered on the operable control, and at the maximum protrusion of the product within the 48 inch length.	R2; Should
RD-2538	26.2.0-5.0-10.0-2	Where any operable control is 10 inches or less behind the reference plane, the height shall be 54 inches maximum and 15 inches minimum above the floor.	R2; Should
RD-2539	26.2.0-5.0-10.0-3	Where any operable control is more than 10 inches and not more than 24 inches behind the reference plane, the height shall be 46 inches maximum and 15 inches minimum above the floor.	R2; Should
RD-2540	26.2.0-5.0-10.0-4	Operable controls shall not be more than 24 inches behind the reference plane	R2; Should
RD-2541	26.2.0-6	Fdsys desktop and portable computer products shall be Section 508 compliant according to 36 CFR Part 1194.26.	R2; Should
RD-2542	26.2.0-6.0-1	All mechanically operated controls and keys shall comply with §1194.23 (k) (1) through (4).	R2; Should
RD-2543	26.2.0-6.0-1.0-1	All mechanically operated controls and keys shall comply with §1194.23 (k) (1).	R2; Should
RD-2544	26.2.0-6.0-1.0-2	All mechanically operated controls and keys shall comply with §1194.23 (k) (2).	R2; Should
RD-2545	26.2.0-6.0-1.0-3	All mechanically operated controls and keys shall comply with §1194.23 (k) (3).	R2; Should
RD-2546	26.2.0-6.0-1.0-4	All mechanically operated controls and keys shall comply with §1194.23 (k)	R2; Should

		(4).	
RD-2547	26.2.0-6.0-2	If a product touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (1) through (4).	R2; Should
RD-2548	26.2.0-6.0-2.0-1	If a product utilizes touch screens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (1).	R2; Should
RD-2549	26.2.0-6.0-2.0-2	If a product utilizes touch screens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (2).	R2; Should
RD-2550	26.2.0-6.0-2.0-3	If a product utilizes touch screens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (3).	R2; Should
RD-2551	26.2.0-6.0-2.0-4	If a product utilizes touch screens or touch-operated controls, an input method shall be provided that complies with §1194.23 (k) (4).	R2; Should
RD-2552	26.2.0-6.0-3	When biometric forms of user identification or control are used, an alternative form of identification or activation, which does not require the user to possess particular biological characteristics, shall also be provided.	R2; Should
RD-2553	26.2.0-6.0-4	Where provided, at least one of each type of expansion slots, ports and connectors shall comply with publicly available industry standards.	R2; Should
RD-2554	27	**27 Requirements for Search**	
RD-2555	27.1	***27.1 Search Core Capabilities***	
RD-2556	27.1.0-1	The system shall provide the capability to search for and retrieve content from the system.	R1B; Must
RD-2557	27.1.0-2	The system shall provide the capability to search for and retrieve metadata from the system.	R1B; Must
RD-2558	27.1.0-3	The system shall provide the capability to search across multiple internal content and metadata repositories simultaneously and separately.	R1C; Must
RD-2559	27.1.0-3.0-1	The system shall provide the capability to search across multiple internal content and metadata collections simultaneously.	R1C; Must
RD-2560	27.1.0-3.0-2	The system shall provide the capability to search internal content and metadata collections separately.	R1C; Must
RD-2561	27.1.0-4	The system shall provide the capability to search content that is currently available on the GPO Access public Web site.	R1C; Must
RD-2562	27.1.0-5	The system shall provide the capability to search cataloging records in order to provide access to select external repositories with which GPO has formal partnership agreements as specified in requirement RD-2311 and its sub requirements.	R2; Must
RD-2563	27.1.0-6	The system shall provide the capability to search and retrieve unstructured content (e.g., text).	R1C; Must
RD-2564	27.1.0-7	The system shall provide the capability to match character strings (e.g., search exact phrases).	R1B; Must
RD-2565	27.1.0-8	The system shall provide the capability to search and retrieve semi-structured content (e.g., inline markup).	R1C; Must
RD-2566	27.1.0-9	The system shall provide the capability to search and retrieve structured content (e.g., fielded).	R1B; Must
RD-2567	27.1.0-10	The system shall provide the capability to search for content by means of querying metadata.	R1B; Must
RD-2568	27.1.0-11	The system shall provide the capability for users to search collections based on user class, user role, and access rights.	R1C; Must
RD-2569	27.1.0-11.0-1	The system shall provide the capability for users to search collections based on user role.	R1C; Must
RD-2570	27.1.0-11.0-2	The system shall provide the capability for users to search collections based on access rights.	R1C; Must
RD-2571	27.1.0-12	The system shall provide the capability to return content packages in any form simultaneously or separately.	R1C; Must
RD-2572	27.1.0-12.0-1	The system shall provide the capability to search for digital objects.	R1C; Must
RD-2573	27.1.0-12.0-2	The system shall provide the capability to search for only work in progress content.	R1C; Must
RD-2574	27.1.0-12.0-3	The system shall provide the capability to search for work in progress content simultaneously with other content.	R1C; Must
RD-2575	27.1.0-12.0-4	The system shall provide the capability to search for only SIPs.	R1C; Must
RD-2576	27.1.0-12.0-5	The system shall provide the capability to search for SIPs simultaneously with	R1C; Must

		other content.	
RD-2577	27.1.0-12.0-6	The system shall provide the capability to search for only AIPs.	R1C; Must
RD-2578	27.1.0-12.0-7	The system shall provide the capability to search for AIPs simultaneously with other content.	R1C; Must
RD-2579	27.1.0-12.0-8	The system shall provide the capability to search for only ACPs.	R1C; Must
RD-2580	27.1.0-12.0-9	The system shall provide the capability to search for ACPs simultaneously with other content.	R1C; Must
RD-2581	27.1.0-13	The system shall provide the capability to ingest PDF files containing "post-it" note comments.	R1C; Must
RD-2582	27.1.0-14	The system shall provide the capability to maintain "post-it" note comments on ingested PDF files as the files are processed through the system.	R1C; Must
RD-2583	27.1.0-15	The system shall provide the capability to maintain PDF features (e.g. bookmarks, comments, links, thumbnails) when PDF files go through a segmentation process.	R1C; Must
RD-2584	27.1.0-16	The system shall provide the capability to maintain PDF features (e.g. bookmarks, comments, links, thumbnails) when PDF files go through a parsing process.	R1C; Must
RD-2585	27.1.0-17	The system shall provide the capability to maintain PDF features (e.g. bookmarks, comments, links, thumbnails) when individual PDF files are combined into a single PDF file.	R1C; Must
RD-2586	27.1.0-18	The system shall provide the capability to index content within a PDF "post-it" note comment.	R1C; Must
RD-2587	27.1.0-19	The system shall provide the capability to deliver PDF files that contain "post-it" note comments.	R1C; Must

RD-2588	27.2	***27.2 Search – Query***	
RD-2589	27.2.0-1	The system shall provide the capability for users to select content collections to search.	R1B; Must
RD-2590	27.2.0-2	The system shall provide the capability to apply business rules to user queries so that content is searched based on query (e.g., intelligent search).	R1B; Should / 1C; Should / R2; Must
RD-2591	27.2.0-3	The system shall provide the capability for users to select search complexity levels (e.g., simple search, advanced/fielded search).	R1B; Must
RD-2592	27.2.0-3.0-1	The system shall allow a simple search, which allows the user to input a search term to search across one or multiple content collections.	R1B; Must
RD-2593	27.2.0-3.0-2	The system shall allow an advanced/fielded search, which allows the user to input multiple fields to filter both content and metadata in addition to the search term.	R1C; Must
RD-2594	27.2.0-4	The system shall allow searching on any number of collections of content.	R1C; Must
RD-2595	27.2.0-4.0-1	The system shall allow users to search any collection based on the metadata associated with that collection.	R1C; Must
RD-2596	27.2.0-4.0-2	The system shall allow users to search collections currently available on GPO Access including the following:	R1C; Must
RD-2597	27.2.0-4.0-2.0-1	Public and Private Laws	R1C; Must
RD-2598	27.2.0-4.0-2.0-2	Congressional Reports including House, Senate, and Senate Executive Reports.	R1C; Must
RD-2599	27.2.0-4.0-2.0-3	Congressional Documents including House Documents, Senate Documents, Senate Executive Documents, and Senate Treaty Documents.	R1C; Must
RD-2600	27.2.0-4.0-2.0-4	Congressional Bills	R1C; Must
RD-2601	27.2.0-4.0-2.0-5	Federal Register	R1C; Must
RD-2602	27.2.0-4.0-2.0-6	History of Bills	R1C; Must
RD-2603	27.2.0-4.0-2.0-7	Congressional Record	R1C; Must
RD-2604	27.2.0-4.0-2.0-8	Congressional Record Index	R1C; Must
RD-2605	27.2.0-4.0-2.0-9	United States Code	R1C; Must
RD-2606	27.2.0-4.0-2.0-10	Code of Federal Regulations	R1C; Must
RD-2607	27.2.0-4.0-2.0-11	List of Sections Affected (LSA)	R1C; Must
RD-2608	27.2.0-4.0-2.0-12	Congressional Hearings (including House and Senate Appropriations Hearings)	R1C; Must
RD-2609	27.2.0-4.0-2.0-13	Congressional Committee Prints	R1C; Must
RD-2610	27.2.0-4.0-2.0-14	Congressional Calendars (including House, Senate, and Committee)	R1C; Must
RD-2611	27.2.0-4.0-2.0-15	Weekly Compilation of Presidential Documents	R1C; Must

RD-2612	27.2.0-4.0-2.0-16	Budget of the United States Government	R1C; Must
RD-2613	27.2.0-4.0-2.0-17	Congressional Record (Bound)	R1C; Must
RD-2614	27.2.0-4.0-2.0-18	House Journal	R1C; Must
RD-2615	27.2.0-4.0-2.0-19	Semiannual regulatory Agenda (Unified Agenda)	R1C; Must
RD-2616	27.2.0-4.0-2.0-20	U.S. Constitution Analysis and Interpretation	R1C; Must
RD-2617	27.2.0-4.0-2.0-21	Economic Indicators	R1C; Must
RD-2618	27.2.0-4.0-2.0-22	Economic Report of the President	R1C; Must
RD-2619	27.2.0-4.0-2.0-23	Congressional Directory	R1C; Must
RD-2620	27.2.0-4.0-2.0-24	U.S. Government Manual	R1C; Must
RD-2621	27.2.0-4.0-2.0-25	Public Papers of the President of the United States	R1C; Must
RD-2622	27.2.0-4.0-2.0-26	House Ways and Means Committee Prints	R1C; Must
RD-2623	27.2.0-4.0-2.0-27	GAO Comptroller General Decisions	R1C; Must
RD-2624	27.2.0-4.0-2.0-28	GAO Reports	R1C; Must
RD-2625	27.2.0-4.0-2.0-29	House Practice	R1C; Must
RD-2626	27.2.0-4.0-2.0-30	Senate Manual	R1C; Must
RD-2627	27.2.0-4.0-2.0-31	House Rules and Manual	R1C; Must
RD-2628	27.2.0-4.0-2.0-32	Privacy Act Issuances	R1C; Must
RD-2629	27.2.0-4.0-2.0-33	Department of Interior Inspector General Reports	R1C; Must
RD-2630	27.2.0-4.0-2.0-34	U.S. Government Printing Office Style Manual	R1C; Must
RD-2631	27.2.0-4.0-2.0-35	Cannon's Precedents of the U.S. House of Representatives	R1C; Must
RD-2632	27.2.0-4.0-2.0-36	Hinds' Precedents of the House of Representatives	R1C; Must
RD-2633	27.2.0-4.0-2.0-37	Independent Counsel's Reports	R1C; Must
RD-2634	27.2.0-4.0-2.0-38	Government Information Locator Service Records (GILS)	R1C; Must
RD-2636	27.2.0-4.0-2.0-39	Davis-Bacon Wage Determinations	R1C; Must
RD-2637	27.2.0-4.0-2.0-40	Commerce Business Daily	R1C; Must
RD-2638	27.2.0-4.0-2.0-41	Congressional Publications (including Miscellaneous House and Senate Publications)	R1C; Must
RD-2639	27.2.0-4.0-2.0-42	Statutes at Large	R1C; Must
RD-2640	27.2.0-4.0-2.0-43	Deschler's Precedents of the U.S. House of Representatives	R1C; Must
RD-2641	27.2.0-4.0-2.0-44	eCFR (Electronic Code of Federal Regulations)	R1C; Must
RD-2642	27.2.0-4.0-2.0-45	Background Material and Data on Programs within the Jurisdiction of the Committee on Ways and Means (Green Book)	R1C; Must
RD-2643	27.2.0-4.0-2.0-46	Conference Reports	R1C; Must
RD-2644	27.2.0-4.0-2.0-47	Education Reports from ERIC	R1C; Must
RD-2645	27.2.0-4.0-2.0-48	History of Line Item Veto Notices, Prior to Supreme Court Opinion No. 97-1374	R1C; Must
RD-2646	27.2.0-4.0-2.0-49	Overview and Compilation of U.S. Trade Statutes (Blue Book)	R1C; Must
RD-2647	27.2.0-4.0-2.0-50	Riddick's Senate Procedures	R1C; Must
RD-2648	27.2.0-4.0-2.0-51	United States Government Policy and Support Positions (Plum Book)	R1C; Must
RD-2649	27.2.0-4.0-2.0-52	Citizens Guide to the Federal Budget	R1C; Must
RD-2650	27.2.0-4.0-2.0-53	Challenger Space Shuttle Accident Selected Congressional Hearings and Reports	R1C; Must
RD-2651	27.2.0-4.0-2.0-54	Comprehensive Revised Report with Addendums on Iraq's Weapons of Mass Destruction (Duelfur Report)	R1C; Must
RD-2652	27.2.0-4.0-2.0-55	Final Report of the National Commission on Terrorist Attacks Upon the United States, Official Government Edition (9/11 Report)	R1C; Must
RD-2653	27.2.0-4.0-2.0-56	Report of the Select Committee on Intelligence U.S. Intelligence Community's Pre-was Assessments on Iraq	R1C; Must
RD-2654	27.2.0-4.0-2.0-57	State of New York, ex rel. Eliot Spitzer, et al. v. Microsoft	R1C; Must
RD-2655	27.2.0-4.0-2.0-58	Export Administration Regulations	R1C; Must
RD-2656	27.2.0-4.0-2.0-59	Bureau of Land Management Publications	R1C; Must
RD-2657	27.2.0-4.0-2.0-60	State of Union Addresses	R1C; Must
RD-2658	27.2.0-4.0-2.0-61	National Labor Relations Board Publications	R1C; Must
RD-2659	27.2.0-4.0-2.0-62	Federal Bulletin Board	R1C; Must
RD-2660	27.2.0-4.0-2.0-63	In-scope publications on GPO's Permanent Server	R1C; Must
RD-2661	27.2.0-4.0-2.0-64	In-scope publications on GPO's Web Servers	R1C; Must
RD-2662	27.2.0-4.0-2.0-65	200 Notable Days: Senate Stories, 1787 to 2002	R1C; Must
RD-2663	27.2.0-4.0-2.0-66	Unclassified Version of the Report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction	R1C; Must
RD-2664	27.2.0-4.0-2.0-67	Supreme Court Nomination Hearings	R1C; Must
RD-2665	27.2.0-4.0-2.0-68	Supreme Court Decisions 1937-1975	R1C; Must
RD-2666	27.2.0-4.0-2.0-69	Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001	R1C; Must

RD-2667	27.2.0-4.0-2.0-70	Featured House Documents	R1C; Must
RD-2668	27.2.0-4.0-2.0-71	Featured Senate Documents	R1C; Must
RD-2669	27.2.0-4.0-2.0-72	Congressional Serial Set	R1C; Must
RD-2670	27.2.0-4.0-2.0-73	Congressional Committee Materials	R1C; Must
RD-2672	27.2.0-6	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).	R1C; Must
RD-2673	27.2.0-6.0-1	The system shall allow authorized users to manage concept relationships.	R1C; Must
RD-2674	27.2.0-6.0-1.0-1	The system shall allow authorized users to add concept relationships.	R1C; Must
RD-2675	27.2.0-6.0-1.0-2	The system shall allow authorized users to delete concept relationships.	R1C; Must
RD-2676	27.2.0-6.0-1.0-3	The system shall allow authorized users to modify concept relationships.	R1C; Must
RD-2677	27.2.0-6.0-1.0-4	The system shall suggest new concept relationships based on ingested content.	R1C; Must
RD-2678	27.2.0-6.0-1.0-4.0-1	The system shall automatically create new concept relationships based on an authorized users acceptance of suggested new concept relationships	R1C; Must
RD-2679	27.2.0-6.0-1.0-5	The system shall use new concepts without requiring previously indexed content is reindexed.	R1C; Must
RD-2682	27.2.0-7	The system shall support standard Boolean search language.	R1C; Must
RD-2683	27.2.0-7.0-1	The system shall support full Boolean operators, including AND, OR, NOT, BEFORE, NEAR, and ADJACENT.	R1B; Must
RD-2684	27.2.0-7.0-2	The system shall support implied Boolean operators, including "+" and "-".	R1C; Must
RD-2685	27.2.0-7.0-3	The system shall support the nesting of Boolean operators via parentheses.	R1C; Must
RD-2686	27.2.0-7.0-4	No user shall be required to enter case sensitive operators.	R1B; Must
RD-2687	27.2.0-8	The system shall allow users to perform a natural language search.	R1C; Must
RD-2688	27.2.0-9	The system shall support a customizable list of stop words.	R1C; Must
RD-2689	27.2.0-9.0-1	The system shall support a customizable list of idioms.	R1C; Must
RD-2690	27.2.0-10	The system shall allow for stemming of search terms.	R1C; Must
RD-2691	27.2.0-10.0-1	The system shall allow for left side stemming.	R1C; Should
RD-2692	27.2.0-10.0-2	The system shall allow for right side stemming.	R1C; Must
RD-2693	27.2.0-11	The system shall allow users to use wildcard characters to replace characters within words.	R1B; Must
RD-2694	27.2.0-12	The system shall support proximity searching.	R1C; Must
RD-2695	27.2.0-13	The system shall support synonyms searching.	R1C; Must
RD-2696	27.2.0-14	The system shall provide the capability for contextual searching.	R1C; Could
RD-2697	27.2.0-15	The system shall conform to ISO 239.50.	R1C; Must
RD-2699	27.2.0-17	The system shall have a documented interface (e.g., API) to allow search by non-GPO systems.	R1C; Must
RD-2701	27.2.0-19	The system shall allow users to select specified search functionality.	R1B; Must
RD-2702	27.2.0-20	The system shall support queries of variable lengths.	R1B; Must
RD-2703	27.2.0-21	The system shall have the ability to limit search query length.	R1C; Must
RD-2704	27.2.0-22	The system shall provide the capability to weight search terms (e.g., term must appear, term must not appear, term is part of an exact phrase).	R1C; Must

RD-2705	27.3	***27.3 Search – Refine***	
RD-2706	27.3.0-1	The system shall provide the capability for users to modify previous search queries to enable execution of subsequent searches.	R1C; Must
RD-2707	27.3.0-1.0-1	The system shall provide the capability to direct subsequent queries against different content collections.	R2; Must
RD-2708	27.3.0-1.0-2	The system shall provide the capability for users to retain selected targets from a result set and modify said query to be rerun against the result.	R2; Must
RD-2709	27.3.0-2	The system shall provide the capability to display a list of terms that are conceptually related to the original search term.	R2; Must
RD-2710	27.3.0-2.0-1	The system shall provide users with the ability to directly execute a search from conceptually related terms.	R1C; Must
RD-2711	27.3.0-3	The system shall be able to recognize alternate spellings of terms.	R1C; Must
RD-2712	27.3.0-3.0-1	The system shall suggest corrected spellings of terms.	R2; Must

RD-2713	27.4	***27.4 Search – Results***	
RD-2714	27.4.0-1	The system shall have the capability to take users to the exact occurrence of	R1C; Must

		the search term or its conceptual equivalent in a result.	
RD-2715	27.4.0-2	The system shall allow a user to navigate the levels of granularity applied to a result from within that result.	R1C; Must
RD-2716	27.4.0-3	The system shall provide the capability for users to bookmark individual search results.	R1C; Must
RD-2717	27.4.0-4	The system shall provide search results to users.	R1B; Must
RD-2718	27.4.0-5	The system shall provide the capability to group versions, renditions, and formats into one entry in a search results list.	R1B; Should / R1C; Must
RD-2719	27.4.0-6	The system shall provide the capability to sort results lists on displayable attributes in the result set.	R1C; Must
RD-2720	27.4.0-7	The system shall provide the capability to categorize results.	R1C; Must
RD-2721	27.4.0-8	The system shall provide the capability to cluster results.	R1C; Should
RD-2722	27.4.0-9	The system shall provide the capability to analyze results.	R2; Could
RD-2723	27.4.0-10	The system shall provide the capability to display results graphically.	R2; Could
RD-2724	27.4.0-11	The system shall provide the capability to apply one or multiple taxonomies.	R1C; Must
RD-2725	27.4.0-12	The system shall provide the capability for users to limit the number of results displayed.	R1C; Must
RD-2726	27.4.0-13	The system shall provide the capability to display the total number of results in the result set returned by the search.	R2; Must
RD-2727	27.4.0-13.0-1	The system shall allow the user to select the number of results in a result set from available options.	R2; Must
RD-2728	27.4.0-13.0-2	The system shall allow a result set equal to the size of all records in all indexes.	R2; Must
RD-2729	27.4.0-14	The system shall allow authorized users to select which metadata attributes are viewable for each collection.	R1B; Must
RD-2732	27.4.0-17	The system shall provide the capability to highlight query terms.	R1C; Could / R2; Must
RD-2733	27.4.0-17.0-1	The system shall provide the capability to highlight query terms in the document.	R1C; Could / R2; Must
RD-2734	27.4.0-17.0-2	The system shall provide the capability to highlight query terms in the document abstract or document summary that appears results list.	R1C; Could / R2; Must
RD-2735	27.4.0-18	The system shall provide feedback to the user in the event of an error.	R1B; Must
RD-2736	27.4.0-19	The system shall provide the capability to display inline image thumbnails of content in a results list.	R2; Must
RD-2737	27.4.0-20	The system shall allow users to save search results individually or as a batch (e.g., without selecting each result individually) for export.	R1B; Should / R1C; Must
RD-2738	27.4.0-21	The system shall provide the capability to return search results at the lowest level of granularity supported by the content package.	R1C; Must
RD-2739	27.4.0-22	The system shall provide the capability for authorized users to modify relevancy ranking factors.	R1B; Should / R1C; Must
RD-2740	27.4.0-23	The system shall provide the capability to filter search results.	R1C; Must
RD-2741	27.4.0-23.0-1	The system shall provide the capability for users to return to their original search results after results have been filtered.	R1C; Must
RD-2742	27.4.0-23.0-2	The system shall provide the capability for authorized users to define search filters.	R1C; Must

RD-2743	27.5	## *27.5 Saved Searches*	
RD-2744	27.5.0-1	The system shall allow users with an established user account and profile to enter or store queries, preferences, and results sets or portions of results sets.	R1C; Should / R2; Must
RD-2745	27.5.0-1.0-1	The system shall allow users with an established user account and profile to enter or store and recall queries.	R2; Must
RD-2746	27.5.0-1.0-2	The system shall allow users with an established user account and profile to enter or store and recall preferences.	R2; Must
RD-2747	27.5.0-1.0-3	The system shall allow users with an established user account and profile to	R2; Must

		enter or store and recall results sets as a whole.	
RD-2748	27.5.0-1.0-4	The system shall allow users with an established user account and profile to enter or store and recall portions of results sets.	R2; Must
RD-2749	27.5.0-2	The system shall provide the capability to automatically execute saved searches on a schedule defined by the user.	R1C; Should / R2; Must
RD-2750	27.5.0-3	The system shall provide the capability to notify users when automatically executed searches return results that were not included in the original search.	R1C; Should / R2; Must

RD-2751	27.6	***27.6 Search Interface***	
RD-2752	27.6.0-1	The system shall provide a search interface that allows users to submit queries to the system and receive results.	R1B; Must
RD-2754	27.6.0-3	The system shall provide the capability to have customizable search interfaces based on user preferences.	R1B; Should / R1C; Must
RD-2755	27.6.0-4	The system shall provide the capability to have navigational elements to allow users to navigate through results.	R1B; Must
RD-2756	27.6.0-5	Deleted.	

RD-2757	27.7	***27.7 Search Administration***	
RD-2758	27.7.0-1	The system shall provide the capability to manage an unlimited number of collections.	R1B; Must
RD-2759	27.7.0-2	The system shall provide a Web-based administrator graphical user interface (GUI).	R1B; Must
RD-2761	27.7.0-4	The system shall provide for the control of search run times, including the ability to preempt runtimes by an administrator-defined limit.	R2; Must
RD-2762	27.7.0-5	The system shall provide the capability to support user search while other system functions are being performed (e.g., re-indexing databases, updating content).	R1B; Must
RD-2763	27.7.0-6	The system shall provide the capability to log search activities.	R1B; Must

RD-2764	28	**28 Requirements for Request**	
RD-2765	28.1	***28.1 Request Core Capabilities***	
RD-2766	28.1.0-1	The system shall provide the capability for users to request delivery of content.	R1B; Must
RD-2767	28.1.0-2	The system shall provide the capability for users to request delivery of metadata.	R1C; Must

RD-2769	28.2	***28.2 No Fee Requests***	
RD-2770	28.2.0-1	The system shall provide the capability for End Users to request no-fee content delivery.	R1B; Must
RD-2771	28.2.0-1.0-1	The system shall not restrict or otherwise diminish access to items that are currently available through GPO Access.	R1C; Must
RD-2772	28.2.0-1.0-2	The system shall provide the capability for users to print and download information currently available through GPO Access.	R1C; Must
RD-2773	28.2.0-1.0-2.0-1	The system shall maintain printing functionality currently available within GPO Access content collections.	R1C; Must
RD-2774	28.2.0-1.0-2.0-2	The system shall maintain downloading functionality currently available within GPO Access content collections.	R1C; Must
RD-2775	28.2.0-2	The system shall provide the capability for Federal Depository Library End Users to select and request content and metadata for delivery to their library	R2; Must

		based on their unique profile and preferences.	
RD-2776	28.2.0-3	The system shall comply with GPO policies related to selection of tangible and electronic titles by Federal Depository Library End Users.	R2; Must
RD-2777	28.2.0-4	The system shall provide the capability to interface with Authorized Representatives designated by GPOs Library Services and Content Management business unit for processing of no-fee delivery requests.	R2; Must
RD-2778	28.2.0-5	The system shall provide the capability to interface with GPO's Integrated Library System and other legacy systems as defined by GPO business units for processing of no-fee requests.	R2; Must
RD-2779	28.2.0-6	The system shall provide the capability to process no-fee requests for delivery of content with access restrictions.	R2; Must
RD-2780	28.2.0-7	The system shall support the delivery of serials and periodicals.	R2; Must
RD-2781	28.2.0-8	The system shall provide the capability for users to cancel full or partial requests prior to fulfillment.	R1C; Must
RD-2782	28.2.0-8.0-1	The system shall provide the capability for users to cancel full requests prior to fulfillment.	R1C; Must
RD-2783	28.2.0-8.0-2	The system shall provide the capability for users to cancel partial requests prior to fulfillment.	R1C; Must
RD-2784	28.2.0-9	The system shall provide the capability to deliver personalized offers to registered users based on user request history or users with similar request histories. (e.g. "you may also be interested in…").	R1C; Could / R2; Must
RD-2785	28.2.0-9.0-1	The system shall provide the capability for users to opt-out of personalized offers.	R1C; Could / R2; Must
RD-2786	28.2.0-10	The system shall provide the capability to provide authorized users with a detailed transaction summary.	R1C; Should / R2; Must
RD-2788	28.2.0-12	The system shall provide the capability to generate reports for no-fee transactions.	R1C; Must

RD-2789	28.3	***28.3 Fee-based Requests***	
RD-2790	28.3.0-1	The system shall provide the capability for users to request fee-based content delivery.	R2; Must
RD-2791	28.3.0-2	The system shall have the capability to interface with external Athorized Representatives as designated by GPO's Publication and Information Sales business unit for processing of fee-based delivery requests.	R2; Must
RD-2792	28.3.0-3	The system shall provide the capability to interface with GPO's financial and inventory systems for processing of fee-based requests.	R2; Must
RD-2793	28.3.0-4	The system shall have the capability to retrieve price information from external systems.	R2; Must
RD-2794	28.3.0-5	The system shall have the capability to adjust price information for fee-based content delivery.	R2; Must
RD-2795	28.3.0-5.0-1	Pricing structures shall comply with GPO's legislative mandates under Title 44 of the United States Code and GPO's Sales Program policies.	R2; Must
RD-2796	28.3.0-5.0-2	The system shall provide the capability for authorized users to manually adjust the price.	R2; Must
RD-2797	28.3.0-5.0-3	The system shall provide the capability to dynamically adjust the price.	R2; Must
RD-2798	28.3.0-5.0-4	The system shall provide the capability to apply price schedules.	R2; Must
RD-2799	28.3.0-6	The system shall adhere to industry best practices for performance of a Web-accessible e-commerce system.	R2; Must
RD-2800	28.3.0-7	The system shall include an online bookstore web interface that complies with the FDsys interface requirements and includes a shopping cart, order tracking, backorder capabilities, third party ordering, thumbnail cover images, and a fully browsable and searchable catalog of items available for purchase that is updated at least daily.	R2; Must
RD-2801	28.3.0-8	The system shall provide the capability to process international and domestic requests for hard copy, electronic presentation, digital media, and service product lines as designated by GPO's Publication and Information Sales business unit.	R2; Must
RD-2802	28.3.0-9	The system shall provide the capability to process fee-based requests for the delivery of content with access restrictions.	R2; Must
RD-2803	28.3.0-10	The system shall support the collection of information (order taking) and pass this information to external systems for processing.	R2; Must

RD-2804	28.3.0-10.0-1	The system shall support the collection of payment information via the following methods:	R2; Must
RD-2805	28.3.0-10.0-1.0-1	Check/electronic transfer	R2; Must
RD-2806	28.3.0-10.0-1.0-2	Major credit cards including Visa, MasterCard, Discover/NOVUS, and American Express	R2; Must
RD-2807	28.3.0-10.0-1.0-3	Debit cards	R2; Must
RD-2808	28.3.0-10.0-1.0-4	Purchase orders	R2; Must
RD-2809	28.3.0-10.0-1.0-5	Requests for invoicing	R2; Must
RD-2810	28.3.0-10.0-1.0-6	Deposit accounts	R2; Must
RD-2811	28.3.0-10.0-1.0-7	Government Account	R2; Must
RD-2812	28.3.0-10.0-1.0-8	Cash	R2; Must
RD-2813	28.3.0-10.0-1.0-9	Gift card	R2; Must
RD-2814	28.3.0-10.0-2	The system shall securely pass information to external systems for processing.	R2; Must
RD-2815	28.3.0-10.0-3	The system shall comply with the Federal Trade Commission's Mail or Telephone Order Merchandise Rule.	R2; Must
RD-2816	28.3.0-10.0-4	The system shall comply with the Fair Credit Billing Act.	R2; Must
RD-2817	28.3.0-10.0-5	The system shall comply with the Fair Credit Reporting Act.	R2; Must
RD-2818	28.3.0-10.0-6	The system shall comply with the Children's Online Privacy Protection Act (COPPA).	R2; Must
RD-2819	28.3.0-10.0-7	The system shall comply with the FTC's rules for implementing the Children's Online Privacy Protection Act (COPPA).	R2; Must
RD-2820	28.3.0-11	The system shall provide the capability to automatically verify and validate payment information submitted by users prior to delivery fulfillment.	R2; Must
RD-2821	28.3.0-11.0-1	The system shall provide the capability to validate payment information in real-time via external GPO systems.	R2; Must
RD-2822	28.3.0-11.0-2	The system shall provide the capability to validate payment information in real-time via the U.S. Treasury Department's Pay.gov credit card processing system	R2; Must
RD-2823	28.3.0-12	The system shall provide the capability for users to delegate requests to other users (e.g. user's "hand-off" orders to other authorized officials to submit payment).	R2; Must
RD-2824	28.3.0-13	The system shall provide the capability to display lists of new and popular titles, best sellers, and other lists as defined by GPO business rules.	R1C; Should / R2; Must
RD-2825	28.3.0-13.0-1	The system shall provide the capability to display lists of all hard copy, electronic presentation, digital media, and service product lines as designated by GPO's Publication and Information Sales business unit.	R2; Must
RD-2826	28.3.0-14	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.)	R2; Must
RD-2827	28.3.0-14.0-1	The system shall provide the capability to manage, secure, and maintain End User information associated with subscriptions.	R2; Must
RD-2828	28.3.0-14.0-2	The system shall provide the capability to notify End Users when their subscriptions are about to end (e.g., renewal notices).	R2; Must
RD-2829	28.3.0-15	The system shall provide the capability to deliver personalized offers based on individual user request history or users with similar request histories. (e.g. "you may also be interested in…").	R2; Must
RD-2830	28.3.0-15.0-1	The system shall provide the capability for users to opt-out of personalized offers.	R2; Must
RD-2831	28.3.0-16	The system shall provide the capability for users to cancel full or partial requests prior to fulfillment.	R2; Must
RD-2832	28.3.0-17	The system shall provide the capability to provide authorized users with a detailed transaction summary.	R2; Must
RD-2833	28.3.0-18	The system shall provide the capability for authorized users to configure transaction summaries.	R2; Must
RD-2834	28.3.0-19	The system shall provide the capability to manage transaction records according to GPO, Federal, and FTC regulations in accordance with GPO privacy and required records retention policies.	R2; Must
RD-2835	28.3.0-19.0-1	The system shall securely maintain electronic copies of orders, shipments, and financial records for at least seven years.	R2; Must
RD-2836	28.3.0-20	The system shall provide the capability to generate reports for fee-based transactions (e.g., order histories, sales transactions, inventory data).	R2; Must

RD-2837	28.4	***28.4 Request – Delivery Options***	
RD-2838	28.4.0-1	The system shall have the capability to determine what options are available for delivery of particular content or metadata.	R1C; Must
RD-2839	28.4.0-2	The system shall provide the capability for users to request delivery of content or metadata from available options as defined by GPO business units.	R2; Must
RD-2840	28.4.0-3	The system shall provide the capability for users to select format from available options (e.g., text based document or publication, audio, video, integrated resource such as a web page, geospatial).	R1C; Must
RD-2841	28.4.0-4	The system shall provide the capability for users to select file type from available options (e.g., DOC, MP3, PDF).	R1C; Must
RD-2842	28.4.0-5	The system shall provide the capability for users to select resolution (e.g., images, video) from available options.	R1C; Could / R2; Must
RD-2843	28.4.0-6	The system shall provide the capability for users to select color space from available options (e.g. RGB, CMYK).	R1C; Could / R2; Must
RD-2844	28.4.0-7	The system shall provide the capability for users to select compression and size from available options.	R1C; Could / R2; Must
RD-2845	28.4.0-8	The system shall provide the capability for users to select transfer rate from available options.	R1C; Could / R2; Must
RD-2846	28.4.0-9	The system shall provide the capability for users to select platform from available options.	R2; Must
RD-2847	28.4.0-10	The system shall provide the capability for users to select the version of content from available options.	R1B; Must
RD-2848	28.4.0-11	The system shall provide the capability for users to select delivery of related content from available options.	R1C; Should / R2; Must
RD-2849	28.4.0-12	The system shall provide the capability for users to select metadata schema or input standards from available supported options (e.g. ONIX, Advanced Book Information, MARC, OAI-PMH).	R1C; Must
RD-2850	28.4.0-13	The system shall provide the capability for users to select quantity of items requested for delivery (e.g., one, five, batch).	R1C; Must
RD-2851	28.4.0-14	The system shall provide the capability for users to select output type from available options (e.g., hard copy, electronic presentation, digital media).	R1C; Must
RD-2852	28.4.0-15	The system shall provide the capability for users to select data storage device from available options (e.g., CD, DVD, server).	R1C; Must
RD-2853	28.4.0-16	The system shall provide the capability for users to select level of granularity from available options (e.g., title, part, section, paragraph, graphic, page).	R1B; Must
RD-2854	28.4.0-17	The system shall provide the capability for users to select electronic delivery method from available options (e.g., FTP, RSS, email, download, broadcast).	R1C; Must
RD-2855	28.4.0-18	The system shall provide the capability for users to schedule delivery from the system.	R1C; Must
RD-2856	28.4.0-19	The system shall provide the capability for users to select tangible delivery method from available options (e.g., air transportation, ground transportation, pickup, overnight, priority, freight).	R2; Must
RD-2857	28.4.0-20	The system shall provide the capability for GPO to offer users separate "bill to" and "ship to" options for delivery or shipment of tangible content.	R2; Must
RD-2858	28.4.0-21	The system shall provide the capability for users to submit multiple address options for delivery or shipment of tangible content.	R2; Must
RD-2859	28.4.0-22	The system shall provide the capability to preview requested content.	R2; Should / R3; Must
RD-2860	28.4.0-22.0-1	The system shall provide the capability to view the access copy of content where available.	R1C; Must
RD-2861	28.4.0-22.0-2	The system shall provide the capability for authorized users to preview publications that have been created from custom composition and content formatting.	R3; Must
RD-2862	28.4.0-23	The system shall have the capability to support custom composition and content formatting from available options (e.g., 2 columns, cover stock, font).	R2; Should / R3; Must

RD-2863	28.5	***28.5 Request – User Accounts***	

RD-2864	28.6	***28.6 Order Numbers and Request Status***	
RD-2865	28.6.0-1	The system shall provide the capability to assign an order number for requests.	R2; Must
RD-2866	28.6.0-2	The system shall not repeat an order number.	R2; Must
RD-2867	28.6.0-3	The system shall record order numbers in metadata.	R2; Must
RD-2868	28.6.0-4	The system shall have the capability to provide order numbers to users.	R2; Must
RD-2869	28.6.0-5	The system shall provide the capability for users to track the status of their requests.	R2; Must

RD-2870	29	**29 Requirements for Cataloging and Reference Tools**	
RD-2871	29.1	***29.1 Cataloging and Reference Tools – Metadata Management***	
RD-2873	29.1.0-2	The system shall support creation of metadata according to specified cataloging rules.	R1B; Must
RD-2874	29.1.0-3	The system shall apply authority control to certain fields to provide cross-referencing of terms.(e.g., a user enters any form of a name, title, or subject in a search and all database items associated with that form must be retrieved).	R1C; Must
RD-2875	29.1.0-4	The system shall support the creation of ONIX metadata	R2; Must
RD-2876	29.1.0-4.0-1	The system shall support the creation of ONIX metadata from existing metadata.	R2; Must
RD-2877	29.1.0-4.0-2	Fdsys shall notify users that content is available for selection for the sales program.	R2; Must
RD-2878	29.1.0-5	The system shall support the creation of library standard bibliographic records (e.g., MARC).	R1B; Must
RD-2879	29.1.0-6	The system shall support the extraction of metadata from content.	R2; Must
RD-2881	29.1.0-8	The system shall provide for the creation of new metadata records based on existing metadata records.	R1B; Must
RD-2882	29.1.0-9	The system shall provide the capability to acquire and integrate metadata from external sources.	R2; Must
RD-2883	29.1.0-10	The system shall relate descriptive metadata with the content described.	R1B; Must
RD-2884	29.1.0-11	The system shall provide capability for authorized users to manage metadata.	R1B; Must
RD-2885	29.1.0-11.0-1	The system shall provide capability for authorized users to add metadata.	R1B; Must
RD-2886	29.1.0-11.0-2	The system shall provide capability for authorized users to modify metadata.	R1B; Must
RD-2887	29.1.0-11.0-3	The system shall provide capability for authorized users to delete metadata.	R1B; Must
RD-2888	29.1.0-12	System shall record the change history of cataloging metadata.	R2; Must
RD-2889	29.1.0-13	The system shall have the ability to provide access to metadata throughout the lifecycle of the content.	R1B; Must
RD-2890	29.1.0-14	The system shall provide the capability to add metadata specifically for GPO sales purposes (e.g., book jacket art, reviews, summaries).	R2; Could
RD-2891	29.1.0-15	The system shall have the capability to record and manage relationships among the issues or volumes of serially-issued publications.	R1B; Must

RD-2892	29.2	***29.2 Cataloging and Reference Tools – Metadata Delivery***	
RD-2893	29.2.0-1	The system shall provide the capability to export metadata as individual records or in batch based on user-defined parameters.	R1C; Must
RD-2894	29.2.0-2	The system will provide for display and output of brief citations.	R1B; Must
RD-2895	29.2.0-3	The system will provide for display and output of basic bibliographic citations.	R1C; Must
RD-2896	29.2.0-4	The system will provide for display and output of full records.	R1B; Must
RD-2897	29.2.0-5	The system will provide for display and output of MARC records.	R1B; Must
RD-2898	29.2.0-6	The system will provide for the delivery of output in a variety user-specified	R2; Must

		methods or formats, including electronic mail or Web pages.	
RD-2899	29.2.0-6.0-1	The system will be capable of delivering metadata to users in electronic mail messages.	R2; Must
RD-2900	29.2.0-6.0-2	The system will be capable of delivering metadata to users in Web pages.	R2; Must
RD-2901	29.2.0-6.0-3	The system shall support the capability to deliver metadata to users in additional formats in the future.	R2; Must
RD-2902	29.2.0-7	The system shall output metadata in formats specified by the user, including MARC, ONIX, ASCII text, or comma delimited text.	R2; Must
RD-2903	29.2.0-7.0-1	The system shall output metadata in MARC format when requested by the user.	R2; Must
RD-2904	29.2.0-7.0-2	The system shall output metadata in ONIX format when requested by the user.	R2; Must
RD-2905	29.2.0-7.0-3	The system shall output metadata in ASCII text format when requested by the user.	R2; Must
RD-2906	29.2.0-7.0-4	The system shall output metadata in comma-delimited format when requested by the user.	R2; Must
RD-2907	29.2.0-7.0-5	The system shall support the capability to output metadata in additional formats in the future.	R2; Must

RD-2908	29.3	***29.3 Reference Tools***	
RD-2909	29.3.0-1	The system shall have the ability to generate lists based on any metadata field.	R2; Must
RD-2910	29.3.0-2	The system shall have the capability to generate lists based on search query (e.g., that match a library's item selection profile).	R2; Must
RD-2911	29.3.0-3	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).	R2; Must
RD-2912	29.3.0-4	The system should have the capability to generate lists that point to metadata (e.g., lists of publications available for selection by depository libraries).	R2; Must
RD-2913	29.3.0-5	The system should have the capability to generate lists that point to related resources or other reference tools (e.g., Browse Topics).	R2; Should
RD-2914	29.3.0-6	The system shall have the capability to link to external content and metadata.	R2; Must
RD-2915	29.3.0-7	The system shall be interoperable with third party reference tools (e.g., search catalogs of other libraries).	R3; Should
RD-2916	29.3.0-8	The system shall have the capability to dynamically generate reference tools.	R3; Could
RD-2917	29.3.0-9	The system will allow GPO to manage reference tools.	R2; Must
RD-2918	29.3.0-9.0-1	The system will allow GPO to add reference tools.	R2; Must
RD-2919	29.3.0-9.0-2	The system will allow GPO to update reference tools with capability of saving previous versions	R2; Must
RD-2920	29.3.0-9.0-3	The system will allow GPO to delete reference tools, with capability of saving previous versions.	R2; Must
RD-2921	29.3.0-10	The system shall be able to generate lists based on user preferences.	R1C; Should / R2; Must
RD-2922	29.3.0-11	The system shall provide the capability for users to customize reference tools.	R1C; Should / R2; Must
RD-2923	29.3.0-12	The system shall support interactive processes so users can create reference tools.	R2; Should

RD-2924	29.4	***29.4 Cataloging and Reference Tools – Interoperability and Standards***	
RD-2925	29.4.0-1	The system shall interface with, and allow full functionality of, the GPO Integrated Library System.	R2; Must
RD-2926	29.4.0-2	The system shall be compliant with NISO and ISO standards commonly used in the information industry.	R2; Must
RD-2927	29.4.0-2.0-1	The system shall be compliant with NISO standard Z39.2 - Information Interchange Format	R2; Must
RD-2928	29.4.0-2.0-2	The system shall be compliant with NISO standard Z39.9 - International	R2; Must

		Standard Serial Numbering-ISSN	
RD-2929	29.4.0-2.0-3	The system shall be compliant with NISO standard Z39.29 - Bibliographic References	R2; Must
RD-2930	29.4.0-2.0-4	The system shall be compliant with NISO standard Z39.43 -Standard Address Number (SAN) for the Publishing Industry	R2; Must
RD-2931	29.4.0-2.0-5	The system shall be compliant with NISO standard Z39.50 -Information Retrieval: Application Service Definition & Protocol Specification	R2; Must
RD-2932	29.4.0-2.0-6	The system shall be compliant with NISO standard Z39.56 - Serial Item and Contribution Identifier (SICI)	R2; Must
RD-2933	29.4.0-2.0-7	The system shall be compliant with NISO standard Z39.69 - Record Format for Patron Records	R2; Must
RD-2934	29.4.0-2.0-8	The system shall be compliant with NISO standard Z39.71 - Holding Statements for Bibliographic Items	R2; Must
RD-2935	29.4.0-2.0-9	The system shall be compliant with NISO standard Z39.85 - Dublin Core Metadata Element Set.	R2; Must
RD-2936	29.4.0-2.0-10	The system shall support commonly used cataloging standards.	R2; Must
RD-2937	29.4.0-3	The system shall support the creation of ONIX records.	R1C; Must
RD-2938	29.4.0-3.0-1	The system shall provide the capability to support search of GPO local data elements that identify unique attributes of the FDLP (e.g., GPO Superintendent of Documents (SuDocs) classification number, Item number, Depository Library number).	R1C; Must
RD-2939	29.4.0-3.0-2	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Library of Congress Classification.	R1C; Must
RD-2940	29.4.0-3.0-3	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Library of Congress Cataloging Rules.	R1C; Must
RD-2941	29.4.0-3.0-4	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the AACR2 Rev.	R1C; Must
RD-2942	29.4.0-3.0-5	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the LC Rule Interpretations.	R1C; Must
RD-2943	29.4.0-3.0-6	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Cooperative Online Serials (CONSER).	R1C; Must
RD-2944	29.4.0-3.0-7	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the CONSER Access Level Record Guidelines.	R1C; Must
RD-2945	29.4.0-3.0-8	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Cataloging Guidelines.	R1C; Must
RD-2946	29.4.0-3.0-9	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Superintendent of Documents Classification Manual.	R1C; Must
RD-2947	29.4.0-3.0-10	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the Library of Congress Subject Headings.	R1C; Must
RD-2948	29.4.0-3.0-11	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the NASA Subject Headings.	R1C; Must
RD-2949	29.4.0-3.0-12	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the MESH Subject Headings.	R1C; Must
RD-2950	29.4.0-3.0-13	The system shall support the use of the following and support all subsequent modifications, updates and revisions to all MARC Formats.	R1C; Must
RD-2951	29.4.0-3.0-14	The system shall support the use of the following and support all subsequent modifications, updates and revisions to the other GPO specified standards and best practices.	R1C; Must
RD-2952	29.4.0-4	The system shall be compliant with the following NISO and ISO standards: Z39.2 - Information Interchange Format, Z39.9 - International Standard Serial Numbering-ISSN, Z39.29 - Bibliographic References, Z39.43 -Standard Address Number (SAN) for the Publishing Industry, 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.	R2; Must
RD-2953	29.4.0-5	The system shall be compliant with the following NISO and ISO standards: Z39.2 - Information Interchange Format, Z39.9 - International Standard Serial Numbering-ISSN, Z39.29 - Bibliographic References, Z39.43 -Standard Address Number (SAN) for the Publishing Industry, Z39.50 -Information	R2; Must

		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.	

RD-2954	30	**30 Requirements for User Interface**	
RD-2955	30.1	***30.1 User Interface Core Capabilities***	
RD-2956	30.1.0-1	The system shall provide a default Graphical User Interface (GUI) for each functional element as required in accordance with the system release schedule.	R1B; Must
RD-2957	30.1.0-2	The system shall provide a default workbench for each user class as required in accordance with the system release schedule.	R1B; Must
RD-2959	30.1.0-2.0-2	The system shall provide the capability for GPO to create workbenches for subsets of user classes.	R2; Must
RD-2960	30.1.0-2.0-3	The system shall provide the capability for GPO to manage the toolsets that are available on default workbenches.	R1C; Must
RD-2961	30.1.0-2.0-4	The system shall provide a default public End User workbench that allows users to access the system without registering.	R1B; Must
RD-2962	30.1.0-2.0-4.0-1	The system shall allow all user to perform the actions allowed to unregistered users.	R1B; Must
RD-2963	30.1.0-2.0-5	Public End User GUIs shall be section 508 compliant.	R1C; Must
RD-2964	30.1.0-2.0-5.0-1	Content Originator GUIs shall be section 508 compliant.	R1C; Must
RD-2965	30.1.0-2.0-6	The system shall provide a default Service Specialist workbench that provides the capability for Service Specialists to handle exception processing.	R1B; Must
RD-2966	30.1.0-2.0-7	The system shall provide the capability for GPO to designate if users are required to register with the system to access certain internal default workbenches such as the default workbench for the System Administrator user class.	R1B; Must
RD-2967	30.1.0-3	The system shall provide the capability to maintain a consistent look and feel throughout workbenches and GUIs to the extent possible.	R1C; Must
RD-2968	30.1.0-3.0-1	GUIs shall conform to GPO design guidelines.	R1C; Must
RD-2969	30.1.0-4	The system shall support web-based GUIs.	R1B; Must
RD-2970	30.1.0-5	The system shall support non web-based GUIs, as necessary.	R1B; Should
RD-2972	30.1.0-7	The system shall provide for non-English language extensibility such that GUIs could contain non-English language text.	R1C; Could / R2; Must
RD-2973	30.1.0-8	The system shall provide GUIs that accept input of information by users.	R1B; Must
RD-2974	30.1.0-9	The system shall provide GUIs that accept submission of content by users.	R1B; Must
RD-2975	30.1.0-10	The system shall provide GUIs that allow users to input and submit registration information and login to the system.	R1B; Must
RD-2976	30.1.0-11	The system shall only display GUI functionality appropriate to the user and the actions the user is taking.	R1B; Must
RD-2977	30.1.0-11.0-1	The system shall have the capability to assign access to system functionality based on a user role.	R1B; Must
RD-2978	30.1.0-11.0-2	The system shall have the capability to assign access to system functionality based on user security settings.	R1B; Must
RD-2979	30.1.0-12	The system shall provide the capability to integrate search tools, cataloging and reference tools, request tools, and user support tools seamlessly into an End User interface.	R1B; Must
RD-2980	30.1.0-13	The system shall provide GUIs that can be displayed on Macintosh, Linux, and Windows environments.	R1B; Must
RD-2981	30.1.0-13.0-1	The system shall provide R1B GUIs that are displayable in Firefox 1.5.x.	R1B; Must
RD-2982	30.1.0-13.0-2	The system shall provide R1B GUIs that are displayable in IE 6.x.	R1B; Must
RD-2983	30.1.0-13.0-3	The system shall provide R1C GUIs that are fully functional in Mozilla Firefox 1.5.x.	R1C; Must
RD-2984	30.1.0-13.0-4	The system shall provide R1C GUIs that are fully functional in Microsoft Internet Explorer 6.x.	R1C; Must
RD-2985	30.1.0-13.0-5	The system shall provide R1C GUIs that are fully functional in Mozilla Firefox 2.0.x.	R1C; Must

RD-2986	30.1.0-13.0-6	The system shall provide R1C GUIs that are fully functional in Microsoft Internet Explorer 7.x.	R1C; Should
RD-2987	30.1.0-13.0-7	The system shall provide R1C GUIs that are fully functional in Netscape Navigator 7.x.	R1C; Should
RD-2988	30.1.0-13.0-8	The system shall provide R1C GUIs that are fully functional in Safari 1.x.	R1C; Should
RD-2989	30.1.0-13.0-9	The system shall provide R1C GUIs that are fully functional in Konqueror 2.x.	R1C; Should
RD-2990	30.1.0-13.0-10	The system shall provide Web pages that are designed based on Web standards.	R1C; Must
RD-2991	30.1.0-13.0-11	The system shall provide static Web pages that are designed using templates.	R1C; Must
RD-2992	30.1.0-14	The system shall provide GUIs that are capable of providing feedback, alerts, or notices to users.	R1B; Must
RD-2993	30.1.0-15	The system shall provide GUIs that are capable of providing context specific help and user support.	R1B; Must
RD-2994	30.1.0-16	The system shall provide GUIs that allow users to browse content by collection.	R1C; Must
RD-2995	30.1.0-17	The system shall provide GUIs that allow users to drill-down into collections.	R1C; Must

RD-2996	30.2	***30.2 User Interface Standards and Best Practices***	
RD-2997	30.2.0-1	The system shall comply with best practices and guidelines regarding usability for graphical user interface design.	R1B; Should
RD-2998	30.2.0-1.0-1	GUIs shall be developed in accordance with the Research Based Web Design & Usability Guidelines, 2006 edition.	R1B; Should
RD-2999	30.2.0-1.0-2	Web GUIs shall be developed in accordance with the Web Style Guide, 2nd edition.	R1B; Should
RD-3000	30.2.0-2	Where the system uses the following technologies for interoperability it will use the stated standards as follows:	R1B; Must
RD-3001	30.2.0-2.0-1	The system shall conform to Extensible Markup Language (XML).	R1B; Must
RD-3002	30.2.0-2.0-2	The system shall conform to Extensible Style sheet Language (XSL).	R1B; Must
RD-3003	30.2.0-2.0-3	The system shall conform to Document Type Definition (DTD) and schema.	R1B; Must
RD-3004	30.2.0-2.0-3.0-1	The system shall conform to Document Type Definition (DTD).	R1B; Must
RD-3005	30.2.0-2.0-3.0-2	The system shall conform to schema.	R1B; Must
RD-3006	30.2.0-2.0-4	The system shall conform to XSL Transformations (XSLT).	R1B; Must
RD-3007	30.2.0-2.0-5	The system shall conform to XML Path Language (Xpath).	R1B; Must
RD-3008	30.2.0-2.0-6	The system shall conform to Extensible HyperText Markup Language (XHTML).	R1B; Must
RD-3009	30.2.0-2.0-7	The system shall conform to Cascading Style Sheets (CSS).	R1B; Must
RD-3010	30.2.0-2.0-8	The system shall conform to DHTML.	R1B; Must
RD-3011	30.2.0-2.0-9	The system shall conform to WML.	R2; Must

RD-3012	30.3	***30.3 User Interface Customization and Personalization***	
RD-3013	30.3.0-1	The system shall provide the capability for authorized users who have registered with the system to customize GUIs.	R1C; Should / R2; Must
RD-3014	30.3.0-1.0-1	The system shall provide the capability to add tools.	R1C; Should / R2; Must
RD-3015	30.3.0-1.0-2	The system shall provide the capability to remove tools.	R1C; Should / R2; Must
RD-3016	30.3.0-1.0-3	The system shall provide the capability to hide tools.	R1C; Should / R2; Must
RD-3017	30.3.0-1.0-4	The system shall provide the capability to modify the placement of tools.	R1C; Should /

			R2; Must
RD-3018	30.3.0-1.0-5	The system shall provide the capability to modify the size of tools.	R1C; Should / R2; Must
RD-3019	30.3.0-1.0-6	The system shall provide the capability to select text size from available options.	R1C; Should / R2; Must
RD-3020	30.3.0-1.0-7	The system shall provide the capability to select color scheme from available options.	R1C; Should / R2; Must
RD-3021	30.3.0-2	The system shall provide the capability to provide personalized GUIs and workbenches to users that have registered with the system.	R1C; Could / R2; Must
RD-3022	30.3.0-3	The system shall provide the capability to provide personalized GUIs and workbenches that are created from user histories as analyzed through data mining.	R1C; Could / R2; Must
RD-3023	30.3.0-4	The system shall provide the capability for users to revert to their original default GUIs and workbenches.	R1C; Should / R2; Must
RD-3024	30.3.0-5	The system shall provide the capability to maintain interface configurations across user sessions.	R1C; Should / R2; Must

RD-3025	30.4	***30.4 User Interface Default Workbenches***	
RD-3026	30.4.0-1	The system shall provide the capability to configure workbenches according to criticality and release schedules specified in individual requirements.	R2; Must
RD-3027	30.4.0-2	The system must provide a workbench for Content Originators that is based on their user role.	R2; Must
RD-3028	30.4.0-3	The system must provide a workbench for GPO Content Evaluators that is based on their user role.	R1B; Must
RD-3029	30.4.0-4	The system must provide a default interface for GPO Service Specialists that is based on their user role.	R1B; Must
RD-3030	30.4.0-5	The system must provide a workbench for Service Providers (e.g., GPO Service Providers and External Service Providers) that is based on their user role.	R1B; Must
RD-3031	30.4.0-6	The system must provide a workbench for End Users (e.g., Public End Users, Library End Users, Small Business End Users, Congressional End Users, Agency End Users, Information Industry End Users) that is based on their user role.	R1B; Must
RD-3032	30.4.0-7	The system must provide a workbench for GPO Business Managers that is based on their user role.	R1C; Could / R2; Must
RD-3033	30.4.0-8	The system shall provide a default interface for System Administrators that is based on their user role.	R1B; Must
RD-3042	30.4.0-17	The system shall provide a default interface for Operations Managers that is based on their user role.	R1B; Must

RD-3043	31	**31 Requirements for User Support**	
RD-3044	31.1	***31.1 User Support Core Capabilities***	
RD-3045	31.1.0-1	The system shall provide multiple methods of contact for user assistance.	R2; Must
RD-3046	31.1.0-1.0-1	The system shall provide multiple methods for users to contact authorized users for user assistance.	R2; Must
RD-3047	31.1.0-1.0-1.0-1	The system shall provide web form for users to contact authorized users for user assistance.	R1C; Must
RD-3048	31.1.0-1.0-1.0-2	The system shall provide phone numbers for users to contact authorized users for user assistance based on their user profile and the function they are performing.	R2; Could
RD-3049	31.1.0-1.0-1.0-3	The system shall provide e-mail addresses for users to contact authorized users for user assistance based on their user profile and the function they are	R2; Must

		performing.	
RD-3050	31.1.0-1.0-1.0-4	The system shall provide mailing addresses for users to contact authorized users for user assistance based on their user profile and the function they are performing.	R2; Could
RD-3051	31.1.0-1.0-1.0-5	The system shall provide real-time text chat for users to contact GPO Service Specialists for user assistance.	R2; Could
RD-3052	31.1.0-1.0-1.0-6	The system shall provide Facsimile numbers for users to contact authorized users for user assistance based on their user profile and the function they are performing.	R2; Could
RD-3053	31.1.0-1.0-1.0-7	The system shall provide desktop facsimile for users to contact authorized users for user assistance.	R2; Could
RD-3054	31.1.0-1.0-1.0-8	The system shall provide users with information on how to contact GPO for assistance.	R1C; Must
RD-3055	31.1.0-1.0-2	The system shall provide multiple methods for authorized users to contact users for user assistance.	R2; Could
RD-3056	31.1.0-1.0-2.0-1	The system shall provide phone numbers for authorized users to contact users for user assistance.	R2; Could
RD-3057	31.1.0-1.0-2.0-2	The system shall provide e-mail addresses for GPO Service Specialists to contact users for user assistance.	R2; Must
RD-3058	31.1.0-1.0-2.0-3	The system shall provide real-time text chat for authorized users to contact users for user assistance.	R2; Could
RD-3059	31.1.0-1.0-2.0-4	The system shall provide facsimile numbers for authorized users to contact users for user assistance.	R2; Could
RD-3060	31.1.0-1.0-2.0-5	The system shall provide desktop facsimile for GPO Service Specialists to contact users for user assistance.	R2; Could
RD-3061	31.1.0-2	The system shall provide users with the ability to opt-out of user support features.	R1C; Must
RD-3062	31.1.0-2.0-1	The system shall provide users with the ability to enable or disable context specific help that consists of customizable descriptive text displayed when a user points the mouse over an item on the user interface.	R1C; Must
RD-3063	31.1.0-2.0-2	The system shall provide users with the ability to enable or disable context specific help that consists of clickable help icons or text on the user interface.	R1C; Must
RD-3064	31.1.0-2.0-2.0-1	The system shall have the capability to provide for address hygiene utilizing CASS certified and National Change of Address certified software to minimize delivery risks.	R2; Could
RD-3065	31.1.0-2.0-2.0-2	The system shall have the capability for Computer Telephone Integration (CTI) with auto screen pop-ups to integrate the agency's telephone and order management systems.	R2; Could
RD-3066	31.1.0-2.0-2.0-3	The system shall have the capability to integrate with GPO's Automated Call Dialer (ACD) system to allow for automatic consumer telephone access to account and transaction data.	R2; Could
RD-3067	31.1.0-2.0-2.0-4	The system shall have the capability to process e-mail marketing campaigns	R2; Could

RD-3068	31.2	***31.2 User Support – Context Specific Help***	
RD-3069	31.2.0-1	The system shall provide context-specific help on user interfaces.	R1B; Could / R1C; Must
RD-3070	31.2.0-1.0-1	Content of context specific help shall be related to what is being viewed on the screen and shall be dynamically generated.	R2; Could / R3; Must
RD-3072	31.2.0-1.0-3	Context specific help shall consist of help menus.	R1B; Could / R1C; Must
RD-3073	31.2.0-1.0-3.0-1	Help menus shall contain user support information related to what is on the current user interface.	R1B; Could / R1C; Must
RD-3074	31.2.0-1.0-3.0-2	Help menus shall provide access to all available user support information for the entire system.	R1B; Could / R1C; Must
RD-3075	31.2.0-1.0-3.0-3	Authorized uses shall have the ability to manage information (text, images, audio, video, multimedia) in the help menu.	R1B; Could / R1C; Must
RD-3076	31.2.0-1.0-3.0-4	All users shall have the ability to search the help menu.	R1B; Could / R1C; Must
RD-3077	31.2.0-1.0-3.0-5	The system shall return search results to the user.	R1B; Could / R1C; Must
RD-3078	31.2.0-1.0-3.0-6	All users shall have the ability to navigate the help menu using an index.	R1B; Could

			/ R1C; Must
RD-3079	31.2.0-1.0-4	Context specific help shall consist of customizable descriptive text displayed when a user points the mouse over an item on the user interface.	R1B; Could / R1C; Must
RD-3080	31.2.0-1.0-4.0-1	Authorized users shall have the ability to manage customizable descriptive text.	R1B; Could / R1C; Must
RD-3081	31.2.0-1.0-5	Context specific help shall consist of clickable help icons or text on the user interface.	R1B; Could / R1C; Must
RD-3082	31.2.0-1.0-5.0-1	All users shall have the ability to click on help icons or text.	R1B; Could / R1C; Must
RD-3083	31.2.0-1.0-5.0-2	Upon clicking on help icons or text, the system shall display text, images, audio, video or multimedia components.	R1B; Could / R1C; Must
RD-3084	31.2.0-1.0-5.0-3	Authorized users shall have the ability to manage information (text, images, audio, video, multimedia) displayed as a result of clicking on help icons or text.	R1C; Could / R2; Must
RD-3085	31.2.0-1.0-5.0-4	Authorized users shall have the ability to place help icons or text where needed on the user interface.	R1C; Could / R2; Must
RD-3086	31.2.0-1.0-5.0-5	All users shall have the ability to view information displayed by clickable help icons.	R1B; Could / R1C; Must

RD-3087	31.3	***31.3 User Support – Helpdesk***	
RD-3088	31.3.0-1	The system shall have the capability to support a helpdesk to route, track, prioritize, and resolve user inquiries to authorized users.	R2; Must
RD-3089	31.3.0-2	Information collected and maintained shall comply with GPO and Federal privacy policies.	R1C; Must
RD-3090	31.3.0-2.0-1	Information collected and maintained shall comply with "Records maintained on individuals", Title 5 U.S. Code Sec. 552a, 2000 edition.	R1C; Must
RD-3091	31.3.0-2.0-2	Information collected and maintained shall comply with H.R. 2458, E-Government Act of 2002.	R1C; Must
RD-3092	31.3.0-3	The system shall have the capability to receive inquiries from registered and non-registered users.	R2; Must
RD-3093	31.3.0-3.0-1	The system shall have the capability to maintain user identification for inquiries and responses after a user no longer has a registered account in the system.	R2; Must
RD-3094	31.3.0-4	Users shall have the capability to select from lists of categories when submitting inquiries.	R1C; Could / R2; Must
RD-3095	31.3.0-4.0-1	Users shall have the capability to select from subgroups of categories when submitting inquiries.	R1C; Could / R2; Must
RD-3096	31.3.0-4.0-2	Authorized users shall have the capability to manage categories and subcategories.	R1C; Could / R2; Must
RD-3097	31.3.0-5	A user shall have the capability to attach files when submitting inquiries.	R1C; Could / R2; Must
RD-3098	31.3.0-6	The system shall have the capability to notify users that their inquiry has been received.	R1C; Could / R2; Must
RD-3099	31.3.0-7	The system shall have the capability to time and date stamp all inquiries and responses.	R1C; Could / R2; Must
RD-3100	31.3.0-8	The system shall have the capability to notify a user that they have been assigned an inquiry.	R1C; Could / R2; Must
RD-3101	31.3.0-9	The system shall have the capability to route, track, and prioritize inquiries and responses received.	R2; Must
RD-3102	31.3.0-9.0-1	The helpdesk shall have the capability to support multiple departments and additional future departments, when needed.	R2; Must
RD-3103	31.3.0-9.0-2	The helpdesk and knowledge base shall have the capability to synchronize with data entered into the system while not connected to the internet.	R2; Must
RD-3104	31.3.0-9.0-3	The helpdesk shall have the capability to integrate with user account information and additional sources of business process information stored outside of the helpdesk. (e.g., Oracle, user accounts in Storage/Access)	R2; Must
RD-3105	31.3.0-9.0-4	Other systems/functional elements shall have the capability to access information stored in the helpdesk.	R2; Must
RD-3106	31.3.0-9.0-5	The helpdesk shall have the capability to access information stored in other systems/functional elements.	R2; Must
RD-3107	31.3.0-9.0-6	The system shall allow users to specify job numbers (e.g., CO Ordering numbers, Request Ordering numbers) and other identifiers (e.g., voucher	R2; Must

		numbers, ISBN numbers) in inquiry fields.	
RD-3108	31.3.0-9.0-7	The system shall allow users to select from various templates for submission of inquiries. (e.g., complaint template for CO Order, template for phone conversation, template for contract modification request)	R2; Must
RD-3109	31.3.0-9.0-8	The system shall assign unique identifiers based on the type of template used. (e.g., to track complaints, modification requests)	R2; Must
RD-3110	31.3.0-9.0-9	The system shall allow authorized GPO users to manage templates for submission of inquiries.	R2; Must
RD-3111	31.3.0-9.0-10	The system shall have the capability for role based access to individual fields on individual helpdesk inquiries and responses. (e.g., Notes field with access to GPO employees only)	R2; Must
RD-3112	31.3.0-9.0-11	The system shall have the capability to display all inquiries and responses related to a particular job number (e.g., Request order number, CO Order number) or other unique identifier. (e.g., voucher numbers, ISBN numbers)	R2; Must
RD-3113	31.3.0-10	The system shall allow authorized users to manually create a new inquiry in order to accommodate inquiries that do not enter the system electronically.	R2; Must
RD-3114	31.3.0-11	The system shall provide the capability to queue inquiries.	R1C; Could / R2; Must
RD-3115	31.3.0-12	The system shall support priority processing.	R1C; Could / R2; Must
RD-3116	31.3.0-13	The system shall allow authorized users to manage the status categories for inquires.	R1C; Could / R2; Must
RD-3117	31.3.0-14	The system shall provide the capability for authorized users to restrict access to inquiry tracking.	R2; Must
RD-3118	31.3.0-15	The system shall provide automated routing of inquiries to the departments/individuals according to workflow guidelines, including the following.	R1C; Could / R2; Must
RD-3119	31.3.0-15.0-1	Automated inquiry routing shall be based on selections made by the user when an inquiry is made.	R1C; Could / R2; Must
RD-3120	31.3.0-15.0-2	Automated inquiry routing shall be based on keywords in the inquiry sent by the user.	R1C; Could / R2; Must
RD-3121	31.3.0-15.0-3	Automated inquiry routing shall be based on the user class of the inquirer.	R1C; Could / R2; Must
RD-3123	31.3.0-16	Authorized users shall have the capability to route inquiries to other authorized users.	R1C; Could / R2; Must
RD-3124	31.3.0-16.0-1	Authorized users shall have the ability to route an inquiry to a selected individual.	R1C; Could / R2; Must
RD-3125	31.3.0-16.0-2	Authorized users shall have the ability to route an inquiry to a selected department.	R1C; Could / R2; Must
RD-3126	31.3.0-16.0-3	Authorized users shall have the ability to route inquiries to users who do not have access to the system using e-mail.	R1C; Could / R2; Must
RD-3127	31.3.0-17	The system shall allow the user to determine the departments or individuals they wish to request answers from.	R1C; Could / R2; Must
RD-3128	31.3.0-17.0-1	The system shall allow the user to determine the departments they wish to request answers from.	R2; Must
RD-3129	31.3.0-17.0-2	The system shall allow the user individuals they wish to request answers from.	R2; Must
RD-3130	31.3.0-18	The system shall provide the capability to request user feedback regarding quality of response given.	R1C; Could / R2; Must
RD-3131	31.3.0-19	The system shall provide users with access to history of their inquiries and responses.	R1C; Could / R2; Must
RD-3132	31.3.0-20	The system shall store inquiries and responses.	R2; Must
RD-3133	31.3.0-21	The system shall have the capability to allow authorized users to amend inquiries and responses.	R1C; Could / R2; Must
RD-3134	31.3.0-22	The system shall have the capability for users to search inquiries and responses.	R2; Must
RD-3135	31.3.0-23	The system shall allow authorized users to search for inquiries by any field.	R2; Must
RD-3136	31.3.0-24	The system shall support the capability to monitor the quality of responses given by helpdesk staff.	R1C; Could; / R2; Must
RD-3137	31.3.0-25	The system shall have the capability to provide users with access to inquiries from other users related to their queries.	R1C; Could / R2; Must
RD-3138	31.3.0-25.0-1	The system shall allow for search of inquiries from other users.	R1C; Could / R2; Must
RD-3139	31.3.0-25.0-2	The system shall provide the capability to assign user access rights to individual questions and answers.	R1C; Could / R2; Must

RD-3140	31.3.0-26	The system shall provide the capability to record users responding to inquiries.	R2; Must
RD-3141	31.3.0-27	The system shall provide the capability to log information exchanges.	R2; Must
RD-3142	31.3.0-27.0-1	Information exchange logs shall store metadata relating to what is being discussed.	R2; Must
RD-3143	31.3.0-28	The system shall provide the capability to spell-check inquiries and responses before submission.	R1B; Could / R2; Must

RD-3144	31.4	***31.4 User Support – Knowledge Base***	
RD-3145	31.4.0-1	The system shall allow authorized users to add information to a knowledge base.	R2; Must
RD-3146	31.4.0-2	The system shall provide the ability for an authorized user to add electronic files to the knowledge base as attachments.	R2; Must
RD-3147	31.4.0-3	The system shall provide the capability to create customized templates for knowledge base entries.	R2; Could
RD-3148	31.4.0-3.0-1	The system shall provide the capability for authorized users to choose from a list of templates when creating knowledge base entries.	R2; Could
RD-3149	31.4.0-4	The system shall have the capability to time and date stamp all knowledge base entries.	R2; Must
RD-3150	31.4.0-5	The system shall provide the ability for authorized users to manage information in the knowledge base.	R2; Must
RD-3151	31.4.0-6	The system shall provide the capability to add inquiries and answers from the helpdesk to the knowledge base.	R2; Must
RD-3152	31.4.0-6.0-1	The system shall allow authorized users to edit and approve inquiries and responses for addition to the knowledge base.	R2; Must
RD-3153	31.4.0-6.0-2	The system shall have the capability for GPO users to recommend helpdesk inquiries and responses for the knowledge base.	R2; Must
RD-3154	31.4.0-7	The system shall provide the ability for authorized users to create categories and subcategories for information stored in the knowledge base.	R2; Must
RD-3155	31.4.0-8	The system shall provide the capability to store standard responses for use by specific user groups or subgroups.	R1C; Could / R2; Must
RD-3156	31.4.0-9	The system shall allow for information stored in the knowledge base to have role-based access restrictions.	R2; Must
RD-3157	31.4.0-9.0-1	The system shall allow for access restrictions to be applied to complete categories.	R2; Must
RD-3158	31.4.0-9.0-2	The system shall allow for access restrictions to be applied to individual knowledge base entries.	R2; Must
RD-3159	31.4.0-9.0-2.0-1	The system shall allow users to assign key words to knowledge base entries.	R2; Must
RD-3160	31.4.0-9.0-2.0-2	The system shall allow for fields (e.g., subject, title) with an unlimited number of characters.	R2; Must
RD-3161	31.4.0-9.0-2.0-3	The system shall have the capability for role based access to individual fields on individual knowledge base entries. (e.g., notes field with access to certain GPO employees only)	R2; Must
RD-3162	31.4.0-9.0-2.0-4	The system shall have the capability for intelligent searching of knowledge base. (e.g., when searching, system asks, "did you mean xxx"?)	R2; Must
RD-3163	31.4.0-9.0-2.0-5	The system shall have the capability to search by title.	R2; Must
RD-3164	31.4.0-9.0-2.0-6	The system shall have the capability to search by unique identifiers.	R2; Must
RD-3165	31.4.0-9.0-2.0-7	The system shall provide the capability to store standard responses for knowledge base entries for use by specific user groups or subgroups.	R2; Must
RD-3166	31.4.0-10	The system shall provide the capability for all users to search the knowledge base.	R2; Must
RD-3167	31.4.0-10.0-1	The system shall provide the capability for all users to perform a full-text search the knowledge base.	R2; Must
RD-3168	31.4.0-10.0-2	The system shall provide the capability for all users to search the knowledge base by phrase.	R2; Must
RD-3169	31.4.0-10.0-3	The system shall provide the capability for all users to search the knowledge base by identification number.	R2; Must
RD-3170	31.4.0-11	The system shall provide the capability to sort results of knowledge base searches.	R2; Must
RD-3171	31.4.0-11.0-1	The system shall provide the capability to sort search results by category.	R2; Must
RD-3172	31.4.0-11.0-2	The system shall provide the capability to sort search results by subject.	R2; Must
RD-3173	31.4.0-11.0-3	The system shall provide the capability to sort search results by a default sort.	R2; Must

RD-3174	31.4.0-12	The system shall provide the capability for a user to receive e-mail updates when the content of information stored in a knowledge base entry is updated.	R1B; Could / R2; Must
RD-3175	31.4.0-13	The system shall provide the capability to perform records management functions on knowledge base data.	R2; Must
RD-3176	31.4.0-14	The system shall provide the capability to spell-check knowledge base entries before submission.	R2; Must

RD-3177	31.5	***31.5 User Support – Alerts***	
RD-3178	31.5.0-1	The system shall have the capability to provide alert services.	R1B; Must
RD-3179	31.5.0-1.0-1	The system shall allow all users to subscribe and unsubscribe to alert services	R1B; Could / R1C; Must
RD-3180	31.5.0-1.0-2	Alert services shall be provided via the following channels.	R1B; Could / R1C; Must
RD-3181	31.5.0-1.0-2.0-1	E-mail messages	R1C; Must
RD-3182	31.5.0-1.0-2.0-2	RSS Feeds conforming to the RSS 2.0 Specification.	R1C; Must
RD-3183	31.5.0-1.0-2.0-3	Messages while logged into Fdsys	R1C; Must
RD-3184	31.5.0-1.0-3	The system shall allow users to chose the method an alert is delivered in from a list of available options.	R1B; Could / R1C; Must
RD-3185	31.5.0-1.0-4	The system shall provide alerts based on user profiles and history.	R1C; Could / R2; Must
RD-3186	31.5.0-1.0-5	The system shall have the capability to automatically send alerts based on system events.	R1B; Could / R1C; Must
RD-3187	31.5.0-1.0-6	The system shall have the capability to automatically send alerts based on business events (e.g., new version of publication available, new services available).	R1B; Could / R1C; Must
RD-3188	31.5.0-1.0-7	The system shall have the capability to automatically send notifications to users based on job processing events.	R1C; Must
RD-3189	31.5.0-1.0-8	Authorized users shall be able to create new alert categories where new alerts are manually generated.	R1B; Could / R1C; Must
RD-3190	31.5.0-1.0-9	The system shall have the capability to populate the knowledge base with alerts.	R1C; Could / R2; Must
RD-3191	31.5.0-1.0-10	The system shall provide the capability for users to add alerts to the knowledge base.	R1C; Could / R2; Must

RD-3192	31.6	***31.6 User Support – Training and Events***	
RD-3193	31.6.0-1	The system shall provide users access to training materials and training history.	R2; Could
RD-3194	31.6.0-1.0-1	The system shall provide access to training materials available as digital video.	R2; Could
RD-3195	31.6.0-1.0-2	The system shall provide access to training materials available as digital documents.	R2; Could
RD-3196	31.6.0-1.0-3	The system shall provide access to training materials available as digital audio.	R2; Could
RD-3197	31.6.0-1.0-4	The system shall provide access to training materials available as digital multimedia.	R2; Could
RD-3198	31.6.0-1.0-5	The system shall provide access to training materials available in other formats.	R2; Could
RD-3199	31.6.0-2	The system shall allow authorized users to manage training materials and training history.	R2; Could
RD-3200	31.6.0-3	The system shall have the capability for authorized users to restrict access to training material and training history.	R2; Could
RD-3201	31.6.0-3.0-1	Access restrictions to training materials shall be based on user class.	R2; Could
RD-3202	31.6.0-3.0-2	Access restrictions to training materials shall be based on individual users.	R2; Could
RD-3203	31.6.0-4	The system shall allow users to enroll in training and events.	R2; Could
RD-3204	31.6.0-5	The system shall allow authorized users to manage training and events.	R2; Could
RD-3205	31.6.0-6	The system shall provide interactive training.	R2; Could
RD-3206	31.6.0-6.0-1	The system shall provide interactive self-paced training.	R2; Could
RD-3207	31.6.0-6.0-2	The system shall provide interactive instructor-led training.	R2; Could
RD-3208	31.6.0-7	The system shall provide users verification of enrollment in training and events.	R2; Could

RD-3209	31.6.0-8	The system shall provide the capability for users to measure their progress and performance.	R2; Could
RD-3210	31.6.0-9	The system shall provide the capability for users to provide feedback on training.	R2; Could
RD-3211	31.6.0-9.0-1	The system shall provide online tutorials.	R2; Could

RD-3212	31.7	***31.7 Contact Management***	
RD-3213	31.7.0-1	The system shall enable GPO users to view and manage contact data while not connected to the internet or internal server.	R2; Must
RD-3214	31.7.0-2	The system shall have the capability to synchronize data managed offline with the contact database when reconnected.	R2; Must
RD-3215	31.7.0-3	The system shall enable GPO users to track contact data (e.g., name, company, address, phone, e-mail, last meeting date, and status).	R2; Must
RD-3216	31.7.0-4	The system shall enable GPO users to create customizable fields for contact data (e.g., billing address code, GPO Express Customer).	R2; Must
RD-3217	31.7.0-5	The system shall enable GPO users to manage notes, history, sales, and attached files to each contact record.	R2; Must
RD-3218	31.7.0-6	The system shall allow each contact to have an owner associated with the contact record.	R2; Must
RD-3219	31.7.0-7	The system shall enable GPO users to manage groups of related contact records (e.g., all contacts at a single agency).	R2; Must
RD-3220	31.7.0-8	The system shall enable GPO users to hierarchically group contact records.	R2; Must
RD-3221	31.7.0-9	The system shall enable GPO users to track sales opportunities.	R2; Must
RD-3222	31.7.0-10	The system shall enable GPO users to generate sales opportunities reports.	R2; Must
RD-3223	31.7.0-11	The system shall have the capability to integrate with GPO's e-mail client (e.g., Microsoft Outlook).	R2; Must
RD-3224	31.7.0-12	The system shall have the capability to integrate with handheld devices used by GPO employees (e.g., Blackberry devices).	R2; Must
RD-3225	31.7.0-13	The system shall have a calendar which synchronizes with GPO's e-mail client calendar.	R2; Must
RD-3226	31.7.0-14	The system shall enable GPO users to schedule calls, meetings and tasks associated with each contact record.	R2; Must
RD-3227	31.7.0-15	The system shall enable users to prioritize tasks.	R2; Must
RD-3228	31.7.0-16	The system shall enable GPO users to generate mail merges using information stored in contact records.	R2; Must
RD-3229	31.7.0-17	The system shall enable GPO users to search records with any field.	R2; Must
RD-3230	31.7.0-18	The system shall enable GPO users to search for empty fields or non-empty fields.	R2; Must
RD-3231	31.7.0-19	The system shall enable GPO users to generate reports.	R2; Must
RD-3232	31.7.0-20	The system shall enable GPO users to create customized report templates/layouts.	R2; Must
RD-3233	31.7.0-21	The system shall allow users to record and store meeting minutes with internal and external contacts.	R2; Could
RD-3234	31.7.0-22	The system shall allow users to associate multiple internal and external contacts with the meeting minutes.	R2; Could
RD-3235	31.7.0-23	The system shall allow users to associate meeting minutes with a list of hierarchical categories.	R2; Could
RD-3236	31.7.0-24	The system shall allow users to record the date, time, location and subject of the meeting.	R2; Could
RD-3237	31.7.0-25	The system shall allow users to record the content of the meeting using an unlimited number of characters.	R2; Could
RD-3238	31.7.0-26	The system shall allow users to create reports with details of all meeting minutes.	R2; Could
RD-3239	31.7.0-27	The system shall allow users to filter the data for the report by contact, department, and category.	R2; Could
RD-3240	31.7.0-28	The system shall allow users to create reports including the following elements:	R2; Could
RD-3241	31.7.0-29	Meeting subject	R2; Could
RD-3242	31.7.0-30	List of all contacts associated with the meeting	R2; Could
RD-3243	31.7.0-31	Date, time and location of meeting	R2; Could
RD-3244	31.7.0-32	Full meeting minutes	R2; Could
RD-3245	31.7.0-33	List of all categories associated with the meeting	R2; Could

RD-3246	32	**32 Requirements for Content Delivery and Processing**	
RD-3247	32.1	***32.1 Content Delivery Core Capabilities***	
RD-3248	32.1.0-1	The system shall have the capability to retrieve ACPs from Access Content Storage based on user request.	R1C; Must
RD-3249	32.1.0-2	The system shall have the capability to create DIPs from ACPs in delivery processing based upon a user request.	R1C; Must
RD-3250	32.1.0-3	The system shall have the capability to create pre-ingest bundles in delivery processing.	R1C; Must
RD-3251	32.1.0-4	The system shall have the capability to deliver DIPs and pre-ingest bundles based on user requests.	R1C; Must
RD-3252	32.1.0-4.0-1	The system shall have the capability to deliver DIPs based on user requests.	R1C; Must
RD-3253	32.1.0-4.0-2	The system shall have the capability to deliver pre-ingest bundles based on user requests.	R1C; Must
RD-3254	32.1.0-5	Users shall have the ability to pull DIPs and pre-ingest bundles from the system.	R1C; Must
RD-3255	32.1.0-5.0-1	The system shall provide the capability for a user to request the download of a DIP from the system.	R1C; Must
RD-3256	32.1.0-5.0-2	The system shall provide the capability for a user to perform an FTP get on a DIP from the system.	R1C; Must
RD-3257	32.1.0-5.0-3	The system shall support the capability for a user to pull a DIP from the system using additional methods in the future.	R3; Must
RD-3258	32.1.0-5.0-4	The system shall provide the capability for a user to request the download of a PIB from the system.	R1C; Must
RD-3259	32.1.0-5.0-5	The system shall provide the capability for a user to perform an FTP get on a PIB from the system.	R1C; Must
RD-3260	32.1.0-5.0-6	The system shall support the capability for a user to pull a PIB from the system using additional methods in the future.	R3; Must
RD-3261	32.1.0-6	The system shall have the capability to restrict Service Providers' access to DIPs and pre-ingest bundles for jobs that they have not been awarded.	R1C; Must
RD-3262	32.1.0-6.0-1	The system shall have the capability to restrict Service Providers' access to DIPs for jobs that they have not been awarded.	R1C; Must
RD-3263	32.1.0-6.0-2	The system shall have the capability to restrict Service Providers' access to pre-ingest bundles for jobs that they have not been awarded.	R1C; Must
RD-3264	32.1.0-7	The system shall have the capability to determine if delivery is possible.	R1C; Must
RD-3265	32.1.0-7.0-1	The system shall have the capability to determine if delivery is possible based upon business rules.	R1C; Must
RD-3266	32.1.0-7.0-2	The system shall have the capability to determine if delivery is possible based upon limitations of delivery mechanisms.	R1C; Must
RD-3267	32.1.0-7.0-3	The system shall have the capability to determine if delivery is possible based upon limitations of content formats.	R1C; Must
RD-3268	32.1.0-7.0-4	The system shall have the capability to inform users that delivery is not possible.	R1C; Must
RD-3269	32.1.0-7.0-5	The system shall have the capability to inform users why delivery is not possible.	R1C; Must
RD-3270	32.1.0-8	The system shall have the capability to provide users with estimated transfer time for delivery.	R1C; Could
RD-3271	32.1.0-9	The system shall have the capability to provide notification of fulfillment to users.	R1B; Must
RD-3272	32.1.0-9.0-1	The system shall have the capability to provide notification based on user preferences.	R1B; Should / R1C; Must
RD-3273	32.1.0-9.0-2	The system shall have the capability to provide notification based on information gathered at time of request.	R1B; Must

RD-3274	32.2	***32.2 Content Delivery Processing***	
RD-3275	32.2.0-1	The system shall have the capability to create DIPs containing zero or more digital objects, zero or more metadata files, and zero or more BPI files.	R1B; Must
RD-3276	32.2.0-1.0-1	The system shall have the capability to package DIPs containing digital objects.	R1B; Must
RD-3277	32.2.0-1.0-2	The system shall have the capability to package DIPs containing metadata.	R1B; Must
RD-3278	32.2.0-1.0-3	The system shall have the capability to package DIPs containing BPI.	R1B; Must
RD-3279	32.2.0-2	The system shall have the capability to assemble pre-ingest bundles containing digital objects, business process information and metadata required for service providers to output proofs and produce end product or service.	R1C; Must
RD-3280	32.2.0-2.0-1	The system shall have the capability to assemble pre-ingest bundles containing digital objects required for service providers to output proofs and produce end products or services.	R1C; Must
RD-3281	32.2.0-2.0-2	The system shall have the capability to assemble pre-ingest bundles containing BPI required for service providers to output proofs and produce end products or services.	R1C; Must
RD-3282	32.2.0-2.0-3	The system shall have the capability to assemble pre-ingest bundles containing metadata required for service providers to output proofs and produce end products or services.	R1C; Must
RD-3283	32.2.0-3	The system shall have capability to transform digital objects to different formats.	R1C; Should / R2; Must
RD-3284	32.2.0-4	The system shall have the capability to make adjustments to digital objects for delivery based on digital object format.	R1B; Could / R2; Must
RD-3285	32.2.0-4.0-1	The system shall have the capability to adjust the resolution of digital objects.	R1B; Could / R2; Must
RD-3286	32.2.0-4.0-2	The system shall have the capability to resize digital objects.	R1B; Could / R2; Must
RD-3287	32.2.0-4.0-3	The system shall have the capability to adjust the compression of digital objects.	R1B; Could / R2; Must
RD-3288	32.2.0-4.0-4	The system shall have the capability to adjust the color space of digital objects. (e.g., CMYK to RGB)	R1B; Could / R2; Must
RD-3289	32.2.0-4.0-5	The system shall have the capability to adjust the image quality settings of digital objects. (e.g., transparency, dithering, anti-aliasing)	R1B; Could / R2; Must
RD-3290	32.2.0-4.0-6	The system shall have the capability to rasterize digital objects.	R1B; Could / R2; Must
RD-3291	32.2.0-5	The system shall have the capability to process DIPs based on user request.	R1C; Must
RD-3292	32.2.0-6	The system shall have the capability to repurpose content from multiple packages into a single DIP.	R2; Must

RD-3293	32.3	***32.3 Content Delivery Mechanisms***	
RD-3294	32.3.0-1	The system shall have the capability to push DIPs and PIBs to users using various delivery mechanisms.	R1C; Must
RD-3295	32.3.0-1.0-1	The system shall have the capability to push DIPs to users using an RSS feeds conforming to the RSS 2.0 Specification.	R1C; Must
RD-3296	32.3.0-1.0-1.0-1	The system shall have the capability for users to sign up to receive DIPS via RSS feed for new publications added to GPO defined collections.	R1C; Must
RD-3297	32.3.0-1.0-1.0-2	The system shall have the capability for users to sign up to receive DIPS via RSS feed for new publications added by user defined criteria.	R2; Must
RD-3298	32.3.0-1.0-2	The system shall have the capability to push DIPs to users using E-mail.	R1C; Must
RD-3299	32.3.0-1.0-2.0-1	Users shall have the capability to request an e-mail of a DIP containing a single publication.	R1C; Must
RD-3300	32.3.0-1.0-2.0-2	Users shall have the capability to sign up to receive e-mails of new publications added to GPO defined collections.	R1C; Must
RD-3301	32.3.0-1.0-2.0-3	Users shall have the capability to sign up to receive e-mails of new publications added by user defined criteria.	R2; Must
RD-3302	32.3.0-1.0-3	The system shall have the capability to push DIPs to users using File Transfer Protocol.	R1C; Must
RD-3303	32.3.0-1.0-3.0-1	Users shall have the capability to request that files be transferred via FTP to	R1C; Must

		their server for a DIP containing a single publication.	
RD-3304	32.3.0-1.0-3.0-2	Users shall have the capability to request that files be transferred via FTP to their server for a DIP based on user defined criteria.	R1C; Must
RD-3305	32.3.0-1.0-4	The system shall have the capability to push DIPs to users using Secure File Transfer Protocol.	R3; Must
RD-3306	32.3.0-1.0-5	The system shall support the capability to push DIPs to users using additional methods in the future.	R3; Must
RD-3308	32.3.0-1.0-7	The system shall have the capability to push PIBs to users using E-mail.	R1C; Must
RD-3309	32.3.0-1.0-7.0-1	Users shall have the capability to request an e-mail of a PIB for a single order they have been awarded.	R1C; Must
RD-3310	32.3.0-1.0-7.0-2	Users shall have the capability to sign up to receive PIBS by e-mail for new orders they have been awarded.	R2; Must
RD-3311	32.3.0-1.0-8	The system shall have the capability to push PIBs to users using File Transfer Protocol.	R1C; Must
RD-3312	32.3.0-1.0-8.0-1	Users shall have the capability to request an FTP of a PIB for a single order they have been awarded.	R1C; Must
RD-3313	32.3.0-1.0-8.0-2	Users shall have the capability to sign up to receive PIBS by FTP for new orders they have been awarded.	R2; Must
RD-3314	32.3.0-1.0-9	The system shall have the capability to push PIBs to users using Secure File Transfer Protocol.	R3; Must
RD-3315	32.3.0-1.0-10	The system shall support the capability to push PIBs to users using additional methods in the future.	R3; Must
RD-3316	32.3.0-1.0-11	The maximum size DIP delivered by HTTP download shall be configurable by an authorized user.	R1C; Must
RD-3317	32.3.0-1.0-12	The maximum size PIB delivered by HTTP download shall be configurable by an authorized user.	R1C; Must
RD-3318	32.3.0-1.0-13	The maximum size DIP delivered by RSS feed shall be configurable by an authorized user.	R1C; Must
RD-3320	32.3.0-1.0-15	The maximum size DIP delivered by e-mail shall be configurable by an authorized user.	R1C; Must
RD-3321	32.3.0-1.0-16	The maximum size PIB delivered by e-mail shall be configurable by an authorized user.	R1C; Must
RD-3322	32.3.0-1.0-17	The maximum size DIP delivered by FTP shall be configurable by an authorized user.	R1C; Must
RD-3323	32.3.0-1.0-18	The maximum size PIB delivered by FTP shall be configurable by an authorized user.	R1C; Must
RD-3324	32.3.0-1.0-19	The maximum size DIP delivered by a future electronic channel shall be configurable by an authorized user.	R3; Must
RD-3325	32.3.0-1.0-20	The maximum size PIB delivered by a future electronic channel shall be configurable by an authorized user.	R3; Must
RD-3326	32.3.0-1.0-21	The time required to deliver via http download a DIP created from an ACP that contains a 100 KB (TBS) screen optimized PDF to an average PC (TBS) connected to the GPO Intranet running Internet Explorer 6 shall be 15 seconds (TBS) or less.	R3; Must
RD-3327	32.3.0-1.0-22	The time required to deliver via http download a DIP created from an AIP in online storage that contains a 100 KB (TBS) screen optimized PDF to an average PC (TBS) connected to the GPO Intranet running Internet Explorer 6 shall be 18 seconds (TBS) or less.	R3; Must
RD-3328	32.3.0-1.0-23	The time required to deliver via FTP a DIP created from an ACP that contains a 10 MB (TBS) set of files to an average PC (TBS) connected to the GPO Intranet running an FTP server shall be 60 seconds (TBS) or less.	R3; Must
RD-3329	32.3.0-1.0-24	The time required to deliver via FTP a DIP created from an AIP in online storage that contains a 10 MB (TBS) set of files to an average PC (TBS) connected to the GPO Intranet running Internet Explorer 6 shall be 65 seconds (TBS) or less.	R3; Must
RD-3330	32.3.0-2	The system shall provide the capability for users to pull DIPs and PIBs from the system using various delivery mechanisms, including, but not limited to Transfer Control Protocol/Internet Protocol.	R1B; Must

RD-3331 33

33 Requirements for Hard Copy Output

RD-3332	33.1	***33.1 Hard Copy Output Core Capabilities***	
RD-3333	33.1.0-1	The system shall have the capability to deliver DIPs and pre-ingest bundles to users from which hard copy output can be created.	R1C; Must
RD-3334	33.1.0-1.0-1	The system shall have the capability to provide DIPs and pre-ingest bundles that support the production of hard copy on any required hard copy output technology (e.g., offset press, digital printing).	R1C; Must
RD-3335	33.1.0-1.0-1.0-1	The system shall have the capability to provide DIPs that support the production of hard copy on any required hard copy output technology.	R1B; Must
RD-3336	33.1.0-1.0-1.0-2	The system shall have the capability to provide pre-ingest bundles that support the production of hard copy on any required hard copy output technology.	R1C; Must
RD-3337	33.1.0-2	The system shall have the capability to deliver DIPs and pre-ingest bundles that support static text and images.	R1C; Must
RD-3338	33.1.0-2.0-1	The system shall have the capability to deliver DIPs that support static text and images.	R1B; Could
RD-3339	33.1.0-2.0-2	The system shall have the capability to deliver pre-ingest bundles that support static text and images.	R1C; Could
RD-3340	33.1.0-3	The system shall have the capability to support hard copy output for variable data printing processes.	R3; Could
RD-3341	33.1.0-4	The system shall have the capability to add the GPO Imprint line to DIPs and pre-ingest bundles per the GPO Publication 310.2 and the New Imprint Line Announcement.	R2; Could
RD-3342	33.1.0-4.0-1	The system shall allow users to manually add the Imprint line.	R2; Could
RD-3343	33.1.0-4.0-2	The system shall automatically add the Imprint Line.	R2; Could
RD-3344	33.1.0-4.0-3	The system shall allow users to manually adjust the location of the Imprint line.	R2; Could
RD-3345	33.1.0-5	Files for hard copy output shall be delivered in file formats that conform to industry best practices	R1B; Must
RD-3346	33.1.0-5.0-1	The system shall have the capability to deliver files in their native application file format.	R1B; Must
RD-3347	33.1.0-5.0-1.0-1	The system shall have the capability to convert native files to PDF.	R1C; Must
RD-3348	33.1.0-5.0-2	The system shall have the capability to deliver optimized (print, press) PDFs.	R1B; Must
RD-3349	33.1.0-5.0-2.0-1	Optimized PDFs shall have fonts and images embedded.	R1B; Must
RD-3350	33.1.0-5.0-2.0-2	Image resolution of PDFs shall conform to industry best practices as defined in GPO's press optimized PDF settings.	R1B; Must
RD-3351	33.1.0-5.0-3	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files.	R1B; Must
RD-3352	33.1.0-5.0-3.0-1	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in Adobe InDesign.	R1B; Must
RD-3353	33.1.0-5.0-3.0-2	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in QuarkXPress.	R1B; Must
RD-3354	33.1.0-5.0-3.0-3	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in Adobe Framemaker.	R1B; Must
RD-3355	33.1.0-5.0-3.0-4	The system shall have the capability to deliver page layout files containing images, fonts, and linked text files formatted in Adobe Pagemaker.	R1B; Must
RD-3356	33.1.0-5.0-3.0-5	The system shall support the capability to deliver page layout files containing images, fonts, and linked text files in additional formats in the future.	R3; Must
RD-3357	33.1.0-5.0-4	The system shall have the capability to deliver vector graphics.	R1B; Must
RD-3358	33.1.0-5.0-5	The system shall have the capability to deliver raster images.	R1B; Must
RD-3359	33.1.0-5.0-6	The system shall have the capability to deliver Microsoft Office Suite application files.	R1B; Must
RD-3360	33.1.0-5.0-6.0-1	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft Word.	R1B; Must
RD-3361	33.1.0-5.0-6.0-2	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft PowerPoint.	R1B; Must
RD-3362	33.1.0-5.0-6.0-3	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft Excel.	R1B; Must
RD-3363	33.1.0-5.0-6.0-4	The system shall have the capability to deliver Microsoft Office Suite application files in Microsoft Visio.	R1B; Must
RD-3364	33.1.0-5.0-7	The system shall have the capability to deliver XML.	R1B; Must
RD-3365	33.1.0-5.0-7.0-1	The system shall support cascading style sheets.	R1B; Must
RD-3366	33.1.0-5.0-7.0-2	The system shall support document type definition/schema.	R1B; Must

RD-3367	33.1.0-5.0-8	The system shall have the capability to deliver text files.	R1B; Must
RD-3368	33.1.0-5.0-8.0-1	The system shall have the capability to deliver text files in Rich Text (RTF) format.	R1B; Must
RD-3369	33.1.0-5.0-8.0-2	The system shall have the capability to deliver text files in ASCII text format.	R1B; Must
RD-3370	33.1.0-5.0-8.0-3	The system shall have the capability to deliver text files in Unicode format.	R1B; Must
RD-3371	33.1.0-5.0-8.0-4	The system shall have the capability to deliver text files in Universal Multi-Octet Coded Character Set that is equivelent to the native file.	R1B; Must
RD-3372	33.1.0-5.0-8.0-5	The system shall support the capability to deliver text files in additional file formats in the future.	R3; Must
RD-3373	33.1.0-5.0-9	The system shall have the capability to deliver OASIS Open Document Format for Office Applications (OpenDocument) v1.0.	R1B; Must
RD-3374	33.1.0-5.0-9.0-1	The system shall have the capability to deliver postscript files.	R1B; Must
RD-3375	33.1.0-6	The system shall have the capability to generate DIPs and pre-ingest bundles that contain Job Definition Format (JDF) data.	R3; Could

RD-3376	34	**34 Requirements for Electronic Presentation**	
RD-3377	34.1	***34.1 Electronic Presentation Core Capabilities***	
RD-3378	34.1.0-1	The system shall have the capability to create DIPs for electronic presentation that comply with the FDsys accessibility requirements.	R1C; Must
RD-3379	34.1.0-1.0-1	The system shall have the capability to manually check digital objects for compliance with FDsys accessibility requirements.	R1C; Must
RD-3380	34.1.0-1.0-2	The system shall have the capability to automatically check digital objects for compliance with FDsys accessibility requirements.	R2; Must
RD-3381	34.1.0-1.0-3	The system shall have the capability to manually transform digital objects so that they are compliant with FDsys accessibility requirements.	R1C; Must
RD-3382	34.1.0-1.0-4	The system shall have the capability to automatically transform digital objects so that they are compliant with FDsys accessibility requirements.	R2; Must
RD-3383	34.1.0-2	The system shall have the capability to render content for presentation on end user devices.	R2; Must
RD-3384	34.1.0-3	The system shall have the capability to render content for presentation on multiple computer platforms, including but not limited to Windows, Macintosh, and Unix.	R2; Must
RD-3385	34.1.0-3.0-1	The system shall have the capability to render content for presentation on a Windows platform.	R1C; Must
RD-3386	34.1.0-3.0-2	The system shall have the capability to render content for presentation on Macintosh platform.	R1C; Must
RD-3387	34.1.0-3.0-3	The system shall have the capability to render content for presentation on a Unix platform.	R2; Must
RD-3388	34.1.0-4	The system shall have the capability to render content for presentation on non-desktop devices.	R2; Should / R3; Must
RD-3389	34.1.0-4.0-1	The system shall have the capability to render content for presentation on Digital Assistants (PDAs).	R2; Should / R3; Must
RD-3390	34.1.0-4.0-2	The system shall have the capability to render content for presentation on Digital Audio Players.	R2; Should / R3; Must
RD-3391	34.1.0-4.0-3	The system shall have the capability to render content for presentation on Electronic Books (E-Books).	R2; Should / R3; Must
RD-3392	34.1.0-4.0-4	The system shall have the capability to render content for presentation on Cell Phones.	R2; Should / R3; Must
RD-3393	34.1.0-5	The system shall have the capability to determine and deliver the file format needed for non-desktop electronic devices.	R2; Could
RD-3394	34.1.0-6	The system shall provide the capability to deliver DIPs that support static and dynamic text in multiple formats.	R2; Must
RD-3395	34.1.0-6.0-1	The system shall have the capability to deliver electronic content in XML that is equivelent to the native file.	R1B; Must
RD-3396	34.1.0-6.0-2	The system shall have the capability to deliver electronic content in HTML with linked files (e.g., JPEG, GIF, MPEG, MP3) referenced in the HTML code that	R1B; Must

		is equivelent to the native file.	
RD-3397	34.1.0-6.0-3	The system shall have the capability to deliver electronic content in XHTML with linked files (e.g., JPEG, GIF, MPEG, MP3) referenced in the XHTML code that is equivelent to the native file.	R1B; Must
RD-3398	34.1.0-6.0-4	The system shall have the capability to deliver electronic content in ASCII text that is equivelent to the native file.	R1B; Must
RD-3399	34.1.0-6.0-4.0-1	The system shall have the capability to convert images to descriptive ASCII text.	R2; Must
RD-3400	34.1.0-6.0-4.0-1.0-1	The system shall have the capability to replace images with descriptive text when available while converting digital objects to ASCII.	R1C; Must
RD-3401	34.1.0-6.0-5	The system shall have the capability to deliver electronic content in Unicode text that is equivelent to the native file.	R1B; Must
RD-3402	34.1.0-6.0-5.0-1	The system shall have the capability to convert images to descriptive Unicode text.	R2; Must
RD-3403	34.1.0-6.0-5.0-1.0-1	The system shall have the capability to replace images with descriptive text when available while converting digital objects to Unicode.	R1C; Must
RD-3404	34.1.0-6.0-6	The system shall have the capability to deliver electronic content in Open Document Format that is equivelent to the native file.	R1B; Must
RD-3405	34.1.0-6.0-7	The system shall have the capability to deliver content in MS Office formats.	R1B; Must
RD-3406	34.1.0-6.0-7.0-1	The system shall have the capability to deliver electronic content in Microsoft Excel (.xls) format.	R1B; Must
RD-3407	34.1.0-6.0-7.0-2	The system shall have the capability to deliver electronic content in Microsoft Word Document File Format (.doc).	R1B; Must
RD-3408	34.1.0-6.0-7.0-3	The system shall have the capability to deliver electronic content in Microsoft PowerPoint File Format (.ppt).	R1B; Must
RD-3409	34.1.0-6.0-7.0-4	The system shall have the capability to deliver electronic content in Microsoft Publisher File Format (.pub).	R1B; Must
RD-3410	34.1.0-6.0-8	The system shall have the capability to deliver electronic content in PDF that is equivelent to the native file	R1B; Must
RD-3411	34.1.0-6.0-9	The system shall have the capability to deliver electronic content in Open eBook Publication Structure (OEBPS) in accordance with Open eBook Publication Structure Specification Version 1.2.	R2; Could
RD-3412	34.1.0-7	The system shall provide the capability to deliver DIPs that support static and dynamic images in multiple formats.	R1B; Must
RD-3413	34.1.0-7.0-1	The system shall have the capability to deliver electronic content in JPEG that is equivelent to the native file.	R1B; Must
RD-3414	34.1.0-7.0-2	The system shall have the capability to deliver electronic content in JPEG 2000 that is equivelent to the native file.	R1B; Must
RD-3415	34.1.0-7.0-3	The system shall have the capability to deliver electronic content in TIFF that is equivelent to the native file	R1B; Must
RD-3416	34.1.0-7.0-4	The system shall have the capability to deliver electronic content in GIF that is equivelent to the native file.	R1B; Must
RD-3417	34.1.0-7.0-5	The system shall have the capability to deliver electronic content in SVG conforming to Scalable Vector Graphic (SVG) 1.1 Specification.	R1B; Must
RD-3418	34.1.0-7.0-6	The system shall have the capability to deliver electronic content in EPS conforming to Encapsulated PostScript File Format Specification Version 3.0.	R1B; Must
RD-3419	34.1.0-8	The system shall provide the capability to deliver DIPs that support audio information in multiple formats, including, but not limited to:	R1B; Must
RD-3420	34.1.0-8.0-1	The system shall have the capability to deliver audio content in MPEG 1 - Audio Layer 3 (MP3) that is equivelent to the native file.	R1C; Must
RD-3421	34.1.0-8.0-2	The system shall have the capability to deliver audio content in FLAC (Free Lossless Audio Codec) that is equivelent to the native file.	R1C; Could
RD-3422	34.1.0-8.0-3	The system shall have the capability to deliver audio content in Ogg Vorbis that is equivelent to the native file.	R1C; Could
RD-3423	34.1.0-8.0-4	The system shall have the capability to deliver audio content in CDDA (Compact Disc Digital Audio) that is equivelent to the native file.	R1C; Must
RD-3424	34.1.0-9	The system shall provide the capability to deliver DIPs that support audiovisual content (e.g., video, multimedia) in MPEG format.	R1B; Should / R1C; Must
RD-3425	34.1.0-10	The system shall have the capability to deliver electronic content that maintains desired user functionality.	R1B; Must
RD-3426	34.1.0-10.0-1	The system shall deliver electronic content that maintains hyperlinks to the extent possible.	R1B; Must
RD-3427	34.1.0-10.0-2	The system shall deliver electronic content that maintains interactive content functionality.	R1B; Must

RD-3428	35	**35 Requirements for Digital Media**	
RD-3429	35.1	***35.1 Digital Media Core Capabilities***	
RD-3430	35.1.0-1	The system shall have the capability to deliver DIPs for digital media containing electronic content for electronic presentation, hard copy output or data storage.	R1C; Must
RD-3431	35.1.0-1.0-1	The system shall have the capability to deliver pre-ingest bundles for digital media containing electronic content for electronic presentation, hard copy output or data storage.	R1B; Must
RD-3432	35.1.0-2	The system shall have the capability to deliver DIPs that support the creation of removable digital media.	R1C; Must
RD-3433	35.1.0-2.0-1	The system shall have the capability to deliver pre-ingest bundles that support the creation of removable digital media.	R1B; Must
RD-3434	35.1.0-2.0-2	The system shall have the capability to deliver DIPs that support the creation of removable optical digital media.	R1C; Must
RD-3435	35.1.0-2.0-2.0-1	The system shall have the capability to deliver pre-ingest bundles that support the creation of removable optical digital media.	R1C; Must
RD-3436	35.1.0-2.0-2.0-2	The system shall have the capability to deliver pre-ingest bundles that support the creation of Compact Discs (CD).	R1C; Must
RD-3437	35.1.0-2.0-2.0-2.0-1	The system shall have the capability to deliver and DIPs that support the creation of Compact Discs (CD).	R1C; Must
RD-3438	35.1.0-2.0-2.0-3	The system shall have the capability to deliver pre-ingest bundles that support the creation of Digital Versitile Disc (DVD) .	R1C; Must
RD-3439	35.1.0-2.0-2.0-3.0-1	The system shall have the capability to deliver DIPs that support the creation of Digital Versital Discs (DVD).	R1C; Must
RD-3440	35.1.0-2.0-2.0-4	The system shall have the capability to deliverDIPs that support the creation of Blue Ray Discs (BD).	R3; Could
RD-3441	35.1.0-2.0-2.0-5	The system shall have the capability to deliver pre-ingest bundles that support the creation of Blue Ray Discs (BD).	R3; Could
RD-3442	35.1.0-3	The system shall have the capability to deliver pre ingest bundles and DIPs that are portable (i.e. can be viewed on other systems) via removable magnetic digital media supported by the client environment.	R1C; Must
RD-3443	35.1.0-3.0-1	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e. can be viewed on other systems) via magnetic tapes supported by the client environment.	R1C; Must
RD-3444	35.1.0-3.0-2	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e. can be viewed on other systems) via magnetic hard disks supported by the client environment.	R1C; Must
RD-3445	35.1.0-3.0-3	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e. can be viewed on other systems) via magnetic floppy disks supported by the client environment.	R1C; Must
RD-3446	35.1.0-3.0-4	The system shall have the capability to deliver DIPs that are portable (i.e. can be viewed on other systems) via magnetic tapes supported by the client environment.	R1B; Must
RD-3447	35.1.0-3.0-5	The system shall have the capability to deliver DIPs that are portable (i.e. can be viewed on other systems) via magnetic hard disks supported by the client environment.	R1B; Must
RD-3448	35.1.0-3.0-6	The system shall have the capability to deliver DIPs that are portable (i.e. can be viewed on other systems) via magnetic floppy disks supported by the client environment.	R1B; Must
RD-3449	35.1.0-4	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e. can be viewed on other systems) via removable semiconductor digital media supported by the client environment.	R1C; Must
RD-3450	35.1.0-4.0-1	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e. can be viewed on other systems) via Universal Serial Bus (USB) flash drives supported by the client environment.	R1C; Must
RD-3451	35.1.0-4.0-2	The system shall have the capability to deliver pre-ingest bundles that are portable (i.e. can be viewed on other systems) via flash memory cards supported by the client environment.	R1C; Must
RD-3452	35.1.0-4.0-3	The system shall have the capability to deliver DIPs that are portable (i.e. can	R1B; Must

		be viewed on other systems) via Universal Serial Bus (USB) flash drives supported by the client environment.	
RD-3453	35.1.0-4.0-4	The system shall have the capability to deliver DIPs that are portable (i.e. can be viewed on other systems) via flash memory cards supported by the client environment.	R1B; Must
RD-3454	35.1.0-5	The system shall have the capability to generate image files that can be used to duplicate/replicate the content that will be stored on removable digital media.	R1C; Could / R2; Should
RD-3455	35.1.0-5.0-1	The system shall have the capability to generate ISO image files.	R1C; Could / R2; Should
RD-3456	35.1.0-5.0-2	The system shall have the capability to generate VCD image files.	R1C; Could / R2; Should
RD-3457	35.1.0-5.0-3	The system shall have the capability to generate UDF image files.	R1C; Could / R2; Should
RD-3458	35.1.0-6	The system shall have the capability to generate autorun files for use on removable digital media.	R1C; Could / R2; Should
RD-3459	35.1.0-6.0-1	Users shall have the capability to specify the file that will open when the removable digital media is inserted into a computer.	R1C; Could / R2; Should
RD-3460	35.1.0-7	The system shall have the capability to deliver DIPs and pre-ingest bundles to digital media.	R1C; Could / R2; Should
RD-3461	35.1.0-7.0-1	The system shall have the capability to deliver DIPs and pre-ingest bundles to GPO storage devices. (e.g., GPO servers).	R1C; Must
RD-3462	35.1.0-7.0-1.0-1	The system shall have the capability to deliver DIPs to GPO storage devices.	R1C; Must
RD-3463	35.1.0-7.0-1.0-2	The system shall have the capability to deliver PIBs to GPO storage devices.	R1C; Must
RD-3464	35.1.0-7.0-2	The system shall have the capability to deliver DIPs and pre-ingest bundles to non-GPO storage devices. (e.g., customer servers, service provider servers)	R1C; Must
RD-3465	35.1.0-7.0-2.0-1	The system shall have the capability to deliver DIPs to non-GPO storage devices.	R1C; Must
RD-3466	35.1.0-7.0-2.0-2	The system shall have the capability to deliver PIBs to non-GPO storage devices.	R1C; Must
RD-3467	35.1.0-7.0-3	The system shall have the capability to deliver DIPs and pre-ingest bundles to non-desktop electronic devices, including, but not limited to: · Personal digital assistants (PDAs) · Digital audio players · Electronic books (E-Books) · Cell phones	R2; Should / R3; Must
RD-3468	35.1.0-7.0-3.0-1	The system shall have the capability to deliver DIPs to Digital Assistants (PDAs).	R2; Should / R3; Must
RD-3469	35.1.0-7.0-3.0-2	The system shall have the capability to deliver DIPs to Digital Audio Players.	R2; Should / R3; Must
RD-3470	35.1.0-7.0-3.0-3	The system shall have the capability to deliver DIPs to Electronic Books (E-Books).	R2; Should / R3; Must
RD-3471	35.1.0-7.0-3.0-4	The system shall have the capability to deliver DIPs to Cell Phones.	R2; Should / R3; Must

Appendix A – References

Adobe Systems Incorporated. Encapsulated PostScript File Format Specification Version 3.0. Mountain View, CA: Adobe Systems Incorporated .1 May 1992.

Adobe Systems Incorporated. PDF Reference, Fifth Edition, Version 1.6. Mountain View, CA: Adobe Systems Incorporated. Nov. 2004.

Adobe Systems Incorporated. TIFF – Revision 6.0. Mountain View, CA: Adobe Systems Incorporated. 3 June 1992.

American National Standards Institute. Audio Recording – Compact disc digital audio system. (IEC 60908 Ed. 2.0). 1999.

American National Standards Institute. Information Systems - Coded Character Sets - 7-Bit American National Standard Code for Information Interchange (7-Bit ASCII). (ANSI INCITS 4-1986 (R2002)). American National Standards Institute. 2002.

American National Standards Institute. Triple Data Encryption Algorithm Modes of Operation (TDES) (ANSI X9.52-1998). ANSI, 1998.

Association for Automatic Identification and Mobility. ANSI/AIM BC1-1995, Uniform Symbology Specification - Code 39. AIM. 20 Mar. 2006 <http://www.aimglobal.org/aimstore/linearsymbologies.asp>. (Reference only. Bar Coding Digital Conversions Service Tracking)

Australia. National Library of Australia. “Emulation.” Preserving Access to Digital Information. 29 Mar. 2006. <http://www.nla.gov.au/padi/topics/19.html>.

Berners-Lee, T, R. Fielding, and L. Masinter. 3986 Uniform Resource Identifier (URI): Generic Syntax. T. Jan. 2005.

Blanchette, J.-F., "The Digital signature dilemma", Annals of Telecommunications (accepted with revisions).<http://polaris.gseis.ucla.edu/blanchette/papers/annals.pdf>. (PDF preprint)

Bradley, Jim. New Imprint Line Announcement. May 2 2005. GPO. 22 Mar 2006 <http://www.gpo.gov/bidupdates/pdfs/GPOimprint.pdf>

Brauer, Michael, Patrick Durusau, and Gary Edwards. New Imprint Line Announcement Office Applications (OpenDocument) v1.0. May 2005. OASIS. 22 Mar 2006. <http://www.oasis-open.org/committees/download.php/12572/OpenDocument-v1.0-os.pdf>.

Brauer, Michael, Patrick Durusau, Gary Edwards, et al. OpenDocument Format for Office Applications (OpenDocument) v1.0. Organization for the Advancement of Structured Information Standards. 1 May 2005.

CENDI Persistent Identification Task Group. Persistent Identification: A Key Component of an E-Government Infrastructure. 2004.

Center for Internet Security. Benchmarks, CIS. 22 Mar 2006. <http://www.cisecurity.org/bench.html>.

Coalson, Josh. Free Lossless Audio Codec. 2004. 23 March 2006. <http://flac.sourceforge.net>

Collaborative Digitization Project Scanning Working Group. General Guidelines for Scanning. Spring 1999. Collaborative Digitization Project. 22 Mar 2006 <http://www.cdpheritage.org>.

CompuServe Incorporated. Graphics Interchange Format: Version 89a. Columbus, OH: CompuServe Incorporated. 31 July 1990.

Computer Security Division. Standards for Security Categorization of Federal Information and Information Systems: Federal Information Processing Standards Publication 199. Feb 2004. National Institute

of Standards and Technology. 22 Mar 2006. <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>.

Consultative Committee for Space Data Systems. Reference Model for an Open Archival Information System (OAIS). Washington, DC: 2002. 29 Mar. 2006. <http://public.ccsds.org/publications/archive/650x0b1.pdf>.

Cornell University Library. Digital Preservation Strategies. 2003. Digital Preservation Management: Implementing Short-term Strategies for Long-term Problems. 29 Mar. 2006 <http://www.library.cornell.edu/iris/tutorial/dpm/terminology/strategies.html>.

Cornwell Consultants in Management and IT. Model Requirements for the Management of Electronic Records (MoReq). 2001. Electronic Document and Records Management (EDRM). 29 Mar. 2006. <http://www.cornwell.co.uk/moreq>.

Data Documentation Initiative Alliance. Data Documentation Initiative. 22 Mar. 2006 <http://www.icpsr.umich.edu/DDI/>.

Digital Imaging Working Group. Western States Digital Imaging Best Practices Version 1.0. Jan 2003. Western States Digital Standards Group. 22 Mar 2006 <http://www.cdpheritage.org/digital/scanning/documents/WSDIBP_v1.pdf>.

Digital Library Federation Benchmark Working Group. Benchmark for Faithful Digital Reproductions of Monographs and Serials. Dec. 2002. Digital Library Federation. 29 Mar. 2006. <http://www.diglib.org/standards/bmarkfin.htm>.

Dublin Core Metadata Initiative. [Website]. 13 Mar. 2006. 22 Mar. 2006 <http://dublincore.org/>.

Eastlake 3rd, D., J. Reagle J., and D. Solo, "(Extensible Markup Language) XML-Signature Syntax and Processing." RFC 3275. March 2002.

Eastlake 3rd, D., J. Reagle J., and D. Solo. "XML Encryption Syntax and Processing." December 2002. <http://www.w3.org/TR/2001/RED-xmlenc-core-20021210/>.

Eastlake 3rd, D., J. Reagle, and D. Solo. "XML-Signature Syntax and Processing. "XMLDSIG. February 2002. <http://www.w3.org/TR/xmldsig-core/>.

Ex Libris. MetaLib. MetaLib, The Library Portal, Ex Libris Group. 29 Mar. 2006. <http://www.exlibrisgroup.com/metalib.htm>.

Ex Libris. SFX Overview. SFX Context Sensitive Linking, Ex Libris Group. 29 Mar. 2006. <http://www.exlibrisgroup.com/sfx.htm>.

Experts on Digital Preservation. Report from the Meeting of Experts on Digital Preservation. March 12, 2004. GPO <http://www.gpoaccess.gov/about/reports/preservation2.pdf>.

Farquhar, Adam, and Sean Martin, Richard Boulderstone, Vince Dooher, Richard Masters, and Carl Wilson. Design for the Long Term: Authenticity and Object Representation. Boston Spa: United Kingdom. The British Library, 2005. <http://www.bl.uk/about/policies/dom/pdf/archiving2005l.pdf>.

Federal Emergency Management Agency. Federal Preparedness Circular 65 (FPC 65). Jul 1999. FEMA. 22 Mar 2006 <http://www.fas.org/irp/offdocs/pdd/fpc-65.htm>.

Federal Geographic Data Committee. Content Standard for Digital Geospatial Metadata. 1998. 22 Mar. 2006 <http://www.fgdc.gov/standards/standards_publications/>.

Ferraiolo, Jon, Dean Jackson, and Fujisawa Jun. Scalable Vector Graphics (SVG) 1.1 Specification. World Wide Web Consortium. 14 Jan. 2003.

Foundations for Technical Standards. 1999. Image Permanence Institute, Rochester Institute of Technology. 22 Mar 2006 <http://www.rit.edu/~661www1/sub_pages/digibook.pdf>.

Freed, N, and Borenstein, N. Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples (IETF RFC 2049). Nov. 1996.
The Internet Engineering Task Force, Network Working Group.

Freed, N., J. Klensin, and J. Postel. Multipurpose Internet Mail Extensions (MIME) Part Four: Registration Procedures (IETF RFC 2048). Nov. 1996.
The Internet Engineering Task Force, Network Working Group.

Frey, Franziska, and James Reilly. Digital Imaging for Photographic Collections

Garrett, John. Important Concepts from the draft ISO standard Reference Model for an Open Archival Information System (OAIS). College Park, MD: National Archives and Records Administration, 1998. 21 Mar. 2006. <http://nost.gsfc.nasa.gov/isoas/dads/OAISOverview.html>.

Grance, Tim, Joan Hash, and Marc Stevens. Security Considerations in the Information Systems Development Lifecycle: NIST Special Publication 800-64, Rev. 1. Jun 2004. National Institute of Standards and Technology. 22 Mar 2006. <http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf>.

Granger, Stewart. "Emulation as a Digital Preservation Strategy." D-Lib Magazine Oct 2000. 29 Mar. 2006. <http://www.dlib.org/dlib/october00/granger/10granger.html>.

IBM. Business Process Execution Language for Web Services version 1.1. 30 Jul. 2002. IBM. 20 Mar. 2006 <http://www-128.ibm.com/developerworks/library/specification/ws-bpel/>.

Information Technology Laboratory. Security Requirements for Cryptographic Modules: Federal Information Processing Standards Publication 140-2. May 2001. National Institute of Standards and Technology. 22 Mar 2006. <http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

International Cooperation for the Integration of Processes in Prepress, Press and Postpress (CIP4).Job Definition Format Specification, Release 1.3, 2005. <http://www.cip4.org>

International Organization for Standardization Committee JTC 1/SC 2. Information Technology -- Universal Multiple-Octet Coded Character Set (ISO/IEC 10646:2003). International Organization for Standardization, 2003.

International Organization for Standardization Committee JTC 1/SC 29. Information technology -- Digital compression and coding of continuous-tone still images: Requirements and guidelines (ISO/IETC 10918-1: 1994). International Organization for Standardization, 1994.

International Organization for Standardization Committee JTC 1/SC 29. Information technology -- Coding of moving pictures and associated audio for digital storage media at up to about 1,5 Mbit/s -- Part 3: Audio (ISO/IEC 11172-3:1993). International Organization for Standardization, 1993.

International Organization for Standardization Committee JTC 1/SC 29. Information technology -- JPEG 2000 image coding system -- Part 6: Compound image file format (ISO/IEC 15444-6:2003). International Organization for Standardization, 2003.

International Organization For Standardization. ISO 17421:2003 Space Data and Information Transfer Systems -- Open Archival Information System -- Reference Model. International Organization for Standardization, 2003. 22 Mar. 2006 <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=24683&ICS1=49&ICS2=140&ICS3>.

International Telephone Union (ITU). Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services: ITU X.500. Feb 2001. ITU.

International Telephone Union (ITU). Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks: ITU X.509. Mar 2000. ITU.

ITU-T. ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework(Certificate Format Standard). June 1997.

J. Jonsson and B. Kaliski. RFC 3447. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1. IETF. February 2003. <http://www.ietf.org/rfc/rfc3447.txt>.

J. Postel and Reynolds, J. File Transfer Protocol (IETF RFC 959). Oct. 1985.

Joint Photographic Experts Group. "JPEG 2000:Our New Standard." JPEG [Website]. 2004. 22 Mar. 2006 <http://www.jpeg.org/jpeg2000/index.html>.

Koyani, 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.<http://usability.gov/pdfs/guidelines.html>.

Kuhn, D. Richard, Vincent Hu, W. Timothy Polk, and Shu-Jen Chang. Introduction to Public Key Technology and the Federal PKI Infrastructure: NIST Special Publication 800-32. Feb 2001. National Institute of Standards and Technology. 22 Mar 2006. <http://www.csrc.nist.gov/publications/nistpubs/800-32/sp800-32.pdf>.

Lavoie, Brian. The Open Archival Information System Reference Model: Introductory Guide. Dublin, Ohio: OCLC Online Computer Library Center, Inc., 2004. 21 Mar. 2006. <http://www.dpconline.org/docs/lavoie_OAIS.pdf>.

Lynch, Patrick J., Sarah Horton, Web Style Guide 2nd Edition, New Haven, CT: Yale University Press, 2001. <http://www.webstyleguide.com/>.

Maler, Eve, John Cowan, Jean Paoli, et al. Extensible Markup Language (XML) 1.1. World Wide Web Consortium. 4 Feb. 2004.

Moats, R. 2141 URN Syntax. May 1997.

Moore, K. MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text (IETF RFC 2047). Nov. 1996.
The Internet Engineering Task Force, Network Working Group.

Network Working Group. Lightweight Directory Access Protocol (LDAP) v.3. Dec 1997. Internet Engineering Task Force (IETF). 22 Mar 2006 <http://www.ietf.org/rfc/rfc2251.txt>.

Network Working Group. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1 – IETF RFC 3447. Feb 2003. RSA Laboratories. 22 Mar 2006 <http://www.ietf.org/rfc/rfc3447.txt>.

NISO Framework Advisory Group. A Framework of Guidance for Building Good Digital Collections, 2nd edition. 2004. National Information Standards Organization. 22 Mar 2006 <http://www.niso.org/framework/framework2.pdf>.

OCLC Worldwide. PREMIS (Preservation Metadata: Implementation Strategies) Working Group. 29 Mar. 2006. <http://www.oclc.org/research/projects/pmwg/>.

Office of Management and Budget. Management of Federal Information Resources: Circular A-130. OMB 22 Mar 2006 <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>.

Open eBook Forum. Open eBook Publication Structure Specification Version 1.2. 27 August 2002. 23 March 2006. <http://www.idpf.org/oebps/oebps1.2/download/oeb12.pdf>

Organisation Internationale de Normalisation. ISO/IEC JTC1/SC29/WG11 Coding of Moving Pictures and Audio. MPEG-21 Overview V.5. Oct. 2002. 22 Mar. 2006 <http://www.chiariglione.org/mpeg/standards/mpeg-21/mpeg-21.htm>.

Pemberton, Steven. XHTML™ 1.0 The Extensible HyperText Markup Language (Second Edition). World Wide Web Consortium.1 Aug. 2002.

PKIX Working Group. Public Key Infrastructure Exchange (PKIX). Dec 2005. Internet Engineering Task Force (IETF). 22 Mar 2006. <http://www.ietf.org/html.charters/pkix-charter.html>.

Postel, Jonathan. Simple Mail Transfer Protocol (IETF RFC 821). Marina del Rey, CA: Information Sciences Institute. Aug. 1982. The Internet Engineering Task Force, Network Working Group.

Preservation Metadata Implementation Strategies (PREMIS) Working Group. Data Dictionary for Preservation Metadata: Final Report of the PREMIS Working Group. May 2005. 22 Mar. 2006 <http://www.oclc.org/research/projects/pmwg/premis-final.pdf>.

Preservation Metadata Implementation Strategies (PREMIS) Working Group. Official Web Site. 7 Feb. 2006. 22 Mar. 2006 <http://www.loc.gov/standards/premis/>.

Puglia, Steven, Reed, Jeffrey, and Rhodes, Erin. Technical Guidelines for Digitizing Archival Materials for Electronic Access: Creation of Production Master Files-Raster Images. Jun 2004. United States. National Archives and Records Administration (NARA), 22 Mar 2006. <http://www.archives.gov/research/arc/digitizing-archival-materials.pdf>.

Purvis, Lisa. A Genetic Algorithm Approach to Automated Custom Document Assembly. Xerox Corporation, 2003.

R. Housley, W. Ford, W. Polk, D. Solo. Internet X. 509 Public Key Infrastructure Certificate and CLR Profile (IETF PKIXX.509 v3). RFC 3280. Internet Engineering Task Force (IETF), April 2002. <http://www.ietf.org/rfc/rfc3280.txt>.

R. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21 (2), pp.120–126. 1978. Previously released as an MIT "Technical Memo" in April 1977. Initial publication of the *RSA* scheme.

Raggett, David, Arnaud Le Hors, and Ian Jacobs. HTML 4.01 Specification. World Wide Web Consortium. 24 December 1999.

Resnick, P. Internet Message Format (IETF RFC 2822). The Internet Society. Apr. 2001. The Internet Engineering Task Force, Network Working Group.

Ross, Ron, Stu Katzke, and Arnold Johnson. Recommended Security Controls for Federal Information Systems: NIST Special Publication SP 800-53. Feb 2005. National Institute of Standards and Technology. 22 Mar 2006. <http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf>.

RSA Security Inc. Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications. Version 2.1. February 2003.

RSA Security Inc. Public-Key Cryptography Standards (PKCS) #11: Cryptographic Token Interface Standard. Version 2.20. June 2004.

RSA Security Inc. Public-Key Cryptography Standards (PKCS) #12: Personal Information Exchange Syntax Standard. Version 1.0, June 1999.

RSA Security Inc. Public-Key Cryptography Standards (PKCS) #7: Cryptographic Message Syntax Standard. Version 1.4. June 1991.

SANS Institute. Configuration Benchmarks. SANS. 22 Mar 2006 <http://www.sans.org>.

Security Services Technical Committee (SSTC). Security and Access Markup Language (SAML) v.2. Mar 2005. OASIS. 22 Mar 2006 <http://www.oasis-open.org/specs/index.php#samlv2.0>.

Social Security Administration, SSA Privacy Policy. SSA. 22 Mar 2006 <http://www.ssa.gov/privacy.html>.

Society of American Archivists. "EAD Application Guidelines for Version 1.0." Library of Congress. 01 Nov. 2000. Library of Congress 21 Mar. 2006 < http://www.loc.gov/ead/ag/agcontxt.html>.

Sollins, K and L. Masinter. RFC 1737 Functional Requirements for Uniform Resource Names. Dec. 1994.

Swanson, Marianne, Joan Hash, and Pauline Bowen. Guide for Developing Security Plans for Federal information Systems: NIST Special Publication 800-18. Feb 2006. National Institute of Standards and Technology. 14 Mar 2006.<http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf>.

Swanson, Marianne. Security Self-Assessment Guide for Information Technology Systems: NIST Special Publication 800-26.Nov. 2001. National Institute of Standards and Technology. 14 Mar. 2006 <http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>.

Technical Advisory Service for Images. Establishing a Digital Preservation Strategy. Technical Advisory Service for Images. 29 Mar 2006. <http://www.tasi.ac.uk/advice/delivering/digpres2.html>.

Text Encoding Initiative. [Website]. 22 Mar. 2006 <http://www.tei-c.org/>.

Thatcher, Jim, Michael Burks, Sarah Swierenga, Cynthia Waddell, Bob Regan, Paul Bohman, Shawn Lawton Henry, Mark Urban, Constructing Accessible Web Sites, United States: Glasshaus, 2002.

The Digital Library Federation Benchmark Working Group (2001-2002). Benchmark for Faithful Digital Reproductions of Monographs and Serials v.1. Dec 2002. Digital Library Federation. 22 Mar 2006 <http://www.diglib.org/standards/bmarkfin.pdf>.

The Netherlands. National Archives and the Ministry of the Interior and Kingdom Relations. Emulation: Context and Current Status, Digital Preservation Testbed White Paper. Jun 2003. Digital Preservation Testbed. The Haag: 29 Mar. 2006. <http://www.digitaleduurzaamheid.nl/bibliotheek/docs/White_paper_emulation_UK.pdf>.

The Unicode Consortium. The Unicode Standard, Version 4.0. Boston, MA, Addison-Wesley Developers Press, 2003.

Transport Layer Security Working Group. The Secure Sockets Layer (SSL) Protocol Version 3.0.Nov 1996. Internet Engineering Task Force (IETF). 22 Mar 2006. <http://wp.netscape.com/eng/ssl3/draft302.txt>.

Transport Layer Security Working Group. Transport Layer Security (TLS). Feb 2002. Internet Engineering Task Force (IETF). 22 Mar 2006.<http://www.ietf.org/html.charters/tls-charter.html>.

United Kingdom. National Archives. "The PRONOM Technical Registry." The National Archives. The U.K. National Archives. 21 Mar. 2006. <http://www.nationalarchives.gov.uk/aboutapps/pronom/default.htm>.

United States. Congress. "Records Maintained on Individuals." Title 5 United States. Code, Sec. 552a. Jan 7, 2003.

United States. Congress. "Access to Federal Electronic Information" Title 44 U.S. Code, Chapter 41, 2000 edition

United States. Congress. "Records About Individuals: Privacy Act." Title 5 U.S. Code, Sec. 552a (2000).

United States. Congress. "Vocational Rehabilitation and Other Rehabilitation Services--Rights and Advocacy" Title 29 U.S. Code Chapter 16, Subchapter V", 2000 edition.

United States. Congress. " Electronic and Information Technology Accessibility Standards" Title 36 Code of Federal Regulations, Chapter 11, Part 1194, 2004 edition.

United States. Congress. "E-Government Act of 2002" (PL 107-347, 17 Dec. 2002). United States. Statutes at Large 116(2002): 2899.

United States. Congress." Depository Library Program" Title 44 U.S. Code, Chapter 19, 2000 edition.

United States. Congress." Distribution and Sale of Public Documents" Title 44 U.S. Code, Chapter 17, 2000 edition.

United States. Department of Justice. Information Technology and People with Disabilities: The Current State of Federal Accessibility. Washington, DC: U.S. Department of Justice. 2000. <http://www.usdoj.gov/crt/508/report/content.htm>.

United States. Department of the Treasury. IRS Privacy Policy. IRS. 22 Mar 2006 <http://www.irs.gov/privacy/index.html>.

United States. General Accounting Office. Internet Privacy: Agencies Efforts to Implement OMB's Privacy Policy (GAO/GGD-00-191). Washington, DC: General Accounting Office, 2000. 21 Mar. 2006 <http://www.gao.gov/new.items/d03304.pdf>.

United States. General Services Administration "Section 508 Acquisition FAQ's." Section508.gov 2002. General Services Administration. 20 March 2006. <http://www.section508.gov/index.cfm?FuseAction=Content&ID=75>.

United States. Government Accounting Office. Internet Privacy -- Agencies' Efforts to Implement OMB's Privacy Policy: GAO/GGD-00-191. Sep 2000. GAO. 22 Mar 2006 <http://www.gao.gov/new.items/gg00191.pdf>.

United States. Government Printing Office. "FDLP Selection Mechanisms: Item Numbers and Alternatives." FDLP Desktop. 14 February 2006. Government Printing Office. 14 March 2006. <http://www.access.gpo.gov/su_docs/fdlp/selection/index.html>

United States. Government Printing Office. "FDLP Guidelines for Determining Supersede Materials." *GPO Access*. 10 Jun. 2004. U.S. Government Printing Office 21 Mar. 2006 <http://www.access.gpo.gov/su_docs/fdlp/coll-dev/supersede.html>.

United States. Government Printing Office. "GPO Access Web Design." GPO Instruction 705.27. Washington, D.C.: U.S. Government Printing Office, 2003.

United States. Government Printing Office. "Legal Information." *GPO Access*. 27 Sep. 2003. U.S. Government Printing Office. 21 Mar. 2006 <http://www.gpoaccess.gov/about/legal.html>.

United States. Government Printing Office. *Requirements Document (RD V2.1) for the Future Digital System*. 18 Apr. 2006. U.S. Government Printing Office. 12 Oct. 2006 < http://www.gpo.gov/projects/pdfs/FDsys_RD_v2.1.pdf>.

United States. Government Printing Office. A Strategic Vision for the 21st Century. Washington: U.S. Government Printing Office, 2004. <http://www.gpo.gov/congressional/pdfs/04strategicplan.pdf>

United States. Government Printing Office. Authentication White Paper. Washington: U.S. Government Printing Office, 2005. <http://www.gpoaccess.gov/authentication/AuthenticationWhitePaperFinal.pdf>.

United States. Government Printing Office. Concept of Operations for the Future Digital System V2.0. 16 May 2005. 22 Mar. 2006 <http://www.gpo.gov/projects/pdfs/FDsys_ConOps_v2.0.pdf>.

United States. Government Printing Office. Government Printing Office Style Manual. 2000.

United States. Government Printing Office. GPO Access Biennial Report to Congress. Washington: U.S. Government Printing Office, 2000.

United States. Government Printing Office. GPO Contract Terms: GPO Publication 310.2. Jun 2001. GPO. 22 Mar 2006 <http://www.gpo.gov/printforms/pdf/terms.pdf>.

United States. Government Printing Office. GPO Form 714 - Record of Visit, Conference, Telephone Call. Washington, DC: Government Printing Office. Feb. 1991.

United States. Government Printing Office. GPO METS Profile. <to be developed>.

United States. Government Printing Office. ILS Statement of Work, Request for Information, and Related Files. U.S. Government Printing Office Jan. 2004 (unpublished 2 CD set).

United States. Government Printing Office. Information Technology Security Program Statement of Policy: GPO Publication 825.33. Jul 2004.GPO.

United States. Government Printing Office. List of Classes of United States. Government Publications Available for Selection by Depository Libraries. October 2005 issue. Washington: Government Printing Office, 2005. <http://www.access.gpo.gov/su_docs/fdlp/pubs/loc/index.html>

United States. Government Printing Office. Oracle Legacy Administrative Systems Replacement Concept of Operations (GPO-OA-OCIO-00001-CONPOS). Mar. 2004.

United States. Government Printing Office. Printing Procurement Regulation: GPO Publication 305.3. May 1999. GPO. 22 Mar 2006 <http://www.gpo.gov/printforms/pdf/ppr.pdf>.

United States. Government Printing Office. Quality Assurance through Attributes Program (QATAP): GPO Publication 310.1. Aug 2002. GPO. 22 Mar 2006 <http://www.gpo.gov/printforms/pdf/qatap.pdf>.

United States. Government Printing Office. The Guidelines - Best Practices for Submitting Electronic Design & Prepress Files: GPO Publication 300.6. Jul 2004. GPO. 22 Mar 2006. <http://www.gpo.gov/forms/pdfs/3006_10_2004.pdf>.

United States. Government Publishing Services Opportunity Request for Information: Solicitation 01: Solicitation number: Reference-Number-ID2005. 21 October 2005. <http://www.fbo.gov>.

United States. Internal Revenue Service. "IRS Privacy Policy." Internal Revenue Service. U.S. Internal Revenue Service. 21 Mar. 2006 <http://www.irs.gov/privacy/index.html>.

United States. Library of Congress. Archival Information Package (AIP) Design Study. Library of Congress. Washington, D.C.: Library of Congress, 2001. 15 Mar. 2006 <http://www.loc.gov/rr/mopic/avprot/AIP-Study_v19.pdf>.

United States. Library of Congress. METS Metadata Encoding & Transmission Standard Official Web Site. 9 Mar. 2006. Library of Congress. Network Standards and MARC Development Office. 15 Mar. 2006 <http://www.loc.gov/standards/mets/>.

United States. Library of Congress. MODS Metadata Object Description Schema Official Website. 9 Sept. 2005. Library of Congress. Network Standards and MARC Development Office. 15 Mar. 2006 <http://www.loc.gov/standards/mods/>.

United States. Library of Congress. National Digital Information Infrastructure and Preservation Program (NDIIPP). The Library of Congress Digital Preservation. 29 Mar. 2006. <http://www.digitalpreservation.gov>.

United States. Library of Congress. Network Development and MARC Standards Office. Encoded Archival Description (EAD). 14 Nov. 2005. 22 Mar. 2006 <http://www.loc.gov/ead/>.

United States. Library of Congress. Network Development and MARC Standards Office. MIX NISO Metadata for Images in XML Standard Official Web Site. 30 Aug. 2005. 22 Mar. 2006 <http://www.loc.gov/standards/mix/>.

United States. National Archives and Records Administration Program Management Office. Electronic Records Archives (ERA) Concept of Operations (CONOPS v 4.0). 27 Jul. 2004. National Archives and Records Administration. 29 Mar. 2006. <http://www.archives.gov/era/pdf/concept-of-operations.pdf>.

United States. National Archives and Records Administration. "Electronic and Information Technology Accessibility Standards" Title 36 Code of Federal Regulations, Chapter 21, Part 1194, 2005 edition.

United States. National Archives and Records Administration. "Federal Acquisition Regulations" Title 48 Code of Federal Regulations, 2005 edition.

United States. National Archives and Records Administration. Trustworthy Repositories Audit & Certification: Criteria and Checklist. College Park, MD: 2005. Research Libraries Group. Feb. 2007 <http://www.crl.edu/content.asp?l1=13&l2=58&l3=162&l4=91>.

United States. National Archives and Records Administration. Records Management Guidance for Agencies Implementing Electronic Signature Technologies. Washington: U.S., 2000. <http://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html>.

United States. National Institutes of Standards and Technology. Advanced Encryption Standard (AES): Federal Information Processing Standards Publication 197. Nov 2001. NIST. 22 Mar 2006 <http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>.

United States. National Institutes of Standards and Technology. Bibliographic References (ANSI/NISO Z39.29). 9 Jun. 2005. NIST. 29 Mar 2006 <http://www.niso.org/standards/resources/Z39-29-2005.pdf>.

United States. National Institutes of Standards and Technology. Dublin Core Metadata Element Set. (Z.39.85). NIST. 26 Mar 1999.

United States. National Institutes of Standards and Technology. Federal Information Processing Standard Publication 197 (FIPS 197). Advanced Encryption Standard (AES). NIST. November 2001. <http://csrc.nist.gov/publications/fips/index.html>

United States. National Institutes of Standards and Technology. Federal Information Processing Standard Publication 198, The Keyed-Hash Message Authentication Code, NIST, March 6, 2002.

United States. National Institutes of Standards and Technology. Federal Information Processing Standard Publication 180-2, Secure Hash Standard (SHS), NIST, August 2002. <http://csrc.nist.gov/publications/fips/index.html>.

United States. National Institutes of Standards and Technology. Holding Statements for Bibliographic Items (Z.39.71). 13 Apr. 1994. NIST. 26 Mar 1999. <http://www.niso.org/standards/resources/Z39-71.pdf>.

United States. National Institutes of Standards and Technology. Information Interchange Format (ANSI/NISO Z39.2). 13 Apr. 1994. NIST. 29 Mar 2006 <http://www.niso.org/standards/resources/Z39-2.pdf>.

United States. National Institutes of Standards and Technology. Information Retrieval: Application Service Definition & Protocol Specification (Z.39.50). 27 Nov. 2002. NIST. 29 Mar 2006 <http://www.niso.org/standards/resources/Z39-50-2003.pdf>.

United States. National Institutes of Standards and Technology. International Standard Serial Numbering (ISSN) (ANSI/NISO Z39.9). 20 Jan. 1992. NIST. 29 Mar 2006 < http://www.niso.org/standards/resources/Z39-9.pdf>.

United States. National Institutes of Standards and Technology. Message Authentication Code (MAC) Validation System - Requirements and Procedures: Standards Publication 500-156. NIST. May 1988.

United States. National Institutes of Standards and Technology. Public Key Interoperability Test Suite (PKITS), Certification Path Validation, NIST, September 2, 2004.

United States. National Institutes of Standards and Technology. Record Format for Patron Records. (Z.39.69). 13 Apr. 1994. NIST. 26 Mar 1999. <http://www.niso.org/standards/resources/Z39-71.pdf>.

United States. National Institutes of Standards and Technology. Secure Hash Standard (SHS): Federal Information Processing Standards Publication 180-2. Aug 2001. NIST. 22 Mar 2006 <http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf>.

United States. National Institutes of Standards and Technology. Serial Item and Contribution Identifier (SICI) Z.39.56). 13 Apr. 1994. NIST. 29 Mar 2006 <http://www.niso.org/standards/resources/Z39-2.pdf>.

United States. National Institutes of Standards and Technology. Space Data and Information Transfer Systems – Open Archival Information System, -- Reference Model (ISO 14721). 24 Feb. 2006. NIST. 29 Mar 2006.

United States. National Institutes of Standards and Technology. Standard Address Number (SAN) for the Publishing Industry (Z.39.43). 28 Jan. 1993. NIST. 29 Mar 2006 <http://www.niso.org/standards/resources/Z39-43.pdf>.

United States. National Institutes of Standards and Technology. System Questionnaire with NIST SP 800-53 References and Associated Security Control Mappings. Apr 2005. National Institute of Standards and Technology. 14 Mar 2006 <http://csrc.nist.gov/publications/nistpubs/>.

United States. Office of Personnel Management, OPM Web Privacy Policy. OPM. 22 Mar 2006 <http://www.opm.gov/html/privacy.asp>.

United States. Social Security Administration. "Our Internet Privacy Policy." Social Security Online. U.S. Social Security Administration. 21 Mar. 2006 <http://www.ssa.gov/privacy.html>.

United States. Government Printing Office. GPO's Press Optimized PDF Settings. GPO. 18 April 2006.<http://www.gpo.gov/epub/files/AcrobatDistiller-JobOptions.zip>

Virtual Private Network Consortium. IPSEC Virtual Private Network (VPN). <http://www.vpnc.org/vpn-standards.html>.

W3C. "Web content accessibility guidelines 1.0." World Wide Web Consortium. 1999. W3C. 20 March 2006. <http://www.w3.org/TR/WCAG10/>.

W3C. World Wide Web Consortium (W3C) Guidelines. 2006. World Wide Web Consortium. 20 March 2006. <http://www.w3.org/>.

Winder, Dave. RSS 2.0 Specification. Berkman Center for Internet & Society at Harvard Law School 15 July 2003.

Workflow Management Coalition. Process Definition Interface -- XML Process Definition Language. 3 Oct. 2005. Workflow Management Coalition. 20 Mar. 2006 <http://www.wfmc.org/standards/docs/TC-1025_xpdl_2_2005-10-03.pdf>.

Xiph.org Foundation. "Vorbis I Specification". Xiph.org: Documentation. 20 July 2004. Xiph.org Foundation. 23 March 2006. <http://www.xiph.org/vorbis/doc/Vorbis_I_spec.html>

Yergeau, Francois, and Others. Extensible Markup Language (XML) 1.0. 3rd ed. W3C (World Wide Web Consortium), 2004. W3C Recommendation 04 February 2004. 22 Mar. 2006 <http://www.w3.org/TR/2004/REC-xml-20040204>.

Appendix B – Acronyms and Glossary

Acronyms

ACRONYM	DEFINITION
ABLS	Automated Bid List System
ACES	Access Certificates for Electronic Services
ACP	Access Content Package
ACS	Access Content Storage
ACSIS	Acquisition, Classification, and Shipment Information System
AES	Advanced Encryption Standard
AIP	Archival Information Package
AIS	Archival Information Storage
ANSI	American National Standards Institute
AP	Access Processor
ARK	Archival Resource Key
ASCII	American Standard Code for Information Interchange
ASP	Application Service Provider
BAC	Billing Address Code
BPEL	Business Process Execution Language
BPI	Business Process Information
BPS	Business Process Storage
CA	Certification Authority
CCSDS	Consultative Committee for Space Data Systems
CD	Compact Disk
CDN	Content Delivery Network
CDR	Critical Design Review
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
CMYK	Cyan, Magenta, Yellow, Black
CO	Content Originator
COOP	Continuity of Operations Plan
CP	Content Processor
CPI	Content Packet Information
CRC	Cyclic Redundancy Checks
CSV	Comma Separated Variable
DARD	Departmental Account Representative
DES	Data Encryption Standard
DIP	Dissemination Information Package
DNS	Domain Name System
DO	Digital Objects
DOI	Digital Object Identifier
DoS	Denial of Service
DPI	Dots Per Inch

ACRONYM	DEFINITION
DSR	Deployment System Review
DVD	Digital Versatile Disc
EAD	Encoded Archival Description
EAP	Estimate at Completion
EAP	Enterprise Application Platform
ePub	Electronic Publishing Section
FAQ	Frequently Asked Question
FBCA	Federal Bridge Certificate Authority
FDLP	Federal Depository Library Program
FICC	Federal Identity Credentialing Committee
FIFO	First In First Out
FIPS	Federal Information Processing Standard
FOB	Free on Board
FOIA	Freedom of Information Act
FTP	File Transfer Protocol
GAO	General Accounting Office
GAP	GPO Access Package
GFE	Government Furnished Equipment
GFI	Government Furnished Information
GILS	Government Information Locator System
GPEA	Government Paperwork Elimination Act
GPO	Government Printing Office
HMAC	Key Hashed Message Authentication Code
HSM	Hardware Security Module
HTML	Hypertext Markup Language
Hz	Hertz
ID	Information Dissemination
IDD	Interface Design Description
IEEE	Institute of Electronics and Electrical Engineers
IETF	Internet Engineering Task Force
ILS	Integrated Library System
IP	Internet Protocol
IPR	Internal Progress Review
IPSEC	Internet Protocol Security
ISBN	International Standard Book Number
ISO	International Organization for Standardization
ISSN	International Standard Serial Number
IT	Information Technology
ITU	International Telecommunication Union
JDF	Job Definition Format
LDAP	Lightweight Directory Access Protocol
LOC	List of Classes
LPI	Lines Per Inch
MAC	Message Authentication Code
MARC	Machine Readable Cataloging
METS	Metadata Encoding and Transmission Standard
MMAR	Materials Management Procurement Regulation
MOCAT	Monthly Catalog of Government Publications
MODS	Metadata Object Descriptive Schema

ACRONYM	DEFINITION
MPCF	Marginally Punched Continuous Forms
NARA	National Archives and Records Administration
NB	National Bibliography
NC	National Collection
NDIIPP	National Digital Information Infrastructure and Preservation Program
NET	New Electronic Titles
NFC	National Finance Center
NIST	National Institutes of Standards and Technology
NLM	National Library of Medicine
OAI	Open Archives Initiative
OAI-PMH	Open Archives Initiative Protocol for Metadata Harvesting
OAIS	Open Archival Information Systems
OCLC	Online Computer Library Center
OCR	Optical Character Recognition
OLTP	On-line Transaction Processing
PCCS	Printing Cost Calculating System
PDA	Personal Data Assistant
PDF	Portable Document Format
PDI	Preservation Description Information
PDR	Preliminary Design Review
PICS	Procurement Information and Control System
PICSWEB	Procurement Information Control System Web
PKI	Public Key Infrastructure
PKITS	Public Key Interoperability Test Suite
PKIX	Public Key Infrastructure Exchange Group within the IETF
PKSC	Public-Key Cryptography Standard
POD	Print On Demand
PPR	Printing Procurement Regulation
PREMIS	PREservation Metadata: Implementation Strategies
PRONOM	Practical Online Compendium of File Formats
PTR	Program Tracking Report
PURL	Persistent URL
RAID	Redundant Array of Inexpensive Disks
RFC	Request for Comments
RGB	Red, Green, Blue
RI	Representation Information
RMA	Reliability, Maintainability, Availability
ROI	Return on Investment
RPPO	Regional Printing Procurement Office
RSA	Rivest, Shamir, Adleman
RVTM	Requirements Verification Traceability Matrix
SAML	Security Assertion Markup Language
SDR	System Design Review
Section 508	Section 508 of the Rehabilitation Act
SF	Standard Form
SGML	Markup Language
SHA	Secure Hash Algorithm
SIP	Submission Information Package
SMP	Storage Management Processor

ACRONYM	DEFINITION
SMS	Storage Management System
SPA	Simplified Purchase Agreement
SSL	Secure Socket Layer
SSP	System Security Plan
SSR	Software Specification Review
SuDocs	Superintendent of Documents
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
U.S.C.	United States Code
URL	Uniform Resource Locator
USGPO	United States Government Printing Office
VPN	Virtual Private Network
W3C	World Wide Web Consortium
WAIS	Wide Area Information Service
WAP	Wireless Application Protocol
WIP	Work in Process
WML	Wireless Markup Language
WMS	Workflow Management System
XML	eXtensible Markup Language
XMLDSIG	XML Signature
XMLENC	XML Encryption

Glossary

Access: Services and functions that allow users to determine the existence, description, location, and availability of content, and request delivery of content and metadata.

Access aids: Tools and processes that allow users to locate, analyze, and order content and metadata.

Access Content Package (ACP): An information package that includes renditions of content and metadata that are optimized for access and delivery. See also **OAIS**

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. See also **Derivative.**

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.

Access Time: Time needed to confirm availability and location of requested data and start the process of returning data to the user.

Activity: A task that is to be completed or has been completed.

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 (AIP): An information package that includes all content, metadata and associated Preservation Description Information (PDI) needed to preserve the content in perpetuity. See also **OAIS**

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

Archive management - See **Preservation**.

Assessment: A pre-defined task that evaluates whether the original attributes of a digital object are correct. The purpose of this assessment is to provide with information needed to identify necessary preservation processes.

Attribute - A feature or characteristic; a property. Often used to describe the nature of electronic data. For example, a data value's attributes may include its data type (numeric, character, or date), range of values, or length.

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: The identity, source, ownership and/or other attributes of content are verified.

Automated Activity: An activity conducted under the direct control of the system.

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

Batch of Jobs: A set of Jobs selected by the user.

Batch of Workflow Instances: A set of Workflow Instances selected by the user.

Beta Testing: Testing that validates that the system meets the mission and business needs for the capabilities allocated to that release that involve end users. This is the last test and is part of the decision for determining if the system is ready to be deployed to public. This testing involves real-world, internal exposure or operation to the system.

Born digital: In the Future Digital System context, digital objects, created in a digital environment, with the potential of multiple output products, including hard copy, electronic presentation, and digital media.

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 Manager: A user class that makes policy decisions and develops business plans to meet Content Originator and End User expectations.

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 Execution Language (BPEL): An XML-based language to allow the sharing of tasks across a system.

Business process information: Administrative, non-content-specific information that is used or created by a business process.

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, it is the process or results of applying bibliographic control to final published versions.
Certification: 1. Proof of verification, validation, or authority. Process associated with ensuring that a digital object is authentically the content issued by the author or issuer. 2. An assessment against a known standard.
Certified: Providing proof of verification of authenticity or official status.

Chain of custody: Physical possession or intellectual ownership of content. Provides details of changes of ownership or custody that are significant in terms of authenticity, integrity, and official status.

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

Collection: A GPO defined group of related content.

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.

Composition: The process of applying a standard style or format to content.

Content: Information presented for human understanding. In FDsys, it is the target of preservation.

Content Delivery Network (CDN): An external service provider utilized for distributed storage and delivery.

Content Evaluator: A user class that determines whether submitted content is in scope for GPO's dissemination programs.

Content Originator: A user class that develops content, submits content to the system, and submits orders to GPO for services.

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.

Customization: Providing the ability for users to tailor options to meet their needs and preferences. Customization is not delivered dynamically (e.g., personalization); it is managed by users and is static until changed.

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 Center: A facility containing enterprise-grade FDsys equipment.

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, analyzing, associating, and presenting BPI and metadata to enhance internal and external business efficiencies.

Delivery time: Time needed to deliver requested data to user.

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

Derivative: A alternate presentation of content, often optimized for a specific function (e.g., access, preservation, print). Language translations are not derivatives; they are a separate publication.

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. A digital object may be an entire document or discrete unit of a document.

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 signer.

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 consists of one or more renditions of content or metadata from an AIP or ACP that is delivered to users in response to a request. See also **OAIS**

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.

End User: A user class that uses the system to access content and metadata.

Ensure: Instruction to make sure an action takes place.

External Activity: An activity that requires manual or automated processing external to FDsys.
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 (EC): The digital Government publications that GPO holds in storage for permanent public access through the FDLP or are held by other institutions operating in partnership with the FDLP.

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, 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.

Fulfillment: the processes related to the packaging and delivery of tangible goods for delivery.

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

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 identification and replication of content resident on web servers outside GPO's control.

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.

Hybrid: A package containing selected content from multiple information packages.

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: 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.

Integrity: Content has not been altered or destroyed in an unauthorized manner.

Integrity Mark: Conveys authentication information to users.

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).

Internal Activity: An activity conducted within FDsys.

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

Job: A set of manual and automated activities that produce a product or service.

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.

List of Jobs: A list of Jobs assigned to a particular user.

List of Workflow Instances: A list of Workflow Instances assigned to a particular user.

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.

Manual Activity: An activity conducted in such a manner that the system cannot exert direct control.

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.

Metadata Encoding and Transmission Standard (METS): An XML schema for encoding metadata associated with objects in a digital library.

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 (NC): A comprehensive collection of all publications in scope for GPO's dissemination programs, content that should be in the Federal Depository Library Program, 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.

Natural Granularity Boundaries: The structure that is set in a document's native format, including volumes, chapters, parts, sections, and paragraphs.

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.

Non-repudiation: Verification that the sender and the recipient were, in fact, the parties who claimed to send or receive content, respectively.

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.

Open Archival Information System Reference Model (OAIS): 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 designated 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.

Online Information eXchange (ONIX): 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.

Operations Manager: A user class that develops and optimizes workflow processes and monitors the quality of system products.

Permanent Public Access (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

Personalization: Dynamically tailoring options to match user characteristics, behavior, or preferences. Personalization is often implemented by analyzing data and predicting future needs.

Policy neutral: Refers to a system which is sufficiently flexible to accommodate changes in hardware, software, communication technology, processes, policy, personnel, locations, etc. without requiring major re-engineering or design changes. FDsys is envisioned as being responsive to policy, but it is not intended to be policy-constrained.

Pre-Ingest Bundle (PIB): Digital objects, related metadata, and BPI, gathered for transfer to a service provider in the event of a Content Originator request for a proof. After approval the PIB becomes a SIP for ingest.

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: Information necessary for adequate preservation of content information, including information on provenance, reference, fixity, and context. See also **OAIS**

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.

Public Key Infrastructure (PKI): A system of digital certificates, Certificate Authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

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

Pull: Downloading content on an as-needed basis. Content is made available for users to select and retrieve ("pull") to local servers or computers. For example, currently users may be said to pull documents from GPO Access.

Push: Intentionally and specifically serving out information to a target recipients. Content is automatically sent ("pushed") from GPO to a list of interested users. This is analogous to shipping a box of depository documents, only with electronic content instead of tangible copy.

Redundant Array of Inexpensive Disks (RAID): A set of different hardware storage configurations where multiple hard disk drives share and/or replicate data.

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.

Relationship: A statement of association between instances of entities. In PREMIS, the association(s) between two or more object entities, or between entities of different types, such as an object and an agent.

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.

Rendition: Instance of a publication expressed using a specific digital format

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

Representation Information: The information that maps a data object into more meaningful concepts. An example is the ASCII definition that describes how a sequence of bits (i.e., a Data Object) is mapped into a symbol.

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: Electronic presentation that uses enhanced sensory features such as images, video, audio, animation and user interactivity

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.

Section 508 - Section 508 of the Rehabilitation Act requires access to electronic and information technology procured by Federal agencies. The Access Board developed accessibility standards for the various technologies covered by the law. These standards have been folded into the Federal government's procurement regulations. http://www.access-board.gov/508.htm

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.

Service Provider: A user class that delivers the expected services and products.
Service Specialist: A user class that supports Content Originators and End users to deliver expected products and services.
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**.

Submission information package (SIP): The information package submitted by a Content Originator for ingest the system. See also **OAIS**

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.

System metadata: Data generated by the system that records jobs, processes, activities, and tasks of the system.

Systems Administration: A user class that directly supports the use, operation, and integrity of the system

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

Transformation: A process that produces one or more content packages from another; e.g., SIPs are transformed into Access Content Packages (ACPs) and Archival Information Packages (AIPs).

Test Case: 1. A set of test inputs, execution conditions, and expected results developed for a particular objective, such as to exercise a particular program path or to verify compliance with a specific requirement. 2. Documentation specifying inputs, predicted results, and a set of execution conditions for a test item.

A document describing a single test instance in terms of input data, test procedure, test execution environment and expected outcome. Test cases also reference test objectives such as verifying compliance with a particular requirement or execution of a particular program path

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.

Use Case: A description of the behavior of a system or part of a system; a set of sequences or actions, including variants that a system performs to yield an observable result of value.

User acceptance testing: Testing that validates that the system meets GPO's mission and business needs for the capabilities allocated to that release, in order to expose issues before the system is released to a wider audience in beta testing. This testing involves real-world, internal exposure or operation to the system.

Validation: A process that ensures (e.g., proves) that data conforms to standards for format, content and metadata.

Variable Data Printing: A form of printing where elements such as text and images may be pulled from a database for use in creating the final package. Each printed piece can be individualized without stopping or slowing the press.

Verification: The process of determining and assuring accuracy and completeness. There is a known input and an expected output is confirmed (e.g. check).

Version: Unique manifestation of content within a content package.

Version control: The activity of identifying and managing versions.

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 to content beyond an agreed upon threshold in certain categories (e.g., title, edition statement, language translation) which constitute a new version or help a Service Specialist make a version determination.

Version information: Information stored in metadata that describes the relationship between versions.

Viable application: Application software which retains all of its original functionality.

Workbench: A set of available tools for each user class (e.g., Content Originator, End User) that are displayed on a graphical user interface. A user's role (e.g., cataloger, Federal depository librarian) determines which of the tools available to his or her class will be displayed on the graphical user interface.

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 Definition: A document that defines the activities, business rules, data flows, and personnel roles that specify how a GPO business process will be performed within FDsys.

Workflow Instance: A workflow definition that is being executed on a specific entities by a specific person.

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.